VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

# DIZERTAČNÍ PRÁCE

Brno, 2017 Ing. Radek Fujdiak


# VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

## FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

## ÚSTAV TELEKOMUNIKACÍ
DEPARTMENT OF TELECOMMUNICATIONS


# ANALÝZA A OPTIMALIZACE DATOVÉ KOMUNIKACE PRO TELEMETRICKÉ SYSTÉMY V ENERGETICE

ANALYSIS AND OPTIMIZATION OF DATA COMMUNICATION FOR TELEMETRIC SYSTEMS IN ENERGY

**DIZERTAČNÍ PRÁCE**
DOCTORAL THESIS


**AUTOR PRÁCE** — **Ing. Radek Fujdiak**
AUTHOR

**ŠKOLITEL** — **prof. Ing. Jiří Mišurec, CSc.**
SUPERVISOR


**BRNO 2017**

## ABSTRAKT

Dizertační práce se zabývá výzkumem v oblasti optimalizace telemetrických systémů v energetice z pohledu informační bezpečnosti. Práce pojednává o současných problémech informační bezpečnosti, její definici a i o metodách, které vedou k naplnění bezpečnostních principů, a soustředí se zejména na oblast, kde jsou využívány zařízení s omezenými zdroji To z toho důvodu, že zařízení s limitovanými zdroji, tj. operační paměť, omezený přístup k elektrické energii, výkon, aj., představují bezpečnostní rizika, která mohou ovlivňovat následně celou energetickou infrastrukturu v případě nasazení technologií v konceptu inteligentních sítí.

Jsou přiblíženy dnešní vědecké výzvy v této oblasti, objasněna terminologie i legislativa, která je pro tuto oblast také velice zásadní. Hlavní část dizertační práce je následně věnována výzkumu vlastního hybridního řešení, kryptosystému. Jedná se o řešení, které nenaplňuje pouze jeden bezpečnostní princip (např. pouze autentičnost), nýbrž o řešení, které nabízí všechny požadované principy informační bezpečnosti v energetice. Je provedena hloubková analýza dnešních řešení, které jsou následně evaluovány vlastními měřeními i pomocí současné aktuální literatury. Následně je proveden návrh kombinací symetrických a asymetrických kryptografických algoritmů, tak aby byla zaručena efektivita výsledného systému, ale také zachována jeho komplexnost systému. Jedná se o kombinaci symetrických blokových algoritmů elektronické kódové knihy, zajišťující autentizaci a integritu pomocí náhodných klíčů, řetězení šifrovaného textu zajišťující důvěrnost, společně s algoritmem Diffieho-Hellmana nad eliptickými křivkami zajišťující bezpečnou distribuci a výměnu symetrických tajných klíčů.

V neposlední řadě je přiblížen provedený vlastní vývoj a optimalizace hybridního kryptosystému. Je představeno vlastní řešení pro reprezentaci velkých čísel a modulární algebru v zařízení s limitovanými zdroji, které je ověřeno experimentálními měřeními. Dále je rozebrán vlastní návrh, validace a optimalizace řešení náhodných hardwarových generátorů (založených na efektivním principu kvantizační chyby a protichůdných oscilátorů). Je také řešena navržená část symetrické kryptografie, kde je využito dvou dostupných knihoven, které jsou následně znatelně optimalizovány. V neposlední řadě je představen provedený rozsáhlý výzkum kryptografie eliptických křivek a možností distribuce symetrického klíče. Jsou implementovány algoritmy pro výpočty s body eliptických křivek nad polem s prvočíselným řádem i nad polem řádu 2. Realizace pak zahrnovala více než 50 eliptických křivek různých standardů, kde největším úspěchem jsou křivky nad polem prvočísel o řádu $p = 256$. Tyto křivky v době řešení nebyly na takto hardwarových platformách řešeny. Nakonec jsou představeny originální výsledky výzkumu, který se zabýval vhodnou volbou křivek a studií jejich doménových parametrů z pohledu vztahu velikosti k rychlosti operací nad křivkou.



## KLÍČOVÁ SLOVA

Telemetrické systémy, optimalizace, senzorické sítě, inteligentní sítě, internet věcí, senzory, informační bezpečnost, kryptografie, kryptografické algoritmy, kryptosystém, důvěrnost, integrita, autentičnost, čerstvost, nepopiratelnost.

# ABSTRACT

The dissertation thesis focuses on research in the optimisation of telemetry systems in energy from the perspective of information security. The thesis deals with nowadays challenges in information security, its definition as well as its methods. The main focus is on the area, where devices with limited resources such as memory or computational power are used. These devices pose security risks that may affect the entire smart grid infrastructure. Nowadays research challenges terminology and legislative, which is crucial in the defined area, are brought closer. The main part of this thesis is devoted to the research of the author's own hybrid solution – the hybrid cryptosystem. The solution fulfils all necessary principles of information security – authenticity, confidentiality, integrity and data freshness. An analysis of today's solutions is provided together with a complex evaluation based on own experimental measurements and available literature sources. Subsequently, a combination of symmetric and asymmetric cryptography algorithms is designed that provides both high efficiency and complexity. It is a combination of the symmetric block cyphers Electronic Code Book, which provides authenticity and integrity by using random keys, Cipher Block Chaining, which provided confidentiality, and the asymmetric algorithm of Diffie-Hellman over Elliptic Curves, which provides key agreement scheme over an unsecured channel. Further, the development and optimisation of the hybrid cryptosystem are brought in light. The proprietary solution of large number representation and modular algebra in a device with limited resources is presented and validated via own experimental measurements. Moreover, the own design is analysed and the two proposed hardware generators (based on efficient methods of quantization error and opposing oscillators) are evaluated and optimised. Additionally, the symmetric part of the cryptosystem is also investigated, where two main solutions are highly optimised. Last but not least, deep research on the cryptography of elliptic curves and the key distribution scheme is presented. Two main curve types are dealt with – over a finite field and over a field of characteristic two. The implementation included more than 50 elliptic curves of different standards. The implementation of the curves of order $p = 256$ has the highest impact. These curves were not addressed on such devices at the time of solution. Finally, the original research results of possible speed optimisation via using special elliptic curves are introduced. The relationship between curve domain parameters and point computational efficiency is studied. This last part brings also promising results for the field of effective cryptographic algorithm – the lightweight cryptography.



# KEYWORDS

Telemetry system, Optimisation, Sensoric networks, Smart Grid, Internet of Things, Sensors, Information security, Cryptography, Cryptography algorithms, Cryptosystem, Confidentiality, Integrity, Authentication, Data freshness, Non-Repudiation



FUJDIAK, Radek. *Název studentské práce*. Brno, Rok, 146 s. Dizertační práce. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací. Vedoucí práce: prof. Ing. Jiří Mišurec, CSc.

# PROHLÁŠENÍ

Prohlašuji, že svou dizertační práci na téma „Název studentské práce“ jsem vypracoval(a) samostatně pod vedením školitele dizertační práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor(ka) uvedené dizertační práce dále prohlašuji, že v souvislosti s vytvořením této dizertační práce jsem neporušil(a) autorská práva třetích osob, zejména jsem nezasáhl(a) nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom(a) následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

Brno ..... .....

podpis autora(-ky)

# PODĚKOVÁNÍ

Rád bych poděkoval svému vedoucímu Prof. Ing. Jiřímu Mišurcovi, CSc., za jeho smysl pro humor, odborné vedení, konzultace, trpělivost a hlavně za to, že mne nenechal spát a studovat ve stanu. Dále bych také rád také tímto poděkoval mému kolegovi a kamarádovi doc. Ing. Petru Mlýnkovi, Ph.D., za jeho neskonalou pomoc při řešení všedních i nevšedních problémů a za to, že mne nenechal nikdy topit. V neposlední řadě velké díky patří také Ing. Pavlovi Maškovi, mému dobrému příteli a skvělému kolegovi, za jeho inspiraci, soudržnost, ale také neskonalou a všudy přítomnou pomoc. Mé díky však patří také všem mým kolegům, přátelům a blízkým, kteří ve mne věřili a stáli při mne v těch dobrých i horších chvílích.

Brno ..... .....

podpis autora(-ky)


Faculty of Electrical Engineering
and Communication
Brno University of Technology
Purkynova 118, CZ-61200 Brno
Czech Republic
http://www.six.feec.vutbr.cz

## PODĚKOVÁNÍ

Výzkum popsaný v této dizertační práci byl realizován v laboratořích podpořených z projektu SIX; registrační číslo CZ.1.05/2.1.00/03.0072, operační program Výzkum a vývoj pro inovace.

Brno ..... .....

podpis autora(-ky)


EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI


OP Výzkum a vývoj
pro inovace

*Mým rodičům, mé sestře a Ině,*
*za jejich rady, trpělivost a neskonalou důvěru i podporu,*
*protože oni tu vždy pro mne byli ...*

# OBSAH

# SEZNAM OBRÁZKŮ

# SEZNAM TABULEK

# ÚVOD

Díky velkému rozvoji nových komunikačních technologií, miniaturizaci v řadě oborů informačních technologií a i díky mnohým dalším vědeckým pokrokům, žijeme dnes již v době digitálního věku [1]. Inteligentní sítě (z angl. Smart Grid), chytrá města (z angl. Smart City), chytré továrny (z angl. Smart Factory), chytré domácnosti (z angl. Smart Home) či mnoho dalších celků se stávají běžnou realitou a začínají tvořit jednu komplexní infrastrukturu, která propojuje celý svět mnohem více, než se vůbec předpokládalo za možné [2]. V této infrastruktuře, jedné globální rozsáhlé celosvětové síti, se nachází miliardy propojených a vzájemně komunikujících zařízení bez nutnosti interakce člověka. Tento koncept shrnuje vize internetu věcí (IoT, z angl. Internet of Things) [3].

Koncept vzájemně propojených chytrých zařízení, byl poprvé diskutován začátkem roku 1982 a předveden na Carnegie Mellon University, kde vytvořili první zařízení svého typu, inteligentní výdejní automat, připojené k internetu [4]. Nicméně pojem internetu věcí byl poprvé použit až Kevinem Ashtonem v roce 1999, který hovořil o jednoznačně identifikovatelných objektech a jejich virtuální reprezentaci ve strukturách typu internet. Těmito objekty myslel cokoliv od velkých budov, průmyslových podniků, letadel, automobilů, strojů, jakéhokoliv druhu zboží, lidí, zvířat, rostlin a dalších. Nicméně až v letech 2003–2005 začal hlavní rozvoj internetu věcí, společně s jeho prvními zmínkami v odborné literatuře [5].

Dnes jsou tyto zařízení již běžnou součástí našeho života a jejich přítomnost si už ani neuvědomujeme. Můžeme se s nimi setkat denně v našich mobilních zařízeních, automobilech, domácnostech, na ulicích ve městech, továrnách, nemocnicích a spousty dalších odvětví či částí našeho života, kde pomáhají zefektivňovat a zjednodušovat každodenní procesy. Jedná se o vzájemně propojené senzory či měřící zařízení, tvořící telemetrický systém, který využívá pro sběr dat distribuovanou senzorovou síť [6]. V posledních letech lze zaznamenat zvyšující se zájem o senzorové sítě, převážné díky velkému rozvoji bezdrátových technologií a jejich dostupnosti [7]. Bezdrátové technologie se stávají mnohem dostupnější díky miniaturizaci a integraci procesorů, rádiových čipů a senzorů do jednoho funkčního čipu (SoC, z angl. System on a chip) [8]. Levné SoC čipy pak dovolují tedy tvořit rozsáhlé senzorové sítě s velkým množství zařízení, které jsou následně využívány ke sběru velkého množství dat tzv. telemetrickými systémy, které tyto data dále zpracovávají. Nízká cena čipů, jejich energetická efektivita a možnost fungovat jednotky až desítky let na baterii je však většinou cenou za nižší výpočetní výkon [9]. Dnes tyto systémy nejsou již nasazeny pouze jako pilotní projekty (PoC, z angl. Proof-of-Concept), ale jsou reálně využívány v celé řadě odvětví mj. v dopravě, průmyslu, bankovnictví a spousty dalších, kde se přenáší citlivá soukromá data [10], ale i v oblastech jako energetika,

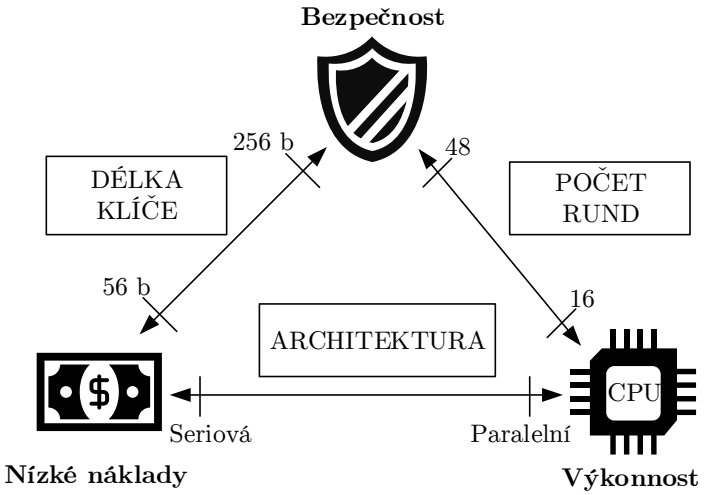
zdravotnictví a vojenství, kde data mají kritický charakter z pohledu životů občanů či integrity a bezpečnosti států [11].

Bezpečnost v těchto oblastech je mnohdy určována dle dosavadních národních či mezinárodních standardů, doporučení a zákonů. Ty však většinou řeší pouze procesní otázky a následně v těchto oblastech doporučují užití robustních a velmi komplexních algoritmů, které mají chránit daný systém z pohledu informační bezpečnosti. Nicméně často užívaná zařízení s limitovaným výpočetním výkonem již z principu nemohou naplnit tyto velké požadavky a je nutno u nich najít vhodný kompromis. Ten by mělo tvořit řešení, které bude mít dostačující úroveň bezpečnosti, ale zabezpečení u něj bude prováděno, co možná nejefektivněji a nejlevněji. Efektivita je zde myšlena z pohledu výpočetní náročnosti i energetická efektivity, která je důležitá z pohledu dlouhé výdrže senzorů na baterii (5–15 let) [12] či snížení netechnických ekonomických ztrát [13]. Ekonomická stránka na druhé straně hraje velkou roli, díky uvažovanému nasazení velkého množství zařízení [14]. To jsou mj. i důvody, proč není možné v těchto oblastech využívat aditivních specializovaných zařízení, které jsou v jiných oblastech běžné. Každé další zařízení zde totiž zvyšuje nejen cenu, ale i energetickou náročnost finálního řešení, kdy navíc každý další prvek potřebuje aditivní energetický zdroj [15]. Z toho důvodu se uvažuje o jednom komplexním zařízení, které slouží nejen k interakci s měřícími prvky, ale také zajistí komunikaci i její zabezpečení [16]. Tuto úlohu znesnadňují nejen výše popsané technologické překážky, ale i neustále se zvyšující nároky na bezpečnost díky rostoucím výpočetním výkonům [17], nejednotnosti standardů [18], velkým nárokům na interoperabilitu [19], multi-technologickému prostředí [20] a dalším.

V posledních letech velice rychle roste zájem právě o informační bezpečnost, kde jedním z důvodů jsou i zvyšující se úspěšné útoky na síťové prvky, infrastruktury států, úniky informací, ohrožení soukromí i životů osob, či až ohrožení samotné integrity a bezpečností států [21]. Náchylnost těchto systémů na pasivní i aktivní útoky dokazuje celá řada nejen laboratorně provedených útoků, ale i spousty reálných útoků. Nejčastější jsou útoky hrubou silou, ale i další již velmi sofistikované útoky. Jedním z nedávných příkladů může být i kybernetický útok na Ukrajině, který způsobil výpadek dodávky elektrického proudu ve velmi velkém rozsahu [22]. Energetika je právě jednou z hlavních oblastí, která dnes prochází velkými změnami. Nové technologie umožňují vybudování energetických inteligentních sítí, které mají napomáhat v řízení energetické infrastruktury, regulace energie, komplexnímu monitoringu a dalšímu zefektivňování procesů. V kontextu zmíněných bezpečnostních rizik to však vytváří i mnoho nových výzev [23].

Uvažujme tedy oblast energetiky a zabezpečení komunikace u telemetrických systémů, využívající zařízení s limitovanými zdroji (paměť, energie, výkon, aj.). V této oblasti se pak v praxi snažíme o komplexní úlohu, kde hledáme vhodné řešení

zabezpečení optimalizováním třech základních parametrů - bezpečnost, náklady a výkonnost (viz Obr. 1, kde počet rund a délka klíče slouží pro budování bezpečnostních algoritmů a architekturou je myšlena hardwarová architektura).




Obr. 1: Ukázka hledání vhodného kompromisu bezpečnosti, nákladů a výkonnosti (myšlenka převzata z [24]).

Obecně je úloha optimalizace dvou ze tří těchto parametrů považována za primitivní (bezpečnost-výkon, bezpečnost-náklady či náklady-výkon). Nicméně neprimitivní složitou úlohou je pak optimalizace všech tří parametrů zároveň (bezpečnost-výkon-náklady). V této práci se dále zaměříme právě na hledání efektivního řešení zabezpečení komunikace u moderních telemetrických systémů v energetice z pohledu všech tří parametrů [24].

Tato práce je dále dělena následovně. V rámci kapitoly 1 je popsána problematika telemetrických systémů, rozebrána oblast bezpečnosti, společně s definováním oblasti práce a její hlavní motivací. Z této kapitoly pak vychází i cíle práce, které jsou popsány společně s metodikou v kapitole 2. Dále pak v kapitole 3 jsou analyzovány jednotlivé technologie používané v moderních telemetrických systémech a rozebrány dnešní možnosti pro zajištění informační bezpečnosti. Kapitola 4 navazuje výběrem vhodných metod pro zajištění informační bezpečnosti ve vybrané oblasti telemetrických systémů, společně s návrhem i popisem realizace vlastního systému pro zabezpečení komunikace. Kapitola 5 pak pokračuje experimentálními měřeními a validací dílčích částí realizovaného systému. V této kapitole je mj. provedena i diskuze výsledků a porovnání s ostatními pracemi. V neposlední řadě pak kapitola 6 závěrem shrnuje práci, dosažené výsledky a nastiňuje možnosti i směr pro budoucí pokračování výzkumu.

# 1 OBLAST ZÁJMU A MOTIVACE PRÁCE

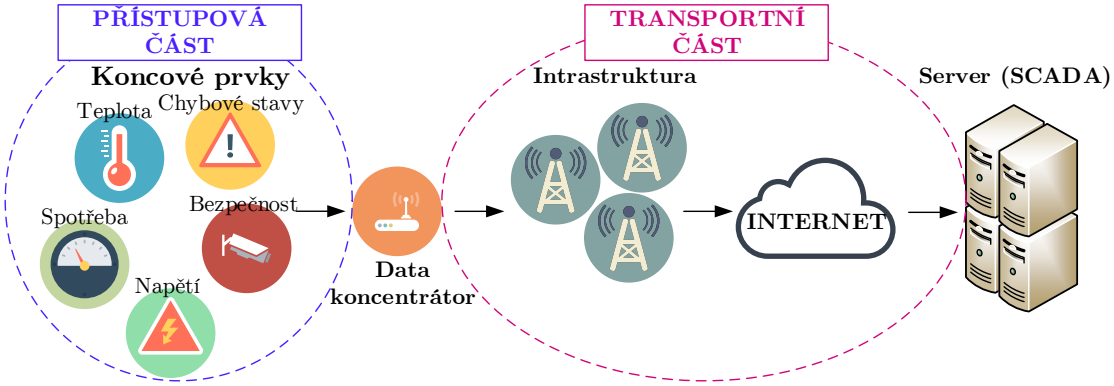
Jestliže internet věcí je jedna globální propojená infrastruktura, pak její jednotlivé části, tedy inteligentní sítě, chytrá města, chytré továrny, chytré domácnosti, a další, představují jednotlivé aplikační oblasti uvnitř této infrastruktury. Pokud uvažujeme inteligentní sítě v energetice, pak aplikační oblastí je zde využití potenciálu měřených či jinak získaných dat k vytvoření automatizované energetické sítě, která bude schopna efektivně a v reálném čase reagovat na různé potřeby, hrozby a další situace. Telemetrické systémy jsou pak tedy jeden z hlavních prostředků či nástrojů k dosahování aplikačního potenciálu této oblasti - získávání relevantních dat, které slouží při rozhodovacích procesech - tzv. inteligenci v síti.

V této kapitole si dále nejprve definujeme uvažovanou oblast telemetrických systémů, jejich vlastností, potřeb a dalších specifik. To je provedeno v kapitole 1.1. Následně v rámci kapitoly 1.2 jsou rozebrány obecné pohledy na řešení bezpečnosti, přiblíženy potenciální hrozby a způsoby jejich prevence. V neposlední řade je v kapitole 1.3 popsána hlavní motivace této práce z aplikačního, výzkumného i legislativního hlediska.

## 1.1 Přehled problematiky telemetrických systémů

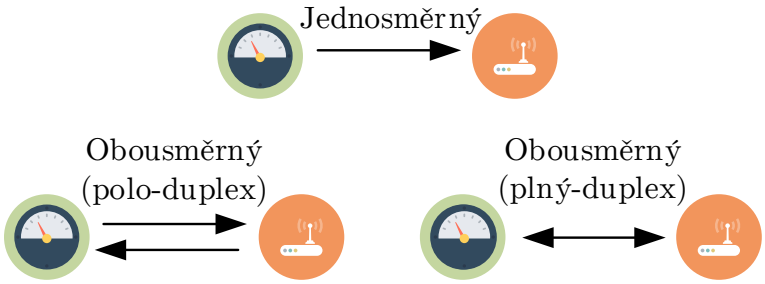
Telemetrické systémy lze rozdělit z pohledu komunikačních technologií na dvě hlavní části - přístupovou a transportní část. Rozdělení vychází z logiky, jakým způsobem je na jednotlivých úrovních komunikováno, jaké parametry tyto úrovně mají či k čemu dané úrovně slouží. Transportní část je řešena robustními technologiemi s vysokou spolehlivostí i propustností [25]. Jedná se o část sítě, která je trvale napájena a bývá často i zálohována jak energeticky, tak i komunikačně [26]. Tato část poskytuje přenos velkého množství dat a informací z data koncentrátorů až do koncového serveru (cloudu). Přenosovým médiem je zde převážně rádiové licenční pásmo např. WiMAX, 2G+, proprietární, aj., metalické či optické kabely [27]. Přístupová část je pak řešena technologiemi, které nabízí dostatečnou přenosovou kapacitu, spolehlivost pro danou aplikaci (senzor), energetickou efektivitu a zároveň nízké náklady [26]. Jedná se o část sítě, která již nemusí být trvale napájena (napájení zajišťuje bateriový zdroj), může mít omezený přístup k dodávkám elektrické energie (např. napájení pouze ze solárního panelu) či je požadována minimální spotřeba z důvodů netechnických ztrát a snižování nákladů na jedno zařízení tak, aby v globálním měřítku byly náklady, co nejmenší. "Dostatečné" parametry jsou v tomto případě velmi relativní pojem a to z důvodu velké různorodosti aplikací. Bez jasné specifikace konkrétní aplikace tak nejde jednoznačně parametrizovat tuto přístupovou část. Přenosovým médiem je v této části většinou rádiové prostředí (2G, LPWAN, WiFi, ZigBee,

Z-Wave, 6LowPAN, Thread, ostatní proprietární, aj.) a ve specifických případech pak jiné médium např. elektrické vedení (PLC) [28]. Samotná topologie se může s jednotlivými aplikačními scénáři a použitými technologiemi měnit, nicméně základní příklad telemetrického systému můžeme vidět na Obr. 1.1.



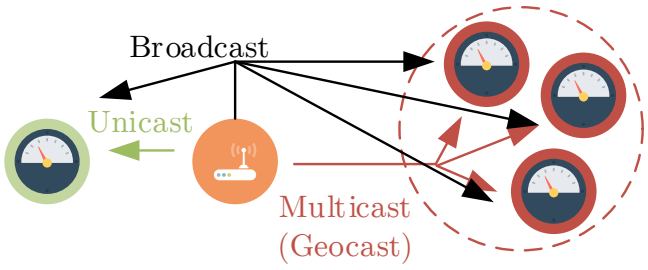

Obr. 1.1: Příklad možné topologie telemetrického systému v energetice.

Podívejme se nyní na jednotlivé techniky, využívané v telemetrických systémech komunikačními technologiemi. Jako první můžeme uvést jednu z nejzákladnějších technik tzv. směrovost spoje resp. typ spoje mezi dvěma komunikujícími body. V rámci komunikace máme dva základní typy spojů [29]: (i) jednosměrné spoje a (ii) obousměrné spoje. Jednosměrné spoje jsou v praxi obecně levnější, jednodušší a bezpečnější oproti obousměrným spojům. Na druhou stranu nám jednosměrné spoje nedovolují kontrolu, řízení, nastavení, aktualizaci software a další, dnes již často požadované vlastnosti, které obousměrné spoje umožňují [30]. U obousměrných spojů navíc určujeme ještě tzv. duplex, tedy zda jsou schopny zařízení komunikovat současně (plný-duplex, z angl. full-duplex) či pouze střídavě (polo-duplex, z angl. half-duplex) [31]. Jednotlivé typy spojů jsou zobrazeny na Obr. 1.2




Obr. 1.2: Ukázka typů spojů.

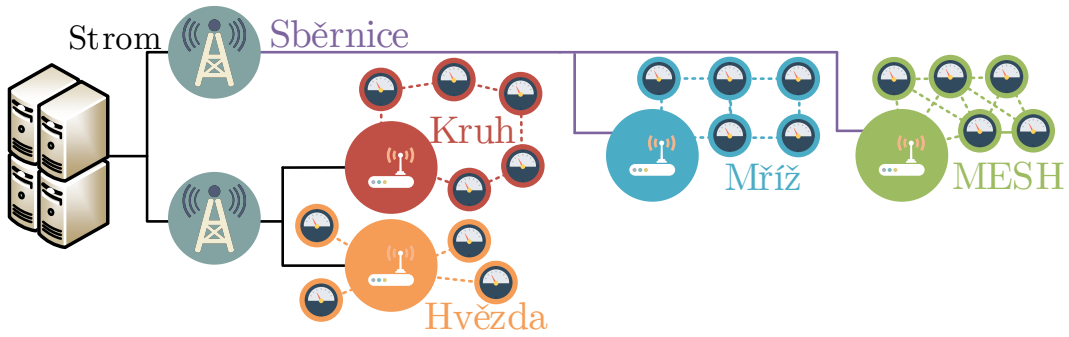
Dále můžeme uvést různé způsoby adresování, tedy [32]: (i) unicast, (ii) multicast, (iii) broadcast, (iv) anycast a (v) geocast. Unicast znamená, že se přenáší data pouze v rámci dvou bodů. Multicast znamená, že se data přenáší z jednoho bodu na více bodů. Broadcast je pak speciální typ komunikace, kdy adresátem jsou všechny připojené stanice ke komunikačnímu mediu. Poslední je geocast. Tento způsob je podobný jako multicast, s podmínkou, že daná množina bodů se vybírá na základě geografické polohy. Každé adresování má samozřejmě své výhody a nevýhody vzhledem k nastavené aplikaci. Pokud budeme skutečně chtít poslat pouze jednu zprávu z jednoho zařízení na jedno další konkrétní zařízení, pak skupinové zasílání zpráv je redundantní, neefektivní a ztrácí zcela smysl. Nicméně pokud budeme chtít poslat stejnou zprávu všem uživatelům (broadcast) či např. vypnout specifickou skupinu senzorů (multicast, geocast), pak je unicast adresování méně vhodnou a mnohem složitější variantou. Obr. 1.3 zobrazuje ukázku jednotlivých způsobů adresování.




Obr. 1.3: Ukázka jednotlivých typů adresování.

V rámci architektury sítí je dále možné sledovat i různé typy topologií [33]: (i) kruhová topologie, (ii) sběrnicová topologie, (iii) topologie hvězda, (iv) mesh topologie, (v) stromová topologie a (vi) mřížová topologie. Sběrnicová topologie většinou není tak častá, setkat se s ní můžeme například u připojení páteřních bran, základnových stanic jednotlivých technologií apod., kde tedy jsou jednotlivé důležité prvky připojeny na tzv. páteř sítě. Kruhová topologie také není příliš častá, většinou se s ní dá setkat v rámci inteligentních sítí. Jedná se o síť, kde každý prvek má vždy dvě komunikační cesty. Mřížová síť pak představuje redundantnější řešení kruhové sítě, kde opravdu samotná, kde okrajové prvky sítě mají 2–3 spoje a vnitřní prvky síť pak 4 spoje. Tato topologie je také velice častá v rámci inteligentních sítí v energetice. Topologie typu MESH je pak teoreticky nejredundantnější topologií (obzvláště pokud se jedná o tzv. plnou MESH, kdy je každý prvek propojený s každým dalším prvkem v síti). Stromová topologie pak představuje základní topologii a hierarchii v sítích, kdy jednotlivé nejdůležitější (páteřní) prvky jsou nahoře a postupně se na ně napojuje celá infrastruktura. Jako poslední je zde topologie hvězda, která je velice často užívána

v místech tzv. přístupového bodu, do kterého se připojují následně větší množství senzorů. Pokud bychom měli probírat jednotlivé výhody a nevýhody těchto topologii. Pak redundantnější topologie vyžadují mnohem větší nároky na administrativu, management, šířku pásma, aj., ale poskytují za to nejspolehlivější typ spojů [34]. Naopak např. topologie typu hvězda poskytuje ideální (nejjednodušší) řešení pro připojení velkého množství zařízení, nicméně po výpadku přístupového bodu vypadne i celá skupina přístupových bodů (to se v praxi často řeší redundantním pokrytím oblasti více přístupovými body či jinými záložními technikami, tak aby při výpadku nedošlo ke ztrátě komunikace) [35]. V praxi je většinou použita kombinace výše uvedených topologií, aby se dosáhlo požadovaných parametrů v rámci celé sítě. Jednotlivé ukázky topologií jsou znázorněny na Obr. 1.4 níže.




Obr. 1.4: Ukázka jednotlivých typů sítí dle topologie.

V neposlední řadě lze dělit sítě dle jejich rozsahu, kde ty nejznámější jsou [36]: (i) lokální sítě (LAN, z angl. Local Area Network), (ii) metropolitní sítě (MAN, z angl. Metropolitan Area Network), a (iii) rozsáhlé sítě (WAN, z angl. Wide Area Network). Sítě typu LAN jsou sítě malého rozsahu o několika komunikačních bodech, dle speciálního užití je možné rozeznávat například domácí sítě (HAN, z angl. Home Area Network), bezdrátové LAN (WLAN, z angl. Wireless LAN), aj. Převážně se jedná tedy o soukromé sítě jednotlivých uživatelů, které se používají na jednoduché sdílení dat a služeb. Rychlostně se tyto sítě dnes již pohybují od stovek Mb/s až po Gb/s [37]. Metropolitní sítě jsou již většího rozsahu než LAN a svou rozlohou odpovídají geografickému území po několik bloků až celá města. Sítě jsou využívaný skupinou jednotlivců, organizacemi či samotným městem. Jedná se také většinou o několik více propojených menších sítí dohromady. V neposlední řadě sítě WAN již pokrývají opravdu velké geografické území, jedná se například o celý stát či kontinent. WAN sítě jsou globální sítě a slouží většinou pro propojení většího počtu menších sítí do jednoho globálního celku. Jednou z nejznámějších a největších sítí je síť Internet. Toto jsou základní typy sítí pro oblast energetiky, pro úplnost, samozřejmě existují

další typy sítí jako např. [38, 39, 40, 41]: osobní sítě (PAN, z angl. Personal Area Network), sítě uvnitř těla (BAN, z angl. Body Area Network), nanosítě (z angl. nanoscale network), sítě tzv. blízkého okolí (NAN, z angl. NearMe-Area Network), sítě tzv. blízkého pole (NFC, z angl. Near-Field communication), korporátní sítě (CAN, z angl. Campus či Corporate Area Network) či sítě v rámci internetu (IAN, Internet Area Network). V energetice či inteligentních sítích se s těmito typy sítí však přímo nesetkáme [19, 42]. Z tohoto důvodu budeme dále uvažovat pouze základní rozdělení sítí dle rozlohy na LAN, MAN a WAN.

Jak můžeme vidět, tak nelze z globálního pohledu na celou infrastrukturu říci, že by se používala pouze jedna technologie či jedna přenosová technika. V praxi jsou telemetrické systémy téměř vždy řešeny více technologiemi a jedná se tedy o hybridní multi-technologické prostředí [20]. Proto je nutné, aby jakékoliv řešení, uvažované pro tyto oblasti, bylo co možná nejvíce nezávislé a zaručovalo vysokou míru interoperability. Z tohoto důvodu se tato práce mj. zaměřuje i na analýzu jednotlivých technologií a standardů, které se v rámci inteligentních sítí uvažují, čímž se zaručí maximální využitelnost uvažovaného řešení. Jedním z cílů je tedy vytvořit takové řešení, které bude možné využít napříč jednotlivými komunikačními technologiemi, používanými v energetice, resp. inteligentních sítích.

## 1.2 Základní principy bezpečnosti

Bezpečnost je možné brát z mnoha pohledů, dle komodity, kterou chráníme. Z tohoto důvodu rozlišujeme [43]: (i) fyzickou bezpečnost, (ii) počítačovou bezpečnost, (iii) síťovou bezpečnost, (iv) datovou bezpečnost, (v) informační bezpečnost, (iv) kybernetickou bezpečnost, a spousty dalších. Z pohledu zabezpečení komunikace je důležité uvažovat o zabezpečení dat resp. informací, které tyto data nesou. Bezpečnost informace či lépe informační bezpečnost je obor, který má kořeny již od dob první lidské komunikace [44]. V dnešní době velkého pokroku v oboru komunikačních technologií však bylo nutné, aby informační bezpečnost prošla jistou formou evoluce. Po dlouhé roky byla základem pro informační bezpečnost tzv. trojice bezpečnostních principů důvěrnost-integrita-dostupnost (CIA Triad, z angl. Confidentiality-Integrity-Availability Triad) [45]. Tento základní princip zajišťování informační bezpečnosti však pro dnešní svět již nebyl dostatečný [46]. Dnes již existuje celá řada názorů a definic, jakým způsobem nahlížet na informační bezpečnost a jaké principy zahrnovat. Tab. 1.1 definuje různé pohledy na informační bezpečnost.

Tab. 1.1: Příklad definice informační bezpečnosti z různých zdrojů.

| Rok | Definice | Zdroj |
|---|---|---|
| 1998 | Definován dnes již známý tzv. Perkerianův Hexagon, kde Donn B. Parker přidal do definice CIA další tři základní principy - autenticita, užitečnost a kontrola. | [47] |
| 2000 | Hewlett-Packard definuje informační bezpečnosti jako proces ochrany intelektuálního vlastnictví organizace. | [48] |
| 2001 | Na konferenci "Workshop on New Security Paradigms" byla definována autorem McDermott informační bezpečnost jako oblast řízení rizik, jejíž úlohou je řídit náklady na informační riziko pro podnik. | [49] |
| 2003 | V magazínu Computer & Security (C&S) byl vydán článek popisující informační bezpečnost jako dobře informovaný pocit jistoty, že informační rizika a kontrola jsou v rovnováze. Článek se dále kriticky zabývá novou definicí informační bezpečnosti z pohledu do té doby známých principů. | [50] |
| 2003 | Ve stejném čísle magazínu C&S vychází jiný článek s jinou definicí a pohledem na informační bezpečnost. Autoři ji definují z pohledu ochrany informace a minimalizace rizik spojených s odhalením informací neoprávněným stranám. | [51] |
| 2005 | Vydána kniha "Information Security Risk Analysis, Second Edition" v této knize se autor zabývá mj. i informační bezpečností, kde její funkci definuje na základě tří principů - datová integrity, datová senzitivita (v tomto případě ve smyslu důvěrnosti) a datová dostupnost. | [52] |
| 2008 | Mezinárodní organizace ISACA (z angl. Information System Audit and Control Association) definovala informační bezpečnost jako zajištění přístupu oprávněných uživatelů (důvěrnost) k přesným a úplným informacím (integrita) a to tehdy, když je to potřeba (dostupnost). | [53] |
| 2009 | Vzniká ISO/IEC27000:2009, kde je informační bezpečnost definována na základě zachování důvěrnosti, integrity a dostupnosti informací s případným zahrnutím i dalších prvky jako autentičnost, odpovědnost, nepopiratelnost, aj. | [54] |
| 2010 | Vydán článek v magazínu C&S, kde byla definována informační bezpečnost jako minimalizace rizik způsobených zaměstnanci, škodlivou interakcí aj. akty s informačními aktivy organizace. | [55] |
| 2010 | Výborem pro systémy národní bezpečnosti USA (CNNS, z angl. Committee on National Security Systems) vydán slovník kybernetických pojmů, kde mj. byla definována i informační bezpečnost. Ta je zde definována jako ochrana informací a informační systémů proti neautorizovanému přístupu, užívání, úpravě či zničení (vzhledem k důvěrnosti, integritě a dostupnosti). | [56] |
| 2013 | Vychází kniha "Organizational, Legal, and Technological Dimensions of Information System Administration", kde autoři definují informační bezpečnost z pohledu cílů, které zahrnují mj.: důvěrnost, integritu, dostupnost, soukromí, bezpečnost, autenticitu, nepopiratelnost, zodpovědnost a auditovatelnost. | [57] |
| 2013 | Ve stejném vychází také kniha "Principles of Information Security", v této knize se autoři zabývají informační bezpečností, její historií i jejími dopady či definicí. Autoři v této knize se při definici odkazují na definici z roku 2010 od Výboru pro systémy národní bezpečnosti USA, CNNS. | [58] |
| 2015 | Výborem pro systémy národní bezpečnosti USA aktualizuje slovník kybernetických pojmů. Definice informační bezpečnosti však zůstává nezměněna. | [59] |

Výše uvedené zdroje však spojuje jedna základní myšlenka. Nároky na bezpečnost dnešních komunikačních, informačních a kybernetických systémů je nutno posuzovat z pohledu tzv. bezpečnostních funkcí, cílů či principů (pro jednoznačnost textu bude dále použit jednotný název bezpečnostní principy). Výčet těchto principů se v rámci odborných zdrojů liší. Postupem času a vzniku nových hrozeb či potřeb,

jsou stanovovány nové požadavky na bezpečnost a i nové principy bezpečnosti. Tyto principy můžeme obecně zařadit do dvou různých oblastí, tedy do informační bezpečnosti a procesní bezpečnosti. Procesní bezpečnost bude definována z pohledu na interní procesy v rámci uvažované sítě, systému či celé infrastruktury. Jedná se o obecnější pohled na bezpečnost, do kterého spadají následující bezpečnostní principy:

- **Autorizace**, zjednodušeně lze tvrdit, že se jedná o přidělení práv účastníkům či prvkům sítě (osoby, zařízení, procesy, systémy, aj.) ke specifickým úkonům. Lze na ni pohlížet jako na proces přidělování přístupu a proto je také tento princip mnohdy označován pojmem řízení přístupu. Jedná se tedy o přidělení přístupu k specifickým zdrojům sítě, datům, informacím či přidělení přístupu do sítě, k přenosovému médiu, k ovládání specifických prvků sítě, aj. Autorizace by měla vždy probíhat až po jednoznačné a důvěryhodné identifikaci, protože bez ní si nemůžeme být jisti, komu daná práva přidělujeme [60]. Autorizace je zajištěna na základě interní politiky v síti [61].
- **Dostupnost**, jedná se o tzv. spolehlivost služby, systému, zařízení aj. Vyjadřuje se v procentech jako poměr mezi střední dobou mezi poruchami (MTBF, z angl. Mean Time Between Failures) a součtem tvořeným z MTFB a průměrnou dobou výpadku (MTTR, z angl. Mean Time To Repair) [62]. Pro zajištění dostupnosti je nutno dodržovat pravidelnou údržbou veškerého hardwaru, aktualizacemi hardwaru i softwaru, zajištěním dostatečné komunikační šířky pásma a zabráněním vzniku úzkých míst v komunikačním řetězci. Kromě výpadků zapříčiněnými vnějšími vlivy je nutno však uvažovat i nežádoucí útoky třetích osob. V rámci dostupnosti se jedná hlavně o tzv. útoky DoS (z angli. denial-of-service) [63]. Jedná se o scénáře, kdy je útočníkem zahlcována síť, zařízení, služba aj. Těmto útokům lze zabránit kvalitním bezpečnostním managementem, jasně stanovenou autorizací v rámci sítě a využitím specializovaného hardwaru (např. firewall či proxy server), sledování provozu sítě v reálném čase pomocí sofistikovaných analytických algoritmů a včasné vyhodnocení příchozích útoků či nežádoucích chování v síti [64].
- **Soukromí**, je očividné, že díky příchozímu internetu věcí, inteligentním sítím a čím dál více se rozrůstajícího digitálního světa, ztrácíme část soukromí. Jedná se např. o osobní údaje, know-how firem, ale i např. údaje o spotřebě aj. [65]. Tato problematika je netriviální a věnuje se jí celá řada zákonů, doporučení aj. [66]. Sběr osobních údajů by měl být pouze na nezbytně dlouhou dobu a pouze pro účely dané služby, je také nutno mít vždy souhlas uživatele s ukládáním a využíváním těchto soukromých údajů. I přesto, že společnosti mají souhlas uživatelů k ukládáním části soukromých údajů, je nutno dodržet zásady neposkytování těchto údajů

třetím stranám a také zaručit, že v žádné části životního cyklu těchto informací nebudou vystaveny tyto údaje možnému úniku, získání či zneužití třetí osobou [67]. V tomto případě je nutno sledovat bezpečnostní standardy, doporučení a zákony, které jasně říkají jak s těmito informacemi má být zacházeno po celou dobu jejich životního cyklu.

- **Auditovatelnost**, jedná se o princip, která se zabývá schopností rekonstrukce kompletní historie chování jednotlivých prvků v systému i akcích prováděných na něm. Tento bod je velice důležitý při rekonstrukcích situace selhání systému a analýzy možných důvodů k selhání, poruše či bezpečnostním incidentům [68]. Auditovatelnost bez důvěryhodné identifikace slouží pouze k diagnostickým účelům [69]. Pokud však vyžadujeme, aby bylo možné v systému nastavit i jasnou zodpovědnost za jednotlivé akce, je v rámci sítě důvěryhodně identifikovat jednotlivé účastníky [70].
- **Ochrana vůči třetím stranám**, jedná se o ochranu zařízení, systému či infrastruktury vůči třetím stranám, tj. lidem, zařízením, softwaru, aj. Jedná se například o techniky zabraňující zneužití komunikačních kanálů k DoS útokům, injektování nežádoucího softwaru v podobě malware aj. Třetí strany by tedy neměli být schopny využít slabost systému ve svůj prospěch či k poškození daného systému. Pro zajištění tohoto principu se asi nejvíce používá kombinace autentizace a autorizace [71].
- **Odolnost či tzv. resilience**, jedná se o odolnost systému či infrastruktury, kdy útočník i přes napadnutí jednoho či více zařízení není schopen ovládnout či poškodit další části systému. Dále pak i přes napadnutí a selhání bezpečnostních mechanik musí být jasně stanovena bezpečnostní politika a plán, jakým způsobem bude jednáno pro zajištění maximální ochrany systému a odvrácení následků nežádoucího chování. Tento princip je zajištěn jasně definovanou bezpečnostní politikou, managementem a krizovým plánem [72].
- **Tolerance poruchy**, kde jednotlivé výpadky zařízení, částí systému, poruchy a další anomálie jsou běžnou součástí každého reálného systému. Útočník by v tomto případě neměl být schopen zneužít anomálií a výpadků jednotlivých částí systému ve svůj prospěch, k získání osobních výhod či ke zneužití k poškození systému. Zajištění tohoto principů závisí na nezávislosti jednotlivých bezpečnostních mechanizmů ať už na softwaru, hardwaru či dalších prvcích celého řetězce [73].
- **Samoléčení**, jedná se o schopnost zařízení nebo systému, který je schopen indikovat jeho nesprávný (chybný) chod a bez lidského zásahu následně provést nezbytné kroky k obnovení normálního provozu. Tyto situace mohou být např. výpadek komunikačního spojení, výpadek elektrického napájení aj., a i v těchto situacích

by systém měl být schopen se vrátit do normálního provozu a začít pracovat tam, kde přestal. Potenciální útočník tak nemá možnost tyto stavy jakkoliv využít [74]. Obecně sítě, které mají integrované prvky samoléčby vykazují mnohem větší odolnost např. i proti DoS útokům [75].

- **Ostatní**, jedná se například ještě o následující principy [76, 77, 78]: (i) důvěryhodnost bezpečnostního systému zajištěnou certifikací, (ii) životnost systému, tedy aby se jednotlivé bezpečnostní mechanismy nestali nebezpečné v průběhu životnosti systému, (iii) interoperabilita bezpečnostních mechanik s různým hardwarem či softwarem, (iv) modulárnost systému, tak aby bylo možné jednotlivé části a bezpečnostní mechanismy měnit dle potřeb, a další.

Jak můžeme vidět, mnoho principů se v tomto případě prolíná. Informační bezpečnost na druhé straně pak definujeme z pohledu ochrany informací ve všech jejich formách a to po jejich celý životní cyklus (vznik, zpracování, přenos, ukládání i likvidace). Jedná se o již velice konkrétní pohled na bezpečnost, do kterého spadají následující bezpečnostní principy:

- **Důvěrnost**, tedy zajištění, aby neautorizovaná osoba nebyla schopna získat důvěrné informace z přenášených dat, zařízení či jinak. Tedy tomuto procesu by měla předcházet autorizace (např. autorizace komunikujících stran), což je možné v rámci důvěrnosti zajistit mnoha způsoby, např. poskytnutí práv k úložišti, poskytnutí určitého "tajemství" (např. heslo, klíč, token, aj.) [79]. Informace by tedy neměly být žádným jiným způsobem získatelné. Jedním z velice častých způsobů zajištění důvěrnosti v rámci komunikace je pak tzv. šifrování [80]. Tedy proces, kdy převádíme čitelnou zprávu neboli prostý text na její nečitelnou podobu neboli šifrovaný text. Tento proces je pak zajišťován pomocí tzv. kryptografických algoritmů [81].
- **Integrita dat**, tedy zajištění celistvosti zprávy a ochranu proti neautorizovanému nepozorovanému pozměnění dat třetí osobou, zařízením či systémem. Jedná se např. o zprávy a data obsahující řídící příkazy, hodnoty senzorů, aj. Porušením integrity zpráv mohou následně vznikat bezpečnostní incidenty, které ohrožují nejen konkrétní osoby, ale i firmy či celé státy (příkladem globálnějšího ohrožení může být pozměnění řídících příkazů pro elektrárnu, kdy následně dojde k výpadku dodávky elektrické energie) [82]. Nejčastějším nástrojem pro zajištění integrity jsou pak např. kontrolní součty, různé matematické (hešovací) funkce, specifické módy šifrovacích algoritmů, aj. [83].
- **Autentizace**, tedy ověření proklamované identity jednotlivých účastníků a prvků v síti i samotných dat (jednoznačná identifikace); poskytování autentizace odesílatele, ale i samotného spojení, tak aby nebylo možné např. falšovat, duplikovat

či podvrhovat zprávy. V rámci informační bezpečnosti je autentizace mnohdy společně i s integritou zajišťována simultánně s důvěrností, např. pomocí tzv. autentizovaného šifrování (AE, z angl. Authenticated Encryption) [84]. Zajištění autentizace pak probíhá pomocí např. tzv. autentizačních kódů (MAC, z angl. Message Authentication Code), specifických módů symetrických šifer, aj. [85]. Autentizace je nutnou podmínkou pro správný proces autorizace [86].

- **Čerstvost dat**, zjednodušeně se jedná o tzv. neopakovatelnost starých zpráv. Jelikož samotná komunikace v inteligentních sítích probíhá v různých časových úsecích a nemusí probíhat kontinuálně, je nutno také zaručit, že zasílaná data jsou čerstvá. To znamená, že data jsou aktuální a žádný útočník nemá možnost přenášené zprávy (data) nahrát a znovu přehrát. Rozlišujeme dva základní způsoby zajištění čerstvosti dat: (i) slabou, která umožňuje pouze částečné řazení zpráv, ale poskytuje žádné další aditivní informace pro kontrolu jako např. velikost zpoždění, aj.; a (ii) silnou, která poskytuje komplexní systém řazení zpráv, odhad zpoždění a další aditivní informace pro celkový přehled. Slabá čerstvost je vyžadována převážně v rámci senzorů a měřících zařízení a silná pak např. pro časovou synchronizaci v sítích. Jak již bylo uvedeno, její zajišťování probíhá právě na základě různých identifikátorů zpráv, časových razítek apod. [87].
- **Nepopiratelnost**, prvky v síti nejsou schopny popřít přijetí ani doručení zprávy. Obecně se jedná tedy o nevyvratitelný důkaz, že konkrétní entita v síti provedla určitou konkrétní akci v daném systému (důkaz musí být poskytnut a to i když samotná ověřovaná entita nespolupracuje). Jedná se o službu, která napomáhá mj. i pro jasné stanovení odpovědnosti a spolehlivosti. V rámci informační bezpečnosti je pak možné nepopiratelnost zajistit jednoduše pomocí autentizace a integrity či pomocí digitálního certifikátu (digitálního podpisu) [88]. Nepopiratelnost nemusí být vždy zajišťována společně s důvěrností [89].

Toto jsou tedy dnešní základní principy pro zajišťování bezpečnosti v rámci informačních systémů, tedy mj. i inteligentních sítí. Pokud se zaměříme pouze na informační bezpečnost, která má pět základních bezpečnostních principů: (i) důvěrnost, (ii) integritu, (iii) autenticitu, (iv) nepopiratelnost a (v) čerstvost dat. Nástroje, sloužící pro jejich naplnění, pojmenujeme jako kryptografické algoritmy. Ty jsou pak stavebním kamenem pro větší celek, tvořen tedy mj. kryptografickými algoritmy, které budeme nazývat analogicky jako tzv. kryptosystém. Návrhem a konstrukcí kryptosystémů se pak zabývá obor známý jako kryptografie, kde jeho podoborem je lehká kryptografie zaměřující se na efektivní algoritmy pro výkonnostně i energeticky limitovaná zařízení. Naopak obor, který se zabývá narušením, obcházením či prolomením těchto kryptosystémů, se jmenuje kryptoanalýza. Pro úplnost, obor zahrnující

kryptografii i kryptoanalýzu se jmenuje kryptologie, která se tedy zabývá studií kryptografických algoritmů. Oblast této práce tedy můžeme definovat v oboru lehké kryptografie, kdy práce bude cílit na výzkumu efektivních kryptografických algoritmů - kryptosystému, který pomůže řešit oblast informační bezpečnosti naplněním definovaných bezpečnostních principů ve specifické přístupové části inteligentních sítí, tedy tam kde je využíváno mj. i zařízení s limitovaným výkonem či přístupem k dodávce elektrické energie.

## 1.3 Motivace práce

Hlavní motivace práce vychází z náplně národního projektu TA02020856, ve kterém byl autor práce od roku 2013 na pozici člena výzkumného týmu. Projekt byl podpořen Technologickou agenturou České Republiky a zabýval se aplikačním výzkumem inteligentních systémů pro sledování energetických sítí. V rámci tohoto projektu byla mj. vyvíjena i nízkoenergetická komunikační jednotka osazená mikrokontrolérem s limitovaným výkonem, kde jedním z cílů projektu bylo provést výzkum v oblasti efektivních kryptografických algoritmů a primitiv s následným využitím pro zabezpečení reálné komunikace v inteligentních sítích v energetice. Projekt a výzkum byl tedy prvotně motivován převážně nedostatky v rámci aplikační sféry a aktuální potřebou samotného trhu. Tento projekt skončil v roce 2015, kdy další motivací pro pokračování ve výzkumu byly chystané legislativní změny, nově definované problémy i vědecké výzvy v oblasti nízkoenergetických a výkonově limitovaných zařízení, ale i aditivní potřeby inteligentních sítí či zcela nové komunikační technologie. V této kapitole je dále rozebrána motivace z pohledu současného stavu bezpečnosti inteligentních sítí (viz kapitola 1.3.1), následně jsou uvedeny nové a chystané legislativní změny týkající se bezpečnosti v inteligentních sítích (viz kapitola 1.3.2), a v neposlední řadě jsou uvedeny standardizace a doporučení pro inteligentní sítě (viz kapitola 1.3.3).

### 1.3.1 Současný stav bezpečnosti inteligentních sítí

Inteligentní sítě se postupně rozvíjeli během několika posledních dekád. Přelom 20. a 21. století pak byl, díky velkým technologickým změnám, novému pojetí internetu věcí a dalším pokrokům v mnoha oblastech, začátkem dnešních inteligentních sítí. Velký rozmach těchto oblastí byl v letech 2003–2005 a již v této době byla definována celá řada vědeckých výzev. V roce 2003 byl vydán článek [90], který shrnoval oblasti bezpečnosti a soukromí v inteligentních sítích. Autoři mj. definují celou řadu bezpečnostních rizik a výzev inteligentních sítí, s kterými je nutné do budoucna při vývoji technologií v těchto oblastech počítat, mj. se jedná např. o problematiku kompromitování jednotlivých senzorů (autentizace), ochrana citlivých a soukromých dat

(důvěrnost, soukromí), útoky na parametry dostupnosti a spolehlivosti (dostupnost), zanášení škodlivého softwaru do infrastruktury, a další. V roce 2009 pak v článku [91] autoři přistupují již k samotným výzvám v oblasti bezpečnosti a soukromí pro inteligentní sítě. Autoři přidělují nejvyšší význam ochrany soukromí v rámci těchto typů sítí a také kompromitaci jednotlivých senzorů s následným zneužitím pro nabourání se do celé infrastruktury s odkázáním na mezistátní konflikty a terorismus. Autoři dále mj. přikládají i velký význam oblasti laboratorního výzkumu a vývoji v oblasti bezpečnosti inteligentních sítí i následného plánování pro případ selhání zmíněných systémů. Od roku 2010 pak v rámci historie inteligentních sítí i internetu věcí započal ve výzkumu opravdu velký rozmach v oblasti bezpečnosti. V roce 2010 autoři článku [92] definují oproti předchozím letům další oblasti v rámci bezpečnosti (i) důvěrnost, autenticity, autorizaci a integritu, (ii) bezpečnost zařízení a komunikace z pohledu případného ovládnutí či kompromitace, (iii) soukromí citlivých a kritických dat, a (iv) bezpečnostní management vzhledem ke komplexitě a škálovatelnosti uvažovaných sítí. Článek [93], vydaný v roce 2011, pak spíše jen již obecně popisuje nastalé rizika a výzvy. V článku jsou mj. zmíněny rizika komunikačních technologií a metodika při výběru technologických řešení v rámci inteligentních sítí. Metodiky je však velice obecná a z pohledu bezpečnosti neurčuje, co vše je nutno splnit proto, aby výsledný systém byl opravdu bezpečný. Zde můžeme vidět i známku toho, jakým způsobem se následně jednotlivé směry bezpečnosti oddělili na procesní a informační, jak se z nich postupně stávaly samostatné oblasti. V roce 2013 pak článek [94] shrnuje motivaci, potřeby a jednotlivé výzvy v budování inteligentních sítí. Pokud se blíže podíváme na definované výzvy, dostaneme opět velice podobné výzvy předchozím: (i) komplexita sítí a velké množství objektů, (ii) efektivita, (iii) spolehlivost, (iv) bezpečnost (již rozdělená na informační bezpečnost a vládní regulace). Z pohledu bezpečnosti jsou tu dále zmíněny také výzvy z pohledu možných vnějších hrozeb, zranitelností sítí a soukromí. Další analýza v témž roce byla provedena v článku [95]. Článek se soustředí na dosavadní stav bezpečnosti a aktuální výzvy pro inteligentní sítě. Článek definuje nejprve základní požadavky na bezpečnost pomocí CIA trojice s následným doplněním o monitoringu a odolnosti sítě, autorizaci s řízením přístupu, bezpečných a efektivních protokolů pro komunikaci. Následně jsou definovány základní známé zranitelnosti např. útoky DoS, útoky na integritu a důvěrnost, aj. Vědecké výzvy jsou zde definovány ve čtyřech základních kamenech: (i) Definice potřeb, (ii) Definice potenciální hrozby, (iii) Prevence a obrana proti těmto útokům, a (iv) výzkum a vývoj vhodných řešení. V roce 2014 byl vydán velice podobný článek [96] opět zabývající se shrnutím problematiky a definováním výzev. Bezpečnost je tu definována hlavně z pohledu informační bezpečnosti a to na základě důvěrnosti, integrity, dostupnosti, autenticity, autorizace a nepopiratelnosti. Následně jsou tu definovány možné útoky na infrastrukturu a diskutovány jejich potenciální dopady z pohledu "malých" až

"velkých" dopadů. Ve většině definovaných scénářů jsou napadány převážně: důvěrnost, integrita či autenticita. Hlavní výzvy jsou pak definovány na dvou úrovních, (i) regulační - standardizace, určení zodpovědnosti, nové metriky pro hodnocení bezpečnosti, dopady na legislativu v návaznosti na inteligentní sítě; a (ii) technické - nové agregační algoritmy, nové autentizační či autorizační schémata či např. klíčový management pro kryptografické algoritmy. V roce 2015 bylo následně vydáno další shrnutí pro bezpečnost v rámci inteligentních sítí, kde autoři v článku [97] se zabývají převážně bezdrátovými technologiemi používanými v dané oblasti. Kromě definice základních technologií a technik, jsou následně definovány i obecné výzvy. Autoři v tomto případě uvádějí jako hlavní výzvy: velkou komplexitu, dostatečnou efektivitu, konzistentnost sítě, bezpečnost sítě, chybějící standardizace, nedostatečná škálovatelnost, malá interoperabilita či nedostatečné mechanismy pro samoléčbu sítě. Tyto výzvy jsou definovány na velmi abstraktní a obecné úrovni. V rámci roku 2016, pak další studie navazují na praxi předchozích let a opět je vydávána celá řada nových studií a shrnutí. Zmínit můžeme např. práce [98, 99, 100]. Autoři v článku [98] již velice konkrétně shrnují jednotlivé výzvy na několika úrovních: (i) analýza dat, (ii) problematika velkého množství dat a jejich zpracování, (iii) výpočetní náročnost na straně serveru (cloudu), a (iv) internet věcí. V těchto oblastech je mj. definována jako velmi důležitý aspekt bezpečnost a soukromí uživatelů. Práce [99] se pak věnuje inteligentním sítím a měření, kde jsou definovány jednotlivá specifika této oblasti, popsány jednotlivé komunikační technologie a jejich vlastnosti, výhody i nevýhody, společně se shrnutím možných hrozeb a definicí potřeb pro bezpečnost, kde jedním z nejdůležitějších prvků je zmiňován klíčový management pro kryptografické algoritmy, sledování standardů, fyzická bezpečnost zařízení, ochrany proti DoS útokům, a mj. také zaručení integrity, důvěrnosti, autenticity, autorizace, či neopakovatelnost zpráv, aj. V neposlední řadě práce [100] popisuje hlavní kritická témata pro inteligentní sítě a jejich technologie. Ty jsou rozděleny na tři základní: (i) komunikace, (ii) sběr a ukládání dat, a (iii) technologie a zařízení. Již v úvodu autoři poukazují na nedostatky jednotlivých technologií v rámci inteligentních sítí a jejich možné dopady v blízké budoucnosti po jejich nasazení do globální sítě či infrastruktury. V rámci komunikace je pak definována informační bezpečnost jako jeden ze základních prvků a předpokladů pro inteligentní sítě i jako hlavní vědecká výzva této oblasti. Z pohledu informační bezpečnost se tedy jednotlivé výzvy spíše více specifikují a vznikají nové a nové výzvy společně s dalšími více sofistikovanějšími útoky. Uveďme si pro úplnost shrnutí v podobě návaznosti jednotlivých uvedených výzev definovaných ve vědecké literatuře vůči námi definovaným principům informační bezpečnosti (viz Tab. 1.2).

Tab. 1.2: Shrnutí hlavních vědeckých výzev v rámci inteligentních sítí.

| Rok | Návaznost na definované principy informační bezpečnosti | Zdroj |
|---|---|---|
| 2003 | Článek vyzdvihuj problémy související s kompromitací senzorů ve smyslu **autentizace** a nedostatky při případném odcizení dat ve smyslu **důvěrnosti**. | [90] |
| 2009 | Z pohledu informační bezpečnosti je definována jako největší výzva bezpečná komunikace limitovaných zařízení a zajištění principu **důvěrnosti**. | [91] |
| 2010 | Výzvy na úrovni informační bezpečnosti jsou zde definovány převážně k **důvěrnosti** ve smyslu ochrany soukromí a citlivých dat. | [92] |
| 2011 | Nejdůležitější výzvou je definováno zajištění **důvěrnosti** a ochrany citlivých dat i nutnost bezpečné **autentizace** zařízení. Dále je zde zmíněna netriviálnost a náročnost případné tříparametrické optimalizace, tedy optimalizace ceny-výkonu-bezpečnosti. | [93] |
| 2013 | Hlavními diskutovanými body jsou velké množství zařízení. Z tohoto pohledu pak velmi obtížná ochrana dat i komunikace z pohledu **důvěrnosti** a vytvoření silné **autentizace**. | [94] |
| 2013 | Definice hlavních nedostatků stávajícího zabezpeční na principech zabezpečení v rámci CIA (**důvěrnost**, **integrita**, **autentizace**) a aditivních procesních principech. Dále také nutnost přemýšlet o poměru efektivity a ceny zabezpečení a najít optimální řešení. | [95] |
| 2014 | Definice bezpečné inteligentní sítě na úrovni **důvěrnosti**, **integrity**, **autentizace** a **nepopiratelnosti**, kdy většinu autory definovaných bezpečnostních incidentů lze řešit pouze principy CIA (a aditivními procesními principy). | [96] |
| 2015 | Hlavní výzvy jsou definovány v kontextu velkého množství zařízení s limitovaným výkonem v rámci telemetrických systémů. Jako obtížné je zde definováno zajištění **důvěrnosti** a **autentizace**. | [97] |
| 2016 | Hlavní výzvou v oblasti telemetrických systémů je označeno zajištění **důvěrnost** pro citlivá data u velkého počtu měřících zařízení, a také vytvoření **autentizačních** mechanismů pro následné zajištění autorizace. | [98] |
| 2016 | Jako nejdůležitější pro informační bezpečnosti v rámci inteligentních sítí je zde analyzováno zajištění **integrity**, **důvěrnosti** a **autentizace** pro velké množství komunikujících bodů. Jako první však musí být zavedeny efektivní opatření v rámci procesní bezpečnosti. | [99] |
| 2016 | V tomto článku autoři definují pro komunikaci a informace bezpečnostní incidenty převážně se dotýkající **autentizace** a **důvěrnosti**. Autoři dále zmiňují nutnost posuzovat jednotlivé komunikační technologie, jelikož sami o sobě přináší do inteligentních sítí své specifické bezpečnostní výzvy, problémy a zranitelnosti. | [100] |

Většina definovaných výzev v rámci inteligentních sítí je na úrovni procesní bezpečnosti, tedy zajištění autorizovaného přístupu, ochrany infrastruktury vůči útokům na dostupnost, ochrana jejích prvků vůči třetím stranám, a další. Výzvy v informační bezpečnosti jsou pak definovány téměř vždy na úrovni telemetrických systémů využívaných inteligentními sítěmi k získávání dat a na úrovni senzorických sítí, které jsou tedy využívány k získávání dat a jejich přenosu do data koncentrátorů v rámci přístupové části telemetrických systémů. Velkým tématem je nasazení velkého počtu senzorů, měřících zařízení a dalších prvků do infrastruktury inteligentních sítí, kdy je nutno zajistit pro všechny tyto jednotlivé prvky bezpečnostní principy CIA a následně i další aditivní principy ať už z informační či procesní bezpečnosti. Motivací této práce je tedy řešit definované výzvy a vytvořit řešení, které bude moci být integrováno i do zařízení s limitovaným výkonem a poskytnout dostatečnou

úroveň zabezpečení, tak aby byly naplněny potřebné bezpečnostní principy. Uvažovat zde budeme tedy převážně principy CIA z informační bezpečnosti, s kterými jsou další principy většinou úzce spojeny.

### 1.3.2 Legislativa v oblasti bezpečnosti inteligentních sítí

V rámci legislativních změn v oblasti bezpečnosti digitálního světa, internetu věcí a inteligentních sítí jsou nejaktuálnějšími tématy následující tři změny: (i) Strategický plán Evropské Unie - vize 20 20 20, (ii) Obecné nařízení o ochraně osobních údajů vydané Evropskou Unií, a (iii) Nový kybernetický zákon České Republiky. V této kapitole si popíšeme jednotlivé chystané legislativní změny v souvislosti s inteligentními sítěmi i jejich bezpečností.

#### Strategický plán Evropské Unie - vize 20 20 20

Evropská Unie v roce 2009 vydala strategický plán (Vize 20-20-20) a nařízení, která udává, že do roku 2020 by měl být v členských státech nainstalován, na minimálně 80 procentech odběrných míst, inteligentní elektroměr [101]. Česká Republika se na přechod na inteligentní sítě připravuje pilotními projekty distribučních společností a jejich partnerů [102]. Tradiční elektroměr funguje na principu, kdy jsou průběžná měření spotřeby ukládána do registru, který je jednou ročně odečítán distribuční společností. Není možné kontrolovat průběžnou spotřebu (denní, týdenní) či jakkoliv dynamicky reagovat na konkrétní situaci v distribuční sítí (nabízení jiných tarifů na základě vytížení sítě apod.). Inteligentní elektroměr nabízí mnohé možnosti, jak zefektivnit domácnost a spotřebu či dodávku elektrické energie. Tyto zařízení mají vlastní paměť (např. je každých 15 minut ukládána spotřeba elektrické energie do paměti), která slouží nejen k měření spotřeby elektrické energie, ale jsou do ní také ukládány statistické údaje například mechanické zásahy do elektroměru, vyhodnocení a zaznamenání přepětí, podpětí, odchylky od požadované frekvence a další informace potřebné k vyhodnocení například kvality dodávky elektrické energie.

Inteligentní elektroměry jsou součástí většího celku, tedy inteligentních domácností a inteligentních sítí. Inteligentní domácnosti jsou opatřeny senzory a zařízeními, které jsou schopny automatizovat domácnost a zefektivnit její chod. V návaznosti na inteligentní elektroměry, pak například reagovat na změnu tarifu a automaticky používat domácí spotřebiče, díky čemuž by měla domácnost ušetřit a distribuční síť by se tak měla zbavit špičkových vytížení sítě [103].

Na druhé straně jsou pak elektroměry spojeny s inteligentními sítěmi, pomocí nichž regulujeme spotřebu elektrické energie v reálném čase. Jejíž největší výhodou oproti stávajícímu hromadnému dálkovému ovládání (HDO), je interaktivní obousměrná komunikace. Díky obousměrné interaktivní komunikaci jsme schopni na základě

získávaných dat v reálném čase reagovat na zvýšenou potřebu elektrické energie v distribuční síti nebo naopak na sníženou potřebu, zákazníci jsou schopni reagovat na různé ceny elektrické energie (založené například na zatížení sítě) a tak regulovat svou spotřebu elektrické energie a rovnoměrněji ji rozkládat do dne, jsme schopni také automaticky obnovovat výpadky v distribuční síti aj. [104].

V České Republice se v rámci inteligentních sítí rozrůstají oblasti, kde jsou tyto technologie testovány například oblast Vrchlabí, kde působí společnost ČEZ [105], ale i další společnosti jako například EON [106], Landys+Gyr [107] a další se věnují v České Republice oblasti inteligentních sítí, jejichž hlavními body pak jsou například naplnění požadavků evropské unie, nahrazení neinteligentního HDO, informovanost obyvatel o inteligentních sítích a jejích možnostech, aj. Průkazný rostoucí zájem o inteligentní sítě nejen v České republice, ale i v zahraničí je jedním z dalších bodů motivace této práce, který mj. také potvrzuje potřebnost řešení. Navíc tlak na cenu roste s blížícím se možným nasazením většího počtu elektroměrů, což má za následek i snižování výkonů, paměť a dalších komponent, což následně z elektroměrů tvoří limitované zařízení.

### Obecné nařízení o ochraně osobních údajů

Obecné nařízení o ochraně osobních údajů (GDRP, z angl. General Data Protection Regulation), je nařízení Evropské Unie pod označením EP 2016/679 [108], které bylo přijato v dubnu 2016 a má nabýt účinnosti již 25. května 2018. Toto nařízení upravuje vztahy mezi uživateli a poskytovaly v rámci osobních údajů, nastavuje například i novou formu souhlasu ke zpracování osobních údajů, rozšiřuje či upřesňuje definici osobních údajů, zadává nutné i nové kroky k jejich ochraně, aj. Pokud by se dotyčné subjekty nepřizpůsobily novým pravidlům zpracování dat, hrozí jim pokuty až do výše 20 milionů Euro nebo do výše 4 % jejich ročního obratu.

GDPR je tedy nový právní rámec sloužící k ochraně osobních údajů v evropské unii, kde cílem je chránit práva občanů (uživatelů) proti neoprávněnému zacházení s jejich daty a osobními údaji. Toto nařízení se týká všech firem, institucí, jednotlivců, poskytovatelů služeb, a dalších, kteří zpracovávají osobní, citlivá či jiná data spojená s konkrétní fyzickou. Zpracováním je v tomto smyslu jakákoliv operace (i automatická) týkající se zmíněných dat, např. jejich shromažďování, ukládání, nahrávání, přizpůsobení, změna, vyhledávání, používání, šíření a další. V rámci Evropy se jedná o historicky největší sjednocení a nejglobálnější účinek ve vztahu k osobním datům, týká se všech členských států EU a navíc i Islandu, Norska a Lichtenštejnska.

Nařízení GDPR není revolucí a nepřináší tedy zcela nové definice, jak by se mohlo zdát, pouze adaptuje a zpřesňuje již známé pojmy pro dnešní digitální svět a reaguje tak na nové formy i typy údajů a dat. Díky zpřesnění osobních údajů, citlivých údajů,

a dalších došlo ke změnám i částečně v oblasti inteligentních sítí. Jakákoliv data, která jsou získávána a je možné z nich vytvořit osobní profil chování, získat osobní či citlivé data musí být podrobena souhlasem a navíc chráněna v celém jejich životním cyklu. V tomto případě se může jednat například o údaje o elektrické spotřebě. Nepouštějme se v tomto případě do kontroverzní diskuze nad vlastníkem těchto dat, což ostatně ani GDPR neřeší. Posuzujme zde však informaci, která může vést ke snadnému profilování chování spojené s konkrétní fyzickou osobou nebo skupinou osob - tedy samotnou informaci o spotřebě v čase. V tomto případě GDPR hovoří jasně a je nutno tuto informaci chránit, tak aby nedošlo k jejímu zneužití. Zabezpečení v tomto případě může mít dle GDPR různou formu, kde jednou z adekvátních technik je považováno i zabezpečení pomocí šifrování (článek 34).

Z tohoto pohledu je tedy další motivací této práce i rozšiřující se zájem o ochranu citlivých dat i ochrana digitální identity. Senzory i měřící zařízení v rámci inteligentních sítí budou čím dál více zasahovat do našeho každodenního života a je nutno, aby jimi získávaná data nebylo možné zneužít. Zabezpečená komunikace je tak v tomto případě základem k bezpečnému získávání dat.

### Nový kybernetický zákon České Republiky

V roce 2014, konkrétně 29. srpna 2014, vešel v České Republice v platnost dlouho připravovaný zákon o kybernetické bezpečnosti (ZKB) č. 181/2014 Sb. [109] Se zákonem následně ještě velice úzce souvisejí vyhláška č. 316/2014 Sb, (vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti - vyhláška o kybernetické bezpečnosti) [110]; Vyhláška č. 317/2014 Sb. (vyhláška o významných informačních systémech a jejich určujících kritériích) [111]; a nařízení vlády č. 315/2014 Sb. (nařízení o kritériích pro určení prvků kritické infrastruktury) [112]. Zákon je účinný od 1. 1. 2015. Cílem zákona bylo a je zvýšit bezpečnost kybernetického prostoru a ochrana kritické infrastruktury (tedy ta část infrastruktury, při jejíž narušení dojde k přímému či nepřímému ohrožení zájmů České Republiky). Další novela tohoto zákona [113] pak přišla jako reakce na evropskou směrnici EU 2016/1148 ze dne 6. 7. 2016 [114], kdy došlo ke zpřesnění některých pojmů.

Definice kritické infrastruktury však není definitivní a s časem se rozšiřuje, což je to dáno jednak trendem propojování jednotlivých částí do globální struktury, ale i novými typy hrozeb. Již dnes je část inteligentních sítí považována za kritickou infrastrukturu a lze předpokládat, že čím dál větší část inteligentních sítí bude v budoucnu zahrnuta pod kritickou infrastrukturu [115]. Samotný zákon řeší většinou procesní otázku bezpečnosti, nicméně ukládá také minimální požadavky na inteligentní sítě, jejich bezpečnost a zavádění tzv. bezpečnostních opatřeních. Kategorie

kryptografických prostředků je podrobněji upravena v rámci přílohy ust. § 5 odst. 3 písm. j) zákona č. 181/2014 Sb. a technický standard pro kryptografické prostředky je pak podrobněji upraven v příloze č. 3 vyhlášky č. 316/2014 sb. Zákon tak zavádí pouze minimální obecně definované požadavky a ponechává stále volnost ve volbě konkrétních technických nástrojů pro účely zajištění bezpečnosti.

Vzniklé nové požadavky na inteligentní sítě a jejich prvky, tedy i ty s limitovaným výkonem, jsou další motivací této práce. Výsledné uvažované řešení pro efektivní a bezpečnou komunikaci ve využívaných telemetrických systémech by tedy mělo splňovat alespoň minimální požadavky stanovené zákonem o kybernetické bezpečnosti i další s ním spojené legislativní doplnění.

### 1.3.3 Bezpečnostní standardy, normy a doporučení

Velkým problémem v oblasti informačních sítí i velice kontroverzním tématem jsou bezpečnostní standardizace, doporučení a normy. Jejich nejednotnost a i velký počet pak tvoří nelehký úkol při jejich výběru. Například samotná evropská agentura pro síťovou a informační bezpečnost ENISA (z angl. European Network and Information Security Agency) vydala již v roce 2012 seznam více než 20 standardů, doporučení a regulačních dokumentů (společně s více než 250 zdroji dokumentů) týkajících se přímo či nepřímo oblasti bezpečnosti inteligentních sítí [116]. V květnu 2013 pak byl uveřejněn další dokument konzultační firmou XANTHUS shrnující jednotlivé skupiny standardů a doporučení souvisejících s inteligentními sítěmi [117]. V dokumentu můžeme nalézt více než 80 standardů dotýkající se tématiky bezpečnosti inteligentních sítí, každý pak navíc obsahuje další jednotky či desítky aditivních dokumentů. Tyto standardy se však zabývají převážně procesní bezpečností a neřeší již konkrétní doporučení pro zajištění informační bezpečnosti.

V rámci informační bezpečnosti pak v dnešní době existuje pouze několik validních dokumentů, které doporučují konkrétní nástroje pro řešení informační bezpečnosti. V rámci ČR to může být právě nový kybernetický zákon (viz kapitola 1.3.2) a dále také např. česká verze evropské normy ČSN EN 62351-3 [118], která mj. diskutuje již konkrétně parametry bezpečnostních nástrojů. V zahraničí pak můžeme vycházet z doporučení BSI TR-02102-1 vydaného v roce 2017 Německým spolkovým úřadem pro bezpečnost v oblasti informačních technologií BSI (z něm. Bundesamt für Sicherheit in der Informationstechnik) [119] či doporučení "Référentiel Général de Sécurité " (Apendix B1) aktuální k roku 2014 a vydané v roce 2010 Francouzskou národní agenturou pro informační bezpečnost ANSSI (z franc. Agence nationale de la sécurité des systèmes d'information) [120]. Oba tyto dokumenty řeší konkrétní parametry a bezpečnostní nástroje pro informační bezpečnost. Pro Evropu pak můžeme vycházet z doporučení od ENISA, která vydala v roce 2014 dokument s doporučeními

a výzvami pro bezpečnost v inteligentních sítích, která mj. řeší přesná doporučení pro bezpečnostní nástroje využívané v inteligentních sítích [121]. V rámci mezinárodních norem je pak ještě možné zmínit uznávané úřady tj. Americkou národní bezpečnostní agenturu NSA (z angl. National Security Agency) a Americký národní institut standardizace a technologií NIST (z angl. National Institute of Standards and Technology), kde NSA vydala v roce 2016 dokument určující směr národní bezpečnosti, řešící mj. právě i konkrétní doporučení pro využívání bezpečnostních nástrojů [122] či NIST, který v roce 2014 [123] vydává doporučení pro bezpečnostní nástroje a jejich parametry pro informační systémy.

Dnes existuje nepřeberné množství různých doporučení, standardů či norem. V rámci této práce se však nebudeme soustředit na procesní bezpečnost, nýbrž pouze informační bezpečnost. V této oblasti pak existuje pouze několik relevantních a uznávaných zdrojů. Za ty budeme považovat právě zmíněné zdroje ČSN, BSI, ANSSI, ENISA, NSA a NIST. Motivace práce je převážně v zajištění bezpečného řešení pro inteligentní sítě. Z tohoto pohledu je tedy vhodné, aby takového řešení, sledovalo nejnovější relevantní standardy a doporučení, čímž následně poskytne komplexní ochranu v současnosti i budoucnosti.

# 2 CÍLE DIZERTACE A METODIKA

Informační bezpečnost je v rámci inteligentních síti velmi aktuálním tématem. Mnoho specializovaných odborných organizací, vlád států aj. tvoří doporučení a legislativní změny pro vytvoření bezpečného prostředí při budování těchto sítí. Nicméně stanovené požadavky v těchto doporučeních či nařízeních mnohdy neberou v potaz limitované zdroje koncových zařízení - senzorů. Ty nejsou mnohdy již z principu schopny pracovat s robustními a výkonově náročnými algoritmy. Z výzkumného hlediska tak vzniká netriviální výzva, kdy je nutno najít optimalizované řešení z pohledu výkonnosti, nákladovosti a bezpečnosti. Tuto úlohu dále znesnadňují i další faktory jako např. multi-technologické prostředí inteligentních sítí, různorodost či nejednotnost standardů. Hlavním cílem této práce je tedy vytvořit vlastní hybridní kryptosystém pro zabezpečenou komunikaci v oblasti inteligentních sítích, využívající zařízení s limitovanými zdroji. Zabezpečením se v této souvislosti myslí poskytnutí či naplnění předem definovaných bezpečnostních principů v rámci informační bezpečnosti definovaných v kapitole 1.2. Jako první tedy bude nutné definovat požadované bezpečnostní principy pro vybranou specifickou oblast inteligentních sítí. Principy jsou vybírány v souladu s aktuálním stavem bezpečnosti, přiblíženém již v rámci kapitoly 1.3.1. Jedná se především o principy CIA, tedy důvěrnost, integrita a autentizace. Ostatní principy budou však brány také v potaz, nicméně jejich naplnění probíhá mnohdy souběžně s principy CIA. Dalším aspektem při výběru bude soulad se současnou národní i evropskou legislativou, viz kapitola 1.3.2. V potaz bude brán hlavně nový kybernetický zákon a nařízení GDPR. V neposlední řadě pak bude také brán ohledem na další doporučení, normy i standardizace představené v rámci kapitoly 1.3.3. Stěžejním zde budou standardy a doporučení od uznávaných organizací typu BSI, ANSSI, ENISA, NSA či NIST i uznávaných norem typu ČSN. Jako další krok bude nutno na základě stanovených principů vypracovat analýzu dnešních možností pro zajištění bezpečné komunikace. Výstup této analýzy bude přehled možných nástrojů pro zajištění bezpečné komunikace. Definované principy bezpečnosti i analyzované možnosti pro zajištění bezpečné komunikace budou následně vstupy k analýze využívaných komunikačních technologií v oblasti inteligentních sítí, ze které vyplynou hlavní nedostatky, s kterými se inteligentní sítě v rámci komunikace potýkají. Dále bude nutno provést kvalitativní i kvantitativní srovnání a výběr nejvhodnějších nástrojů pro zajištění definovaných principů a nalezených nedostatků v inteligentních sítích. Výsledné řešení bude nejen splňovat veškeré aktuální požadavky stanovené legislativou či standardizacemi, ale také řešit aktuální nedostatky v rámci inteligentních sítí. Dalším krokem bude algoritmizace vybraných nástrojů, stanovení jejich požadavků pro realizaci a výběr vhodného nízkovýkonového i energeticky efektivního zařízení. Následně bude proveden výzkum a vývoj efektivní

realizace vybraných nástrojů na specifických hardwarových platformách, společně s jejich integrací do jednoho komplexního hybridního kryptosystému, který tedy bude sloužit k zajištění bezpečné komunikace. Realizace musí být provedena efektivně, tj. tak aby bylo možné integrovat i další funkční prvky jako komunikační protokol, funkce pro interakci se senzory aj. V neposlední řadě se práce bude soustředit na výzkum v oblasti optimalizace a ověření dílčích částí zrealizovaného kryptosystému. Jako poslední pak bude provedena diskuze a vyhodnocení dosažených výsledků práce v kontextu současných obdobných řešení. Cíle dizertace tak v návaznosti na výše popsanou metodiku můžeme tedy rozdělit dle následujících bodů:

- *Analýza současného stavu problematiky bezpečnosti inteligentních sítí.*
  - Stanovení základní principů bezpečnosti pro inteligentní sítě.
  - Analýza současných možností pro zabezpečení komunikace senzorových sítí.
  - Analýza využívaných komunikačních technologií, jejich bezpečnost, slabiny a nedostatky.
  - Zhodnocení současného stavu a stanovení požadavků na vlastní hybridní kryptosystém.

- *Návrh hybridního kryptosystému pro efektivní zabezpečení komunikace.*
  - Teoretická a praktická evaluace jednotlivých možností vyplynutých z provedené hloubkové analýzy.
  - Výběr nejvhodnějších nástrojů pro zajištění bezpečné komunikace a naplnění stanovených požadavků.
  - Samotný návrh vlastního hybridního kryptosystému.

- *Vývoj, verifikace a optimalizace navrženého kryptosystému.*
  - Výzkum a vývoj v oblasti efektivní realizace dílčích částí vlastního kryptosystému na specifických hardwarových platformách.
  - Experimentální měření a evaluace vytvořeného systému i jeho dílčích částí.
  - Výzkum v oblasti optimalizace navržených algoritmů a metod vlastního hybridního kryptosystém.

- *Zhodnocení dosažených výsledků a srovnání se současnými dostupnými řešeními.*
  - Analýza obdobných řešení a posouzení vlastního řešení, jeho dílčích části i dosažených výsledků vůči současnému stavu.
  - Finální shrnutí, kritické zhodnocení vlastních výsledků a určení dalšího směru výzkumu.

# 3 ANALÝZA SOUČASNÉHO STAVU PROBLEMATIKY

Tato kapitola se věnuje analýze současného stavu inteligentních sítí, jako první jsou zde rozebrány v kapitole 3.1 současné možnosti pro naplnění definovaných bezpečnostních principů informační bezpečnosti v kapitole 1.2. Kapitola 3.2 se věnuje dnešním využívaným komunikačním technologiím v oblasti inteligentních sítí. Kapitola 3.2 se následně blíže zaměřuje na ty technologie, které jsou využívány pro telemetrické systémy a jejich přístupovou část, z tohoto pohledu jsou zde uvedeny specifika i nedostatky těchto technologií i z pohledu bezpečnosti.

## 3.1 Analýza dnešních kryptografických možností

V rámci kapitoly 1.2 byly definovány základní bezpečnostní principy pro informační bezpečnost: důvěrnost, integrita, autenticita, nepopiratelnost a čerstvost dat. Jejich naplnění tedy probíhá za pomocí kryptografických algoritmů (kryptosystému). Kryptosystém je definován uspořádané $n$-tice:

$$(P, C, K, E, D), \tag{3.1}$$

kde $P$ je otevřený či prostý text (z angl. Plaintext), $C$ je šifrovaný text (z angl. Ciphertext), $K$ je klíčový prostor (z angl. Keyspace). Dále dešifrovací algoritmus $E$ definujeme jako:

$$E = \{E_{K_E} : K_E \in K\}, \tag{3.2}$$

představující soubor šifrovacích funkcí:

$$E_{K_E} : P \to C, \tag{3.3}$$

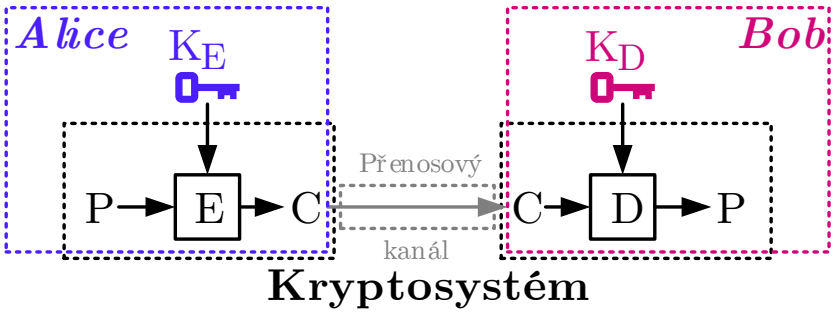
kde $K_E$ je šifrovací klíč. Následně definujeme dešifrovací algoritmus $D$ jako:

$$D = \{D_{K_D} : K_D \in K\}, \tag{3.4}$$

představující soubor dešifrovacích funkcí:

$$D_{K_D} : C \to P, \tag{3.5}$$

kde $K_D$ je dešifrovací klíč. Nyní uvažujme komunikaci mezi dvěma účastníky, které pojmenujeme jako Alice a Bob. Komunikace mezi těmito účastníky využívající námi definovaný kryptosystém pak bude dle Obr. 3.1.




Obr. 3.1: Ukázka definovaného kryptosystému.

V dnešní době jsou kryptosystémy tvořeny většinou třemi základními typy kryptografických algoritmů [124]: (i) kryptografické hašovací funkce, (ii) symetrické algoritmy, a (iii) asymetrické algoritmy. Symetrické algoritmy byly jediné algoritmy, které byly známy do pozdních 70. let 19. století, kdy byly poprvé definovány algoritmy asymetrické [125] a jedny z prvních hašovacích algoritmů [126]. Tab. 3.1 následně shrnuje, jaké jednotlivé bezpečnostní principy tyto funkce mohou zajišťovat.

Tab. 3.1: Zajištění bezpečnostních principů jednotlivými kryptografickými algoritmy.

| **Princip** | **(i)** | **(ii)** | **(iii)** |
|---|---|---|---|
| Důvěrnost | ✗ | ✓ | ✓ |
| Integrita | ✓ | ✓ | ✓ |
| Autenticita | ✗ | ✓ | ✓ |
| Nepopiratelnost | ✗ | ✗ | ✓ |
| Čerstvost | - | - | - |

Čerstvost dat jako jediná není zajištěna přímo pomocí kryptografických algoritmů, ale využívá se tzv. tokenu, což může být identifikátor relace, zprávy, jednorázové heslo, časové razítko aj., které následně mohou být využity společně s kryptografickým algoritmem pro zajištění čerstvosti zprávy [87]. Tato kapitola se dále věnuje nejprve základními prepozicemi a definicemi primitiv využívaných v kryptografii (kapitola 3.1.1). Následně je podstatná část věnována vlastní analýze dnešních možností pro naplnění bezpečnostních principů pomocí definovaných typů kryptografických algoritmů, tj. kryptografické hašovací funkce (kapitola 3.1.2), symetrické algoritmy (kapitola 3.1.3) a asymetrické algoritmy (kapitola 3.1.4).

### 3.1.1 Definice základní primitiv používaných v kryptografii

V rámci této kapitoly budou přiblíženy základní primitiva, která budou dále v této práci používána. Jedná se o [127]: (i) velká čísla, využívána většinou dnešních kryptografických algoritmů k zajištění jejich dostatečné odolnosti vůči kryptoanalýze

a dalším útokům, (ii) algebraické struktury konečných polí a operace modulární algebry, které tvoří základní funkčnost kryptografických algoritmů, a (iii) náhodná čísla, která opět zajišťují ochranu proti útokům a je na nich mj. založena bezpečnost kryptosystémů.

### I. Velká čísla v kryptografii

Jak bylo uvedeno, většina dnešních kryptografických algoritmů využívá velkých čísel o velikosti např. 128 b, 192 b či 256 b a více. Tyto velikosti zpravidla odpovídají velikostem klíčům a dalším parametrům, používaných v dnešních kryptografických algoritmech [76]. S takto velkými čísly však není možné v rámci dnešních výpočetních zařízení pracovat přímo [127]. Je nutno vytvořit speciální reprezentaci těchto čísel, tak aby bylo možné s nimi dále pracovat v navržených kryptografických algoritmech. Jedním z nejpoužívanějších způsobů jak reprezentovat zápis velkých čísel je tzv. poziční číselná soustava [127]. Poziční soustavy jsou charakterizovány svým základem neboli bází. Tato báze bude značena symbolem $b$ (z angl. base či radix). V běžném životě se nejčastěji vyskytuje poziční číselná soustava s bází 10, tj. $b = 10$ (decimální). Například pokud máme číslo $x = 1234$ s bází $b = 10$, tak lze psát:

$$x_{10} = 1234_{10} = 1 \cdot 10^3 + 2 \cdot 10^2 + 3 \cdot 10^1 + 4 \cdot 10^0. \tag{3.6}$$

Podobně je tomu i pro binární soustavu, tj. kde $b = 2$. Pak vyjádření čísla např. $x = 1011_2$ lze psát jako:

$$x_2 = 1011_2 = 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0. \tag{3.7}$$

Pokud zobecníme 3.6 a 3.7, pak pro obecné celé číslo $x \in \mathbb{Z}$ lze psát:

$$x_r = \sum_{i=0}^{n-1} x_i b^i = x_{n-1} b^{n-1} + x_{n-2} b^{n-2} + ... + x_0 b^0, \tag{3.8}$$

kde platí, že $0 \leq x_i \leq b$. Dále zde $b$ značí bázi ($b \in \mathbb{N}$), $x_n$ jsou číslice neboli cifry ($x_n \in 0, 1, \ldots, b-1$) a $n$ je velikostí čísla $x$. Mějme tedy $x$ jako celé velké kladné číslo, tj. $x \ggg 1$. Je tím myšlena skutečnost, že typické velikosti $x$ se pohybují od 128 výše, tedy:

$$x \geq \sum_{i=0}^{n} 2^i = 2^i + 2^{i+1} + \cdots + 2^{n-1}, \tag{3.9}$$

kde $n$ je např. právě 128 b. V rámci výpočetních systému je pak méně efektivní pracovat s reálnými čísly, proto se využívá převážně čísel celých a to hlavně v konečném poli.

## II. Konečná pole a modulární algebra v kryptografii

Celá čísla $\{\ldots, -2, -1, 0, 1, 2, \ldots\}$ jsou pak obecně značena jako množina $\mathbb{Z}$. Mějme konečnou množinu $\mathbb{Z}_m$, kde definujeme $m$ jako celé velké kladné číslo vyjadřující velikost této množiny (platí, že $m \gg 0$). Pak konečná množina $\mathbb{Z}_m$ vznikne z množiny celých čísel $\mathbb{Z}$ tak, že jsou ztotožněna čísla se stejným zbytkem po dělení číslem $m$. Množina $\mathbb{Z}_m$ je tedy definována jako:

$$\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}. \tag{3.10}$$

Mějme tedy celé velké číslo $x \in \mathbb{Z}_m$, kde zbytek po dělení čísla $a$ číslem $m$ (tj. po dělení $x/m$), bude dále v textu značen jako $r = (a \bmod m)$ definovaný jako:

$$(x \bmod m) = x - \left\lfloor \frac{x}{m} \right\rfloor \cdot m, \tag{3.11}$$

kde závorky $\lfloor\rfloor$ označují nejbližší celé číslo menší než podíl $x/m$. Aritmetické operace prováděné na konečné množině $\mathbb{Z}_m$ budou dále označovány jako operace modulární aritmetiky. Příkladem takovéto modulární aritmetiky může být sčítání dvou čísel $x$ a $y$ na množině $\mathbb{Z}_m$, tj. $(x + y) \pmod m$.

Obecně pak můžeme říci, že konečné pole je uzavřená množina čísel, nad kterými jsou definovány algebraické operace. V odborné literatuře je často konečné pole označováno také jako tzv. Galoisové polem GF (z angl. Galois Field). V kryptografii pak jako algebraické operace využíváme sčítání $(+)$ a násobení $(\cdot)$, operace odečítání je pak řešena přičítáním opačného prvku a operace dělení jako násobení inverzního prvku. Pokud uvažujeme konečné pole $\mathbb{F}$ s operacemi sčítání a násobení, pak pro každé pole $(\mathbb{F}, +, \cdot)$, kde $\forall a, b, c \in \mathbb{F}$, platí vztahy definované v Tab. 3.2.

Tab. 3.2: Vztahy pro definované konečné pole.

| **Název** | **Definice** |
|---|---|
| Asociativní zákon | $(a + b) + c = a + (a + b)$ |
| Komutativní zákon | $a + b = b + a$; $a \cdot b = b \cdot a$ |
| Distributivní zákon | $a \cdot (b + c) = a \cdot b + a \cdot c$ |
| Existence opačného prvku | $\forall a \in \mathbb{F}$ existuje $-a$: $a + (-a) = 0$ |
| Existence neutrálního prvku | $a, 0, 1 \in \mathbb{F}$: $a + 0 = a$; $a \cdot 1 = a$ |
| Existence inverzního prvku | $a, a^{-1}, 1 \in \mathbb{F}$: $a \cdot a^{-1} = 1$ |
| Uzavřenost pole vůči sčítání a odčítání | $a + b = c \Rightarrow c \in \mathbb{F}$; $a \cdot b = c \Rightarrow c \in \mathbb{F}$ |

Strukturu dle Tab. 3.2 budeme tedy označovat jako konečné pole $\mathbb{F}$ [128]. Následně můžeme definovat tedy základní algebraické operace jako:

- **Sčítání** $(+)$: Nechť $p$ je prvočíslo definující řád konečné pole $\mathbb{F}_p$. Mějme dvě čísla $a, b \in \mathbb{F}_p$, potom $a + b = c \in \mathbb{F}_p$, kde $c \in \{0, ..., p-1\}$, tuto hodnotu budeme dále označovat jako zbytek $r$. Poté tedy můžeme definovat tzv. sčítání modulo $p$ jako

$a + b \equiv r \pmod{p}$.

- **Násobení** $(\cdot)$: Nechť $\mathbb{F}_p$ o řádu $p$ a dvě čísla $a, b \in \mathbb{F}_p$, potom $a \cdot b = r \in \mathbb{F}_p$, kde $r \in \{0, ..., p-1\}$. Poté tedy můžeme definovat tzv. násobení modulo $p$ jako $a \cdot b \equiv r \pmod{p}$.
- **Odčítání**: Nechť $\mathbb{F}_p$ o řádu $p$ a dvě čísla $a, b, r \in \mathbb{F}_p$. Definujme opačný prvek $-a$ k prvku $a$, pro který platí $a + (-a) = 0$, tedy odčítání dvou prvků zavedeme jako součet $b - a \ = b + (-a)$. Následně můžeme definovat odečítání podobně jako sčítání modulo $p$, tedy jako $b + (-a) \equiv r \pmod{p}$.
- **Dělení**: Nechť $\mathbb{F}_p$ o řádu $p$ a dvě čísla $a, b, r \in \mathbb{F}_p$. Definujme inverzní prvek $a^{-1}$ k prvku $a$, pro který platí $a \cdot a^{-1} = 1$, tedy dělení dvou prvků zavedeme jako násobení $b/a = b \cdot a^{-1}$. Následně můžeme definovat dělení podobně jako násobení modulo $p$, tedy jako $b \cdot a^{-1} \equiv r \pmod{p}$.

### III. Využití náhodných jevů v kryptografii

Obecně se náhodná čísla využívají v kryptografických algoritmech jako vstupní sekvence (z angl. Seed) nebo jako samostatné náhodné parametry vstupující do samotných kryptografických algoritmů. Tedy jak bylo řečeno, i v uvažovaném hybridním modelu je zapotřebí nějakým způsobem generovat náhodná čísla, což je v současné době řešeno náhodnými generátory dat. Základní rozdělení pro generátory náhodných čísel (RNG, z angl. Random Number Generator), z pohledu jakým způsobem čísla generujeme, je: (i) hardwarový generátor (generování je založeno na fyzikálních principech) a (ii) softwarový generátor (generování je založeno na matematických funkcích a výpočtech). Z pohledu náhodnosti generovaných posloupností můžeme ještě najít rozdělení na: (i) skutečně náhodné generátory a (ii) pseudonáhodné generátory. Skutečně náhodné generátory mohou být pouze hardwarové, vykazují skutečnou náhodnost a neperiodičnost v generování posloupností. Pseudonáhodné generátory můžou být softwarové (ty jsou pseudonáhodné vždy, pouze se určuje jak kvalitní či po jak dlouhé době nastává periodičnost) nebo hardwarové (při změně fyzikálních vlastností apod., kdy je například díky této změně způsobena periodičnost generování). Pro jednoduchost budeme uvažovat hardwarové generátory pouze jako skutečně náhodné (TRGN, z angl. True Random Number Generator) a softwarové generátory pouze jako pseudonáhodné generátory (PRGN, z angl. Pseudo-Random Number Generator).

V zařízeních s limitovanými zdroji, můžeme najít oba typy generátoru. Každý z nich má pro limitovaná zařízení jisté výhody a nevýhody:

- **Hardwarové generátory** nezatěžují výpočetní sílu limitovaných zařízení, nicméně jsou pomalejší a můžou tak vytvářet úzká místa či zpožďovat již tak časově náročné kryptografické algoritmy. Řešení popsané např. v [129] se pak zabývá vytvořením hardwarového generátoru náhodných čísel založeném na kruhovém oscilátoru. Tato práce by měla řešit problematiku nestabilních řešeních či řešeních s vyskytujícími se bezpečnostními problémy při generování náhodných čísel při použití kruhového oscilátoru. V této práci však autor uvádí, že je daná problematika vyřešena, nicméně chybí zde průkazné testy náhodnosti či ověření generátoru náhodných čísel obecně. Práce je spíše zaměřena na popis samotné metody či generátoru samotného, než na dokázání vyřešené problematiky, prokázání bezpečnosti a kvality generátoru. Zde tedy chybí kompletně nějaká analýza výsledků či testování vygenerované sekvence, je tedy velice těžké posoudit kvalitu tohoto generátoru. Dalšími řešeními může být například průmyslové řešení Elliptic (CLP-800) [130], toto řešení nabízí inteligentní náhodný generátor jako jedno speciální zařízení, toto zařízení by mělo být vhodné pro bezpečnostní protokoly, síťové infrastruktury i například pro inteligentní sítě. Řešení by mělo být vysoko-rychlostní a založeno na FIPS 140-2 [131] a FIPS 140-3 [132], což jsou mezinárodní standardy. Nevýhoda tohoto řešení je, že bychom museli mít opět komerční speciální zařízení čistě na generování čísel, to je hlavně nevýhoda tam, kde bychom potřebovali větší počet komunikačních jednotek, což je právě příklad odběrných míst, kterých je několik stovek tisíc až miliónů.
- **Softwarové generátory** naopak zatěžují limitované zařízení dalšími výpočty, nicméně pokud máme dostatek výpočetního výkonu, jsou tyto generátory rychlejší než hardwarové (například je limitována pouze velikost paměti, ale výpočetní výkon máme velký). Další možností je pak například využít hardwarový generátor jako zdroj pro pseudo-náhodný generátor. Tímto způsobem jsme schopni zvýšit množství generovaných bitů pseudo-náhodným generátorem a kvalitu samotného pseudo-náhodného generátoru a to hlavně díky stále se měnící sekvenci, kterou užíváme jako zdroj a kterou generujeme pomocí hardwarového generátoru. Pro limitovaná zařízení existuje mnoho softwarových (pseudonáhodných) řešeních. Prvním z nich je například AKARI-X [133] řešení, tedy pseudonáhodný generátor pro tzv. odlehčené systémy (lightweight systems). Tento generátor byl testován na 100 kHz s napájením 1,2 V, byl otestován na standardních testech od NIST [134], DIEARD [135] a byla otestována i entropie tohoto generátoru, nicméně zde chybí údaj o tom, kolik bitů bylo testováno či podrobný popis vstupu do testu. Tato práce se snaží vyřešit nedostatečná řešení pro identifikátory k identifikaci zboží založené na technologii identifikace na rádiové frekvenci (RFID, z angl. Radio Frequency Identification). Na generátory náhodných čísel pro RFID je zaměřeno

mnoho dalších prací [136, 137, 138, 139, 140, 141]. Jedná se o velice zajímavá řešení, kde i při limitovaných zdrojích jsou některé z nich schopny dodávat kvalitní pseudonáhodné sekvence bitů, které vyhovují dnešním testům. Při takto nízkém výkonu se však vždy jedná o kompromis. Tyto generátory jsou velice specificky optimalizovány, kdy se snažíme o kompromis rychlosti generování, náročnosti algoritmu a kvality pseudonáhodné posloupnosti. I když je tato práce spíše zaměřena na inteligentní sítě (s limitovanými zdroji), kde jsme schopni pracovat se zařízeními s vyšší vnitřní frekvencí (řádově MHz), je možné v této oblasti hledat jistou inspiraci pro budoucí postup. Jedno z obecných řešení náhodného generátoru popsané v [142] se soustředí na vytvoření náhodného generátoru kryptografických klíčů. Citovaná práce se zabývá nízko-výkonovým řešením pseudonáhodného generátoru s využitím Park-Millerova algoritmu. V této práci bylo použito čipu o frekvenci 33,3 MHz, generátor je srovnán s podobnými řešeními. Park-Millerův algoritmus zde dosáhl lepších výsledků než generátory s frekvencí několika násobně vyšší. Jeho průměrná spotřeba byla 4,595 mW a jedná se tedy o 32-bitovou architekturu CMOS technologie. Je nutné však poznamenat, že se jedná o řešení čipu, který je specializovaný čistě na generování náhodných čísel a tedy není možné jej využít na žádný jiný proces. Další nedostatek vidím v provedených testech náhodnosti, je využito statistických testů NIST [134], ale není jasné, kolik bitů bylo testováno, či vstup do tohoto testu, potom nelze posoudit kvalitu výsledků. Vhodnější variantou může být pak například řešení s fyzicky neklonovatelných funkcí (PUF, z angl. Physical Unclonable function), jedná se o funkci, která má vlastnost lehkého výpočtu a těžké predikce. Touto problematikou se zaobírají i dnešní aktuální práce například [143]. V této práci je pak velice dobře popsána samotná problematika PUF funkce, kde se tato práce také snaží řešit náchylnost na kryptografické útoky. V práci je řešeno několik problému a ve shrnutí autor uvádí, že některé slabosti PUF funkce se stále nepodařilo vyřešit a jejich řešení stále zůstává otevřené. PUF funkce se jeví jako jedna z vhodných variant pro limitovaná zařízení, pokud by byly odstraněny nedostatky samotné funkce, jednalo by se o kvalitní a rychlý pseudonáhodný generátor čísel. Obecným pseudonáhodným generováním se zabývá mnoho prací a to i pro limitovaná zařízení, ještě pro příklad můžeme uvést [144], kde však chybí větší hloubka testů náhodnosti a kvality generátoru či [145], kde již první výsledky ukázali velké sekvence jedniček či nul při generování binární sekvence. Další možností jsou pak již konkrétní neobecná řešení na jednotlivých zařízeních (např. nízko-výkonových mikrokontrolerech). Práce [146, 147] se již zabývají konkrétními mikrokontrolery (MCU), avšak opět se jedná o návrh samotného generátoru založeném na MCU, tedy výsledkem je opět jedno zařízení, které generuje čísla a k němu je nutné mít další zařízení, které by nám zajišťovalo ostatní kryptografické algoritmy. Poslední práce [148] již pak popisuje konkrétní možnost hardwarové

implementace náhodného generátoru do MCU MSP430, toto řešení však představuje pouhý návrh, bližší měření samotné implementace tohoto řešení však chybí.

Generátory pro RFID jsou v oblasti limitovaných zdrojů využitelné, nicméně se jedná o velice specifické odvětví, kde samotná implementace do jiné situace či problematiky. Práce zabývající se implementaci RFID generátorů do jiných odvětví chybí. Nicméně je nutné poznamenat, že při implementaci takto specifických generátorů může dojít k nepředvídatelným problémům v zabezpečení (vyšší náchylnost například na útok postranními kanály aj. bezpečnostní problémy), navíc například v inteligentních sítích je možné pracovat s mnohem většími frekvencemi. Dalším řešením můžou být obecné pseudo-náhodné generátory, nicméně u nich velice záleží na konkrétní implementaci do vybraného zařízení a také na způsobu optimalizace. Pseudo-náhodné generátory pak představují pro odvětví inteligentních sítí s limitovanými zdroji možnost, nicméně hlubší a jednotné měření těchto generátorů chybí a je tedy velice těžké jejich kvalitativní posouzení. Předposlední možností je vytvořit speciální zařízení, které nám zaštítí funkci náhodného generátoru, tyto generátory jsou výkonné a vykazují jedny z nejlepších vlastností, v přehledu byly představeni někteří zástupci, nicméně problémem u tohoto řešení je, že pro inteligentní sítě konkrétně pro komunikaci pro sítě s milióny uzly není možné zajistit tak velký počet speciálních zařízeních, které řeší jen část problému. Posledním řešením je ukázka řešení na konkrétním MCU, kdy díky vlastnostem a zapojení MCU je možné dosáhnout fyzikálního jevu, který nám vytvoří nezávislý hardwarový generátor náhodných čísel přímo na MCU, tímto způsobem by bylo možné využít samotný MCU ke generování čísel a také pro další kryptografické úkony (například šifrování) a i pro samotnou komunikaci. V tomto odvětví, ale chybí dostatečné množství relevantních prací.

### 3.1.2 Kryptografické hašovací funkce

Hašovací funkce $H$ (z angl. hash function) je taková matematická funkce, která převádí vstup funkce do výstupu o předem definované délky, označovaného jako haš $h$ (z angl. Hash). Uvažujme rovnici 3.3, pak hašovací funkci $H$ můžeme definovat jako:

$$H : P \rightarrow h, \tag{3.12}$$

kdepoté můžeme tedy definovat hašovací funkci $H$ jako funkci:

$$H\left(P\right) = H\left(\left\{0,1\right\}^{l_p}\right) = \left(\left\{0,1\right\}^{l_h} = h, \tag{3.13}$$

kde $H\left(P\right)$ je hašovací funkce, $0, 1$ představuje jednotlivé bity (exponent pak určuje velikost bitového bloku), $P$ je zpráva o bitové velikosti $l_P$, $h$ je výsledný haš o velikosti $l_h$. Hašovací funkce nepoužívají pro svou funkci žádný klíč. Kryptografické hašovací

funkce jsou pak takové funkce, které umožňují jejich nasazení v kryptografických algoritmech pro zajištění informační bezpečnosti a splňuje určité na ní kladené požadavky (nicméně také nepoužívají klíč). V kryptografických hašovacích funkcí musí být deterministická. To znamená, že jakýkoliv otevřený text $P$ o různé velikosti $l_P$ vede vždy ke stejně velkému haši $h$ s předdefinovanou délkou $l_h$. Dále je nutno, aby $H$ byla tzv. jednosměrnou funkcí a nebyla reverzibilní. To znamená, že ze známého haše $h$ a jeho délky $l_h$ je nutné, aby bylo systematicky obtížné (tj. výpočetně i časově velmi náročné) rekonstruovat původní otevřený text $P$. Platit musí také to, že ze známé dvojice $(h, l_h)$ ani není možno odvodit pouze část otevřeného textu $P$ či jeho velikost $l_P$. Toto je rozdíl oproti šifrovací funkci $E$, kdy z jejího výstupu $C$ je následně možné pomocí dešifrovacího klíče $K_D$ odvodit (vypočítat) zpětně otevřený text $P$. Dále platí, že pouhou malou změnou otevřeného textu $P$ (např. změna jednoho bitu) dosáhneme vždy velké změny výstupního haše $h$, tj. výsledný haš se od původního zásadně a na první pohled liší. To také mj. znamená, že je systematicky obtížné najít takovou dvojici $(P_1, P_2)$, pro kterou by platilo:

$$H(P_1) = h_1 = h_2 = H(P_2). \tag{3.14}$$

Nicméně dvojice $(h_1, h_2)$ by si neměla být ani podobná. To znamená, že pokud definujeme podobné obrazy $h_1 \to h_1'$ a $h_2 \to h_2'$, tak musí být systematicky obtížné nalézt i takové dvojice $(P_1, P_2)$, pro které by platilo:

$$(H(P_1) = h_1 = h_2') \vee (H(P_2) = h_2 = h_1') \tag{3.15}$$

Hlavními dnes známými zástupci kryptografických hašovacích funkcí jsou algoritmy: MD5, SHA-1/2/3 a Tiger [127]. Hašovací funkce jsou velice často využívány k hašování hesel u databázových systémů či operačních systémů (haš je stále možné dál použít, ale je nečitelný pro případného útočníka). Dále také pro poskytnutí autenticity v elektronické komunikaci, pomocí vytvoření haše zasílané zprávy, která se k původní zprávě přidává jako tzv. autentizační kód zprávy (MAC, z angl. Message Authentication Code) v případě symetrických kryptografických algoritmů či jako elektronický podpis v případě asymetrických kryptografických algoritmů [125].

### 3.1.3 Symetrické algoritmy

Symetrické algoritmy jsou založeny na použití stejného klíče $K_S$ (tzv. symetrický či tajný klíč) pro šifrování i dešifrování. Tedy $K_S = K_E = K_D$ či existuje možnost jednoduché transformace z $K_E$ na $K_D$:

$$(K_E = f(K_D)) \vee (K_D = f(K_E)) \tag{3.16}$$

Výhodou symetrických algoritmů oproti asymetrickým je jejich rychlost [127]. Největší nevýhodou je pak nutnost distribuce symetrického klíče před začátkem komunikace a šifrování [124]. Dále pak i počet nutných klíčů, tedy pokud máme počet komunikujících stran $n$ je počet nutných klíčů ke komunikaci $n(n-1)/2$ (pokud uvažujeme komunikaci každý s každým). V rámci dnešních symetrických kryptografických algoritmů pak rozeznáváme dva základní druhy [127]: (i) symetrické blokové algoritmy a (ii) symetrické proudové algoritmy.

### I. Symetrické proudové algoritmy

Symetrické proudové algoritmy zpracovávají otevřený text bit po bitu a to nejčastěji pomocí operace bitové exkluzivní disjunkce (XOR, z angl. Exclusive OR) značená jako $\oplus$. Pravdivostní tabulka pro $x \oplus y$ je následující:

Tab. 3.3: Pravdivostní tabulka funkce exklusivní disjunkce využívané v rámci symetrických proudových algoritmů.

| **Vstup $x$** | 0 | 0 | 1 | 1 |
|---|---|---|---|---|
| **Vstup $y$** | 0 | 1 | 0 | 1 |
| **Výstup *XOR*** | 0 | 1 | 1 | 0 |

Symetrické proudové algoritmy zpracovávají bit po bitu (pracují s jednotlivými bity) otevřeného textu $P$ o bitové velikost $l_p$:

$$P = \left\{ \{0,1\}_{l_P-1}, \{0,1\}_{l_P-2}, ..., \{0,1\}_0 \right\}; l_P \in \mathbb{N}^+, \tag{3.17}$$

kde $0, 1$ představuje jednotlivé bity otevřeného textu a dolní index jejich bitovou pozici. Tyto bity jsou tedy šifrovány do šifrovaného textu $C$ o bitové velikost $l_C$, který je složen také z jednotlivých bitů:

$$C = \left\{ \{0,1\}_{l_C-1}, \{0,1\}_{l_C-2}, ..., \{0,1\}_0 \right\}; l_C \in \mathbb{N}^+. \tag{3.18}$$

Vyjděme teď z definice 3.2, 3.2, 3.17 a 3.18, pak lze psát šifrovací funkce symetrického proudového algoritmu jako:

$$E_{K_S}(P) = P \rightarrow C = E_{K_S} : \{0,1\}^{l_P} \bullet \{0,1\}^{l_{K_S}} \rightarrow \{0,1\}^{l_C}, \tag{3.19}$$

kde $\bullet$ značí vnitřní operaci funkce šifrování (či dešifrování), která u proudových šifer bývá nejčastěji právě XOR, a $l_{K_S}$ značí bitovou velikost klíče $K_S$:

$$K_S = \left\{ \{0,1\}_{l_{K_S}-1}, \{0,1\}_{l_{K_S}-2}, ..., \{0,1\}_0 \right\}; l_{K_S} \in \mathbb{N}^+, \tag{3.20}$$

Dešifrovací proces je pak oproti šifrování opačný proces, tedy $E_{K_S}^{-1} = D_{K_S}$. Díky tomu lze snadno odvodit dešifrovací algoritmus:

$$E_{K_C}^{-1}(C) = D_{K_S}(C) = C \to P = D_{K_S} : \{0,1\}^{l_C} \bullet \{0,1\}^{l_{K_S}} \to \{0,1\}^{l_P}, \quad (3.21)$$

neboli

$$\forall K_S : D_{K_S}(E_{K_S}(P)) = P. \quad (3.22)$$

V současné době existují dva základní typy proudových šifer [127]:

- **Synchronní proudové algoritmy**, při jejich použití musí být Alice i Bob přesně synchronizováni na stejném kroku, tak aby přijatý bit byl vždy správně dešifrován. Pokud například nějaký bit nebude doručen např. vlivem chyby přenosového kanálu, pak je synchronizace ztracena. Tento stav musí být včas detekován, tak aby byla navázána opětovná synchronizace.
- **Asynchronní proudové algoritmy** (známe taky jako tzv. samosynchronní proudové algoritmy), jsou algoritmy, kdy Alice a Bob jsou automaticky synchronizováni po přijetí určitého počtu bitů. Výhodou zde tedy je, že ztráta jednoho bitu tedy během komunikace tak nezapříčiní ztrátu synchronizace a přerušení procesu dešifrování. Nevýhodou těchto algoritmů oproti synchronním však je, že jsou náchylné na aktivní útoky, kdy útočník nedetekovaně přidává vlastní bity, tak aby nežádoucím způsobem ovlivnil komunikaci.

V rámci proudových šifer existuje celá řada algoritmů, nicméně dnes již není mnoho z nich považováno za bezpečné či jsou považovány za pouze částečně bezpečné např. A5/1, A5/2, Achterbahn 128/80, FISH, Grain, ISAAC, MUGI, PANAMA, Phelix, Py, RC4, SOBER-128 a další [149]. V současnosti existuje pouze několik šifer, na které dosud není znám žádný úspěšný útok či kryptoanalýza nebyla dostatečně úspěšné [124]: HC-256, CryptMT, Pike, Rabbit, Scream, SEAL, SNOW, SOSEMANUK a VEST. V rámci mezinárodních doporučení se pak můžeme řídit např. projektem excelence ENCRYPT (z angl. European Network of Excellence for Cryptology) a jeho pokračování ENCRYPT II. V těchto projektech se řešitelé v letech 2004–2013 mj. snažili o nalezení nejvhodnějších symetrických proudových šifer, kde v dubnu 2008 [150] vytvořili první doporučení, které následně aktualizovali již v září 2008 [151] a následně v roce 2009 [152] a 2012 [153].

V rámci nejaktuálnější verze ENCRYPT II 2012 pak zůstávají algoritmy považované za vhodné a bezpečné [153]: pro (i) softwarové implementace: HC-128, Rabbit, Salsa20/12 a SOSEMANUK; a pro (ii) hardwarové implementace: Grain v1, MICKEY 2.0 a Trivium. Nicméně některé práce poukazují na přílišnou implementační složitost některých algoritmů jako HC-256 či Sosemanuk, která může zapříčinit mj. i bezpečnostní problémy výsledného systému [154].

Obecně lze říci, že proudové šifry jsou rychlejší jak blokové, nejsou tolik náchylné na chyby v přenosu a potřebují mnohem méně paměti (jelikož nezpracovávají bloky bitů) [127]. Nicméně jejich implementace bývá z pohledu bezpečnosti náročná. Další nevýhodou těchto algoritmů je, že poskytují pouze důvěrnost, nikoliv však integritu či autenticitu [124]. Proudové šifry se využívají převážně tam, kde předem neznáme velikost otevřeného textu $P$ či kde se předpokládá např. kontinuální tok dat (z angl. streaming) apod.

### II. Blokové symetrické algoritmy

Blokové symetrické algoritmy pracují oproti proudovým s jednotlivými stejně velkými a předem definovanými bitovými bloky otevřeného textu $P$:

$$P = \left\{ \{0,1\}_{P_n}^{l_m}, \{0,1\}_{P_{n-1}}^{l_m}, ..., \{0,1\}_{P_1}^{l_m} \right\}, \tag{3.23}$$

kde $l_m$ je velikosti bloku a $n$ je počet bloků. Platí tedy:

$$l_P = n \cdot l_m; l_m, n, l_P \in \mathbb{N}^+. \tag{3.24}$$

Jednotlivé bloky otevřeného textu jsou v rámci blokových kryptografických algoritmů šifrovány do šifrovaného textu $C$ o velikost $l_C$, který je složen také z jednotlivých bloků o velikosti $l_m$:

$$C = \left\{ \{0,1\}_{C_n}^{l_m}, \{0,1\}_{C_{n-1}}^{l_m}, ..., \{0,1\}_{C_1}^{l_m} \right\}, \tag{3.25}$$

kde $l_m, n \in \mathbb{N}^+$. Vyjděme z definice 3.23 a 3.25, pak lze tedy definovat proces šifrování jako funkci:

$$E_{K_S}(P) = P \rightarrow C = E_{K_S} : \{0,1\}_{K_{S_n}}^{l_m} \bullet \{0,1\}_{P_n}^{l_m} \rightarrow \{0,1\}_{C_n}^{l_m}, \tag{3.26}$$

kde pro tajný klíč $K_S$ blok symetrického blokového algoritmu platí:

$$K_S = \left\{ \{0,1\}_{K_{S_n}}^{l_m}, \{0,1\}_{K_{S_{n-1}}}^{l_m}, ..., \{0,1\}_{K_{S_1}}^{l_m} \right\}; l_m, n \in \mathbb{N}^+, \tag{3.27}$$

Dešifrovací proces je pak oproti šifrování procesem vice versa, tedy $E_{K_S}^{-1} = D_{K_S}$. Díky tomu lze snadno odvodit dešifrovací algoritmus:

$$E_{K_S}^{-1}(P) = D_{K_S}(C) = C \rightarrow P = D_{K_S} : \{0,1\}_{K_{S_n}}^{l_m} \bullet \{0,1\}_{C_n}^{l_m} \rightarrow \{0,1\}_{P_n}^{l_m}. \tag{3.28}$$

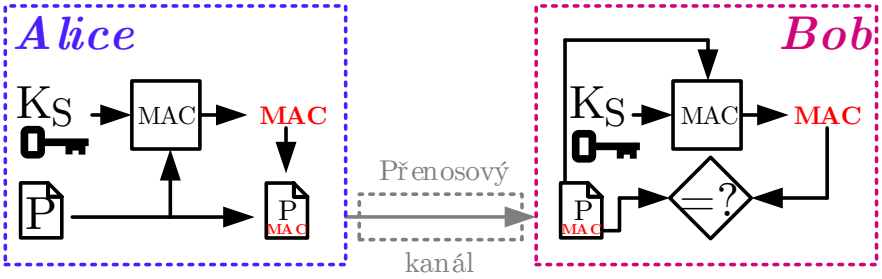
Pokud vycházíme z 3.26 a 3.28 pak lze stanovit vztah:

$$\forall K_S : D_{K_S}(E_{K_S}(P)) = P. \tag{3.29}$$

V rámci blokových algoritmů pak existuje několik módů blokových šifer [127]:

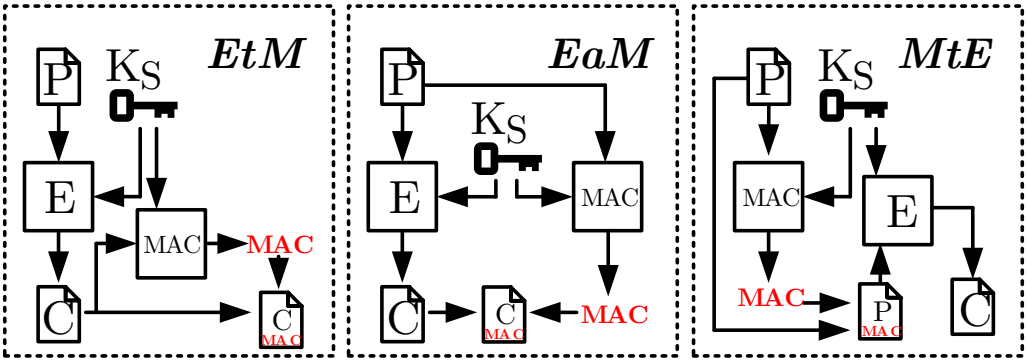
- **Elektronická kódová kniha** (ECB, z angl. Electronical Code Book) tento mód je jeden z nejzákladnějších. Základní vlastností je, že pokud šifrujeme stejný blok otevřeného textu stejným klíčem, pak výsledný blok šifrovaného textu bude vždy totožný. Z tohoto důvodu je tento mód velice náchylný na útok hrubou silou či útok pomocí vkládání vlastních bloků. Další vlastností tohoto módu je, že jakákoliv chyba v přenosu šifrovaného textu pak ovlivní dešifrovací proces celého bloku (nikoliv však bloky další). Použití tohoto módu je všude tam, kde jsme schopni zaručit použití vždy jiného klíče $K_S$ či pokud má otevřený text náhodný charakter.
- **Řetězení šifrovaného textu** (CBC, z angl. Cipher Block Chaining) režim přidává tzv. mechanismus zpětné vazby do šifrovacího procesu. Otevřený text je XORován s předchozím blokem šifrovaného textu před jeho šifrováním tak, aby dva identické bloky otevřeného textu byly šifrovány vždy jinak. Zatímco mód CBC díky této vlastnosti chrání proti mnoha útokům hrubou silou, či vkládání, tak i jediná bitová chyba u přenášeného bloku šifrovaného textu tak může zapříčinit chybu v dešifrování tohoto bloku do otevřeného textu a všech následujících bloků.
- **Zpětnovazební módy** je mód zpětné vazby ze šifrovaného textu (CFB, z angl. Cipher Feedback) a mód zpětné vazby z výstupu (OFB, z angl. Output Feedback). Jedná se o módy, které převádí blokovou šifru na proudovou. CFB je kombinací vlastností CBC a proudové šifry, jedná se o samosynchronní proudovou šifru, kdy ke samosynchronizaci stačí pouze dva předchozí správné bloky. OFB je pak synchronní proudová šifra.
- **Čítačový modus** (CTR, z angl. Counter mode) je mód velmi podobný OFB, také převádí blokovou šifru na synchronní proudovou šifru. S rozdílem, že je u této šifry použit čítač resp. předem daný stav čítače.

V rámci blokových šifer opět existuje nepřeberné množství algoritmů, proto si uvedeme již jen ty nejznámější: AES, Blowfish, DES, 3DES, Serpent, Twofish, Camellia, CAST-128/256, IDEA, RC2/5/6, SEED, ARIA, Skipjack, TEA, XTEA a XXTEA. Blokové šifry jsou obecně, díky zpracovávání většího bloku dat najednou, náročnější na paměť, pomalejší a náchylnější na chyby v přenosu oproti např. proudovým šifrám [127]. Použití blokových algoritmů je všude tam, kde známe již dopředu velikost dat a data samotná, např. periodická vzdálená měření, šifrování souborů, aj. Blokové algoritmy oproti proudovým mohou poskytovat navíc i autenticitu a integritu zprávy [124]. Využívá se k tomu tzv. autentizačního kódu zprávy (MAC, z angl. Message Auhentication Code) [127]. Funkčnost MAC je zobrazena na Obr. 3.2.




Obr. 3.2: Ukázka funkčnosti MAC algoritmu.

Pro tvorbu MAC může být použita libovolná bloková šifra např. mód CBC či haš funkce (takový MAC kód se pak označuje za HMAC) [86]. Jelikož MAC používá dva stejné klíče (symetrický tajný klíč), tak u něj není možné zaručit nepopiratelnost. Otevřený text může být jako na Obr. 3.2 zasílán nešifrovaně nebo při nutnosti zaručit i důvěrnost se zpráva ještě navíc šifruje. Potřeba zaručit důvěrnosti společně s autentizací a integritou zprávy vedla k vytvoření tzv. autentizačního šifrování (AE, z angl. Authenticated Encrpytion) [124]. Existují tři základní typy AE [127]: (i) Šifruj-pak-MAC (EtM, z angl. Encrypt-then-MAC), (ii) šifruj-a-MAC (E&M, z angl. Encrypt-and-MAC), a (iii) MAC-pak-šifruj (MtE, z angl. MAC-then-Encrypt); viz Obr. 3.3.




Obr. 3.3: Ukázka různých typů autentizačního šifrování.

Autentizační šifrování tedy může být zajištěno jako spojení šifrovacího (blokového) algoritmu a MAC nebo pomocí speciálních módů blokových šifer, které již šifrování a MAC nativně spojují. Takovými módy jsou např. CCM, EAX, GCM či OCB [124].

### 3.1.4 Asymetrické algoritmy

Asymetrické algoritmy oproti symetrickým používají tzv. klíčového páru (z angl. keypair), tedy dvou klíčů $K_E$ a $K_D$. Ty představují klíčový pár $k = (K_E, K_D)$, pro

který platí $k \in K$. Pro šifrování je uvažován veřejný (šifrovací) klíč $\mathrm{K}_E$ a pro soukromý (dešifrovací) klíč $\mathrm{K}_D$. Platí také, že klíče nejsou stejné a není možné vypočíst druhý klíč ze znalosti prvního a naopak (viz rovnice 3.30).

$$(K_E \neq K_D) \wedge (K_E \neq f(K_D)) \wedge (K_D \neq K_E) \wedge (K_D \neq f(K_E)) \tag{3.30}$$

Výhodou asymetrických algoritmů je, že je možné pomocí nich dohodnout přes nezabezpečený kanál tajný klíč [124]. Další velkou výhodou v rámci klíčového managementu je počet klíčů [127]. Asymetrické algoritmy potřebují v rámci systému pouze $2n$ klíčů, oproti symetrickým algoritmům, které potřebují $n(n-1)/20$ klíčů. K šifrování pak asymetrické algoritmy využívají tzv. jednosměrných či jednocestných funkcí (z angl. one-way function). Jednocestná funkce je funkce, kterou je jednoduché vyčíslit, ale je velice časově náročné spočítat její inverzi (tzn. z výstupu získat zpětně vstup). Oproti hašovacím funkcím jsou tyto funkce reverzibilní při znalosti "tajemství", tj. privátního klíče $K_D$. Platí tedy, že funkce $f$ je jednosměrná pouze a jedině tehdy, pokud:

- Popis funkce $f()$ je veřejně znám.
- Pokud máme $x$, pak je výpočetně velice jednoduché spočítat $f(x)$.
- Pokud máme $y$, které je v rozsahu $f()$, je výpočetně složité (obtížné) nalézt takové $x$, pro které platí $f(x) = y$.

V rámci asymetrické kryptografie se pak využívá dvou základních problémů jednocestných funkcí [124]: (i) problém diskrétního logaritmu, a (ii) problém faktorizace. V rámci diskrétního logaritmu máme např. šifrovací funkci:

$$f(P) \equiv E_{K_E} \equiv P^{K_E} \pmod{n} \equiv C, (n, K_E) \in N^+. \tag{3.31}$$

V tomto případě je tedy výpočetně triviální vypočítat $C$ z daných $P, K_E, n$ ($n$ je velké prvočíslo), nicméně netriviální a výpočetně náročná je pak úloha výpočtu $P$ ze znalosti $K_E, C$. To vše za předpokladu, že tyto parametry jsou dostatečně velké, tj. $(K_E, n) \ggg 1$. V rámci faktorizace je pak dán problém rozkladu velkého čísla na prvočísla, mějme dvě velké odlišná prvočísla $(q_1, q_2) \ggg 1$ (platí tedy $q_1 \neq q_2$). Jejich součin bude funkce:

$$f(x) = q_1 \cdot q_2 = n, (q_1, q_2) \in N^+, \tag{3.32}$$

kde $n, q_1, q_2$ jsou velká prvočísla a $n$ je veřejný parametr. V tomto případě je následně opět výpočetně triviální vypočítat $n$ z daných $(q_1, q_2)$, nicméně netriviální úlohu pak tvoří vypočtení $(q_1, q_2)$ z pouhé znalosti $n$.

Dostatečná velikost parametrů ($\ggg 1$) je u asymetrických algoritmů relativní pojem, který je dán současným maximálním teoreticky dosažitelným výpočetním

výkonem v dané době. Velkou slabinou asymetrických algoritmů je totiž jejich náchylnost na útok hrubou silou (tj. útok kdy útočník např. zkouší všechny klíčové kombinace), z tohoto důvodu se u asymetrických algoritmů používá mnohem větších parametrů než u symetrických algoritmů (mnohdy o jeden až dva řády větších) [125]. Zvětšením parametrů pak dosahujeme u asymetrických algoritmů větší výpočetní náročnost pro úlohu inverzního výpočtu $f(x)$, tak aby nebylo možné v reálném čase tuto úlohu řešit [124]. Bohužel tím roste také náročnost již tak složitých operací asymetrických algoritmů (násobení, mocnění, modulární operace), které jsou tedy také mnohonásobně pomalejší oproti symetrickým algoritmům (které většinou používají bitové operace) [127].

Asymetrické algoritmy se využívají pro [125]: (i) šifrování krátkých zpráv (dat), (ii) dohodu či sestavení symetrických tajných klíčů v nezabezpečených kanálech pomocí veřejných parametrů asymetrických algoritmů; a (iii) pro elektronické podepisování (certifikace). Jako hlavní zástupce asymetrických algoritmů pak můžeme jmenovat [124]:

- **Pro šifrování:** Rivest Shamir Adleman (RSA), Cramer-Shoup, ElGamal, Paillier
- **Pro dohodu či sestavení klíče:** Diffie-Hellman (DH)
- **Pro podepisování:** Digital Signature Algorithm (DSA), RSA

Jak již bylo řečeno, asymetrické algoritmy pro zajištění dostatečné úrovně bezpečnosti potřebují velké vstupní parametry. Z tohoto důvodu vznikl nový přístup k asymetrickým algoritmům, kdy se využívá algebraické struktury eliptických křivek nad uzavřeným polem. Tento přístup je dnes známý jako tzv. kryptografie eliptických křivek (ECC, z angl. Elliptic Curve Cryptography) [127].

### Kryptografie eliptických křivek

Eliptické křivky byly studovány jako matematický koncept od druhého století našeho letopočtu. Nicméně název "eliptický" byl přiřazen až v devatenáctém století [124]. Koncept kryptografie eliptických křivek je však znám pouhých posledních 30 let. První použití eliptických křivek v kryptografii použil H. W. Lenstra pro rychlou faktorizaci dvou velkých celých čísel nad eliptickými křivkami [155]. Původce kryptografie eliptických křivek, tak jak je známa dnes, jsou považování N. Koblitz a V. Miller. V roce 1985 N. Koblitz [156] a V. Miller [157] nezávisle na sobě poprvé navrhli kryptografické algoritmy používající strukturu eliptických křivek nad uzavřeným polem. Následně se eliptické křivky staly klíčovou částí mnoha dnešních kryptografických algoritmů. Většinou se jedná o klasické asymetrické algoritmy diskrétního logaritmu, které následně využívají eliptických křivek nad uzavřeným polem, jedná se například

o: ECDH (tedy algoritmus Diffie-Hellman DH, využívající eliptické křivky), ECDSA (algoritmus digitálního podpisu DSA, využívající eliptické křivky) a spousty dalších.

ECC tedy využívá algebraickou strukturu eliptických křivek nad konečným polem. Definujme si nyní křivku nad konečným polem $\mathbb{F}$ [158]:

$$E(\mathbb{F}) : y^2 = x^3 + ax + b \in \mathbb{F}, \tag{3.33}$$

v rámci ECC je nutno dodržet singularitu křivky, tedy aby diskriminant $\Delta$ [159]:

$$\Delta = 4a^3 + 27b^2, \tag{3.34}$$

nebyl nulový. Pokud pro křivku z 3.33 tedy platí:

$$4a^3 + 27b^2 \neq 0, \tag{3.35}$$

tak se jedná o eliptickou křivku ($E$). V opačném případně je křivka tzv. singulární a nejedná se pak o eliptickou křivku (je deformována a má ostrý body). V kryptografii se setkáme převážně s konečným polem prvočíselného řádu $p$ ($\mathbb{F}_p$), označováno někdy jako prvočíselné pole) a polem o řádu $2^m$ ($\mathbb{F}_{2^m}$), označováno někdy jako binární pole), kde $m \in \mathbb{N}+$. V rámci ECC se analogicky pak setkáváme převážně s eliptickými křivkami nad polem s prvočíselným řádem ($E(\mathbb{F}_p)$) či nad polem s řádem $2^m$ ($E(\mathbb{F}_{2^m})$). Eliptickou křivku nad polem o řádu $p$ budeme tedy značit jako $E(\mathbb{F}_p)$ a definujeme ji jako:

$$E(\mathbb{F}_p) : y^2 \equiv x^3 + ax + b \pmod{p} \in \mathbb{F}_p. \tag{3.36}$$

Každá eliptická křivka $E$ je pak definována doménovými parametry (z angl. domain parameters). Tyto křivky jsou specifikovány v rámci $E(\mathbb{F}_p)$ šesti doménovými parametry, tzv. sextule:

$$T_{\mathbb{F}_p} = (p, a, b, G, n, h), \tag{3.37}$$

kde $p$ je velké prvočíslo definující pole $\mathbb{F}_p$; $a$, $b$ jsou dva elementy z $\mathbb{F}_p$ (tedy $a, b, \in \mathbb{F}_p$), specifikující eliptickou křivku $E(\mathbb{F}_p)$. Dále $G$ je tzv. základní bod ($G = (x_G, y_G)$) na křivce $E(\mathbb{F}_p)$; celé číslo $n$ je pak řád bodu $G$ a celé číslo $h$ je tzv. kofaktor ($h \leq 4$, nejlépe však $h = 1$), definovaný jako:

$$h = \frac{\#E(\mathbb{F}_p)}{n}. \tag{3.38}$$

Eliptickou křivku nad polem o řádu $2^m$ budeme značit jako $E(\mathbb{F}_{2^m})$ a definujeme ji jako:

$$E(\mathbb{F}_{2^m}) : y^2 + xy = x^3 + ax^2 + b \in \mathbb{F}_{2^m}. \tag{3.39}$$

Tyto křivky jsou specifikovány sedmi doménovými parametry, tzv. septule:

$$T_{\mathbb{F}_{2^m}} = (m, f(x), a, b, G, n, h), \tag{3.40}$$

kde $m$ je celé číslo definující pole $\mathbb{F}_{2^m}$ a $f(x)$ je neredukovatelný binární polynom stupně $m$ definující polynomiální bázi reprezentace $\mathbb{F}_{2^m}$. V tomto případě tedy platí, že konečného pole $\mathbb{F}_{2^m}$ je množina o $2^m$ prvcích, kde $m \in \mathbb{N}+$. Jednotlivé prvky jsou pak reprezentovány jako binární polynomy maximálního stupně $m-1$ (z toho častý název binární):

$$\left\{a_{m-1}x^{m-1} + a_{m-2}x^{m-2} + ... + a_1x + a_0, a_i \in \{0,1\}\right\}. \tag{3.41}$$

Tyto vektory se následné ukládají pro větší výpočetní efektivitu do tzv. $m$-bitových vektorů koeficientů $a_i$:

$$(a_{m-1}, a_{m-2}, ..., a_1, a_0). \tag{3.42}$$

Aby následně nedocházelo k zvýšení stupně polynómu nad $m-1$ (např. násobením), zavádíme tzv. binární redukční polynom $f(x)$ stupně maximálně $m-1$ nad polem $\mathbb{F}_{2^m}$. Tento polynom je ireducibilní (tedy nerozložitelný na součin polynómů nižšího stupně). V ECC se následně využívá dvou typů polynómů:

- **Trinomiální**, s tvarem $x^m + x^k + 1$, kde platí $1 \leq k \ \leq m-1$
- **Pentanomiální**, s tvarem $x^m + x^{k_3} + x^{k_2} + x^{k_1} + 1$, kde platí $1 < k_1 < k_2 < k_3 \leq m-1$

$a$, $b$ jsou opět dva elementy z $\mathbb{F}_{2^m}$ (tedy $a, b, \in \mathbb{F}_{2^m}$) specifikující eliptickou křivku $E(\mathbb{F}_{2^m})$. Dále $G$ je tedy základní bod ($G = (x_G, y_G)$) na křivce $E(\mathbb{F}_{2^m})$, celé číslo $n$ je pak následně řád bodu $G$ a celé číslo $h$ je kofaktor ($h \leq 4$, nejlépe však $h = 1$), definovaný jako:

$$h = \frac{\#E(\mathbb{F}_{2^m})}{n}. \tag{3.43}$$

Největší výhodou ECC oproti klasickým asymetrickým algoritmům je stejná úroveň bezpečnosti s použitím mnohem menších parametrů (řádově srovnatelných se symetrickými algoritmy), viz Tab. 3.4.

Tab. 3.4: Srovnání přibližné bitové velikosti parametrů pro stejnou úroveň bezpečnosti u typů jednotlivých kryptografických algoritmy [160].

| **Symetrické alg.** | 64 b | 128 b | 160 b | 192 b | 256 b |
|---|---|---|---|---|---|
| **Klasické Asymetrické alg. (faktoriace)** | 745 b | 6974 b | 13730 b | 23475 b | 53516 b |
| **Klasické Asymetrické alg. (logaritmus)** | 640 b | 4400 b | 7864 b | 12548 b | 26268 b |
| **Asymetrické alg. na bázi ECC** | 128 b | 256 b | 320 b | 384 b | 256 b |

To následně vede k redukci potřebné paměti i výkonu pro jednotlivé operace

uvnitř kryptografických algoritmů či nižšího využití komunikačního pásma [127, 124]. Tato hlavní výhoda je také důvodem, proč jsou eliptické křivky používány nejen napříč internetovými aplikacemi, ale také preferovanými algoritmy v zařízeních s limitovaným výkonem a pamětí [125].

## 3.2 Analýza využívaných technologií v inteligentních sítích

V rámci inteligentních sítí a internetu věcí je obecně uvažováno či představováno spousty různých komunikačních technologií i řešení a to jak kabelových, tak bezdrátových. V rámci odborné literatury však existuje jasný pohled na to, které technologie jsou nejčastějšími v rámci použití u inteligentních sítí v energetice. Tab. 3.5 shrnuje jednotlivé vědecké práce (tzv. survey), které se věnují shrnutí a přehledu využívaných komunikačních technologií v energetických inteligentních sítích.

Tab. 3.5: Analýza využívaných technologií v rámci inteligentních sítích.

| **Rok** | **Drátové technologie** | **Bezdrátové technologie** | **Zdroj** |
|---|---|---|---|
| 2010 | PLC, DSL | WiMAX, Celulární, ZigBee, WLAN | [161] |
| 2011 | PLC, optika DSL | WiMAX, Celulární, ZigBee, WLAN, | [162] |
| 2013 | PLC, optika | WiMAX, Celulární, ZigBee, WLAN, | [163] |
| 2014 | PLC, optika, Ethernet, DSL | WiMAX, Celulární, ZigBee, WLAN | [164] |
| 2014 | PLC, optika, Ethernet | WiMAX, Celulární, ZigBee Satelit | [165] |
| 2015 | PLC, optika, Ethernet, | WiMAX, Celulární, ZigBee, WLAN, Z-Wave, | [166] |
| 2016 | PLC | WiMAX, Celulární, ZigBee, WLAN | [167] |
| 2016 | PLC, optika, Ethernet, DSL | WiMAX, Celulární, ZigBee, WLAN, Z-Wave, RF MESH, Satelit | [168] |
| 2016 | PLC, optika, Ethernet, DSL | WiMAX, Celulární, ZigBee, RF MESH, Satelit | [169] |
| 2016 | PLC, optika | WiMAX, Celulární, ZigBee, LPWAN | [170] |

V tabulce zkratka PLC představuje technologii komunikace po elektrické síti (z angl. Power Line Communication); optika představuje obecné použití optických vláken vlákna pro komunikaci; Ethernet představuje standardizovanou technologii z větší části dle IEEE 802.3; DSL zde značí drátové vedení digitální technologie účastnických linek dle ITU standardizace (z angl. Digital Subscriber Line); celulární značí buňkové (celulární) technologie druhé generace a vyšší (tzv. 2G+); RF MESH značí rádiovou síť typu MESH; Satelit tedy značí satelitní komunikaci; a LPWAN je pak bezdrátová nízko-energetická WAN technologie na dlouhé vzdálenosti (z angl. Low-power Wide Area Network); dále pak už jsou jen standardizované bezdrátové komunikační technologie ZigBee (IEEE 802.15.4), WLAN (802.11) a Z-Wave. Rozdělme tyto technologie dle definovaného komunikačního modelu (viz Obr. 1.1):

- **Technologie v transportní části sítě**: optika, Ethernet, DSL, WiMAX, Celulární, Satelit.
- **Technologie v přístupové části sítě**: PLC, Celulární (pouze druhá generace, 2G), IEEE 802.15.4, IEEE 802.11, Z-Wave, RF MESH, LPWAN.

Rozložení technologií v rámci transportní a přístupové části sítě, stejně jako použité technologie v rámci těchto částí i jejich vhodnost pro jednotlivé části byla řešena autorem samostatně i ve spolupráci s distributorem E.ON či firmou MEgA na vážených tuzemských odborných konferencích ČK CIRED [171, 172, 173]. Tato práce se zabývá převážně přístupovou částí sítě, z tohoto důvodu budou dále v této kapitole přiblíženy pouze technologie z této části sítě.

### 3.2.1 Power Line Communication

Power Line Communication (PLC) je přenos dat po elektrické síti, kde existují tři hlavní typy této technologie [174]:

- **PLC s velmi nízkou přenosovou rychlostí**, označovaná také jako PLC v ultra úzkém pásmu (z angl. ultra narrow band PLC). Tento typ PLC využívá velmi úzkého frekvenčního pásma 30–300 Hz, kde se propustnost pohybuje do 100 b/s. Tyto komunikační technologie mají velký komunikační dosah v řádu desítek či stovek kilometrů bez opakovače. Nicméně tento typ technologií není standardizovaný a jedná se většinou tedy o proprietární řešení. Další nevýhodou těchto technologií je, že nepoužívají žádné zabezpečení. Tyto technologie se většinou používají na automatické odečty, detekce výpadků, kontrolu zatížení, aj.
- **Úzkopásmové PLC** (NB-PLC, z angl. Narrowband PLC), tento typ PLC využívá frekvenčního pásma 3–500 kHz (v Evropě 3–148,5 kHz), kde se propustnost pohybuje do 500 kb/s. V této skupině PLC se již objevuje několik standardů jako např. PRIME, G3, ITU-T G.990x/hnem, IEEE P1901.2 a další. Většina standardů již řeší i bezpečnost, kdy se většinou soustředí na poskytování důvěrnosti. Tento druh PLC je využíván na vzdálenou komunikaci se smart metry, vzdálenou telemetrii či např. i energetické řízení v reálném čase (většinou na středí vzdálenost v řádu stovek metrů až jednotek kilometrů).
- **Širokopásmové PLC** (BPL-PLC, z angl. Broadband PLC), tento typ PLC pak využívá frekvenčního pásma 1,8–250 MHz, kde propustnost může být i v řádu stovek Mb/s. Tato skupina PLC má vsobě také řadu standardů jako např. HomePlug, ITU-T G.996x, ITU-T G.hn, IEEE P1901, a další. Využití BPL-PLC je pak převážně v HAN sítích, kde většinou poskytují již autenticitu i důvěrnost.

Obecně je pak největším problémem na úrovni informační bezpečnosti u PLC technologií následující [175]: (i) autenticita dat a uživatelů během komunikace, (ii) zajištění dostatečné úrovně důvěrnosti, a (iii) zajištění klíčového managementu resp. distribuce tajemství (klíče, aj.). Tyto aktuální problémy a nedostatky potvrzují i zkušenosti autora s technologií PLC, prokázané řadou experimentální testů a výzkumem v oboru převážně zaměřeném na inteligentní sítě, kde většina výsledků byla následně i publikovány v řadě mezinárodních konferencích (indexovaných ve WoS/Scopus) [176, 177, 178, 179, 180, 181] i impaktovaných časopisech [182, 183, 184].

### 3.2.2 Celulární technologie

Celulární technologie jsou vyvíjeny pod standardem 3GPP (z angl. 3rd Generation Partnership Project) [185]. 3GPP je standard vyvíjen řadou mezinárodních firem v rámci moderních celulárních telekomunikačních sítí [186]. Jedná se převážně o operátorské sítě, které pracují nejčastěji v licencovaném pásmu. V rámci těchto technologií je používána tzv. generace (G), která určuje stupeň vývoje (evoluce). Vývoj dle jednotlivých generací je zobrazen v Tab. 3.6

Tab. 3.6: Jednotlivé generace celulárních technologií.

| | |
|---|---|
| **1. Generace (1G)** | Jedná se o první generaci celulárních technologií, její historie sahá do 80. let 19. století, od té doby téměř každých deset let přichází nová generace celulárních technologií. Je označována jako 1G a jednalo se o analogovou technologii, kde koncová zařízení měla velmi špatnou energetickou efektivitu a kvalita služeb stejně jako bezpečnost byla na velmi nízké úrovni. Maximální propustnost byla 2,4 kb/s. |
| **2. Generace (2G)** | Druhý vývojový stupeň, který v roce 1991 přenesl celulární technologie z analogové oblasti do digitální. Technologie je označována jako GSM (nicméně v rámci 2G jsou používány i další protokoly jako např. CDMA, TDMA, iDEN či PDC), umožňovala již přenos jednoduchých multimedií. Propustnost je zde 50 kb/s. Díky novým vizím a rychlému vzestupu digitální komunikace pak vznikají stupně označované jako 2.5 a 2.75G. Jedná se o mezistupně pro přechod na třetí generaci celulárních sítí. 2.5G představuje nový a více efektivní techniku přepínání paketů a 2.75G přináší zvýšení kapacity a propustnosti teoreticky až na 1 Mb/s, prakticky pouze stovky kb/s (technologie je známa jako EDGE). |
| **3. Generace (3G)** | Třetí generace celulárních sítí byla představena v roce 1998. Největší přínos představuje celulární internet a další aditivní služby s tím spjaté. Propustnost se zde zvýšila na 2 Mb/s pro nepohyblivá koncová zařízení. Opět se zde následně objevují tzv. 3.5G a 3.75G, které mají připravit síť na přechod do 4G. |
| **4. Generace (4G)** | Čtvrtá generace v roce 2008 přinesla navýšení propustnosti, kvality služeb a dalších parametrů. Propustnost je zde 0,1 Gb/s–1 Gb/s. |
| **5. Generace (5G)** | Pátá generace pak představuje současnou vizi celulárních sítí, kdy by mělo dojít k představení nízkoenergetických koncových prvků, ale také opět zvýšení propustnosti, příchod nových služeb i propojení stávajících technologií do multitechnologické interoperabilní celulární sítě. |

V rámci přístupové části inteligentních sítí jsou pak zajímavé technologie druhé generace GSM/GPRS resp. dnes již hlavně EDGE (označována jako 2.75, jedná se o další generační vývojový stupeň GSM), které se v této oblasti již běžně používají [170]. V rámci této technologie jsou pak známy šifrovací algoritmy GEA využívající proudové algoritmy A5 [187]. Varianty A5/1 a A5/2 jsou dnes již považovány za nebezpečné a existuje řada kryptonalytických technik, jak tyto algoritmy napadnout [188], [189]. Novější současná varianta A5/3 pracuje s parametry o velikost 64 bitů. Dnes je však již považována za pouze částečně bezpečnou, protože na ní již bylo provedeno také několik úspěšných útoků [188, 189], kde některé z nich dokázaly v reálném čase (řádu desítek minut až jednotek hodin) zkompromitovat zařízení a získat tajný klíč [190]. Nová připravovaná varianta A5/4 pracuje již se 128-bitovými parametry a poskytuje tak větší bezpečnost než předchozí varianty [191]. Obecně lze říci, že algoritmy A5 poskytují společně s logikou sítě autentizaci a důvěrnost. Nicméně největším problémem této technologie je, že i přes používání algoritmů s doporučovanou délkou parametrů je správa těchto parametrů pod kontrolou operátora sítě, nikoliv uživatele. Díky tomu, i když technologie poskytuje autentizaci a důvěrnost, tak z pohledu uživatele tyto principy zajištěny nejsou, protože on sám nemá pod kontrolou samotné parametry pro kryptografické algoritmy. Výše popsané nedostatky jsou potvrzeny i praxí autora s technologiemi i v rámci již nové vize 5. generace, kdy výzkum vedený v této oblasti autor zaměřoval převážně na potenciál těchto typů sítí pro aplikace inteligentních sítí, telemetrických systémů, chytrých domácností, chytrých měst a internetu věcí. Výsledky z experimentálních měření s těmito technologiemi byly také publikovány na vědeckých konferencí (indexováno ve WoS/Scopus) [192, 193, 194], v impaktovaném časopise [195], a vědecké soutěži na konferenci EEICT2014, kde autor získal cenu za druhé míst v oboru "Telecommunication" [196]

### 3.2.3 Nízkoenergetické bezdrátové sítě dlouhého dosahu

Nízkoenergetické bezdrátové sítě dlouhého dosahu (LPWAN, z angl. Low Power Wide Area Network) se stávají novým trendem ve světě komunikačních technologií a senzorových sítí. Jsou to bezdrátové komunikační sítě pokrývající rozsáhlé geografické území - WAN (města, kraje, státy) za účelem připojení velkého počtu koncových zařízení. Mezi hlavní vlastnosti těchto technologií patří zejména: nízká energetická náročnost, cenová dostupnost koncových zařízení i služeb a malá datová propustnost. Tyto technologie se dále také vyznačují ve většině případů průměrným či spíše horším kryptografickým zabezpečením (složitější implementace vyšší úrovně zabezpečení) v porovnání s klasickými sítěmi.

Základní rozdělení LPWAN je dle podstaty pásma, v kterém komunikují, na

technologie komunikující: (i) v licenčním pásmu, a technologie komunikující (ii) v nelicenčním pásmu.

Nelicenční LPWAN technologie jsou technologie využívající nelicenční pásmo (v Evropě 868 MHz). V rámci ČR je toto pásmo spravováno pod ČTÚ (Český Telekomunikační Úřad). Pásmo se řídí dle oprávnění ČTÚ č. VO-R/10/05.2014-3 [197]. Z tohoto oprávnění vyplývají omezení pro zařízení komunikující v tomto pásmu převážně ve formě omezení vysílacího výkonu a délky doby, kdy je možné vysílat. V rámci technologií LPWAN v nelicenčním pásmu existuje poměrně velké množství technologií, mezi něž se řadí zejména:

- **Long Range Wide Area Network** (LoRaWAN), jedná se o širokopásmovou technologii založenou na modulaci LoRa a standardizovanou LoRa Alliancí (aktuálně open standard LoRaWAN R1.0, momentálně se hovoří o druhé verzi) [198]. Názory na to, zda je technologie proprietární či standardem, se liší. Problémem je, že technologie je založená na proprietární modulaci, avšak samotná WAN technologie postavená na této modulaci je standardem [199]. V ČR momentálně existují dva hlavní integrátoři (České Radiokomunikace a Things.cz). I přesto, že se jedná o technologii primárně určenou pro operátory, tak ji lze bez omezení využít i pro privátní sítě.
- **SigFox**, jedná se o úzkopásmovou technologii, globální síť, v ČR je momentálně integrátorem společnost SimpleCell spolupracující s T-Mobilem [200]. Jedná se o proprietární řešení firmy SigFox, nicméně se hovoří o budoucí standardizaci pod většími aliancemi jako 3GPP či ETSI [201].
- a celé řada dalších (Weigtless –W/–N/–P/–Neul , OnRamp, Tlensa, Amber Wireless, M2M Spectrum, aj. [202]), tyto technologie však parametricky odpovídají téměřbez výhrady technologii LoRaWAN (či SigFox), navíc jejich integrace v rámci Evropy je mnohem pomalejší než předchozí dvě technologie LoRaWAN a SigFox.

V rámci nelicenčních LPWAN technologií je tedy dostačující uvažovat technologie SigFox a LoRaWAN, jako hlavní zástupce technologií této kategorie. V rámci licenčních technologií LPWAN existuje velmi omezené množství technologií, které navíc v rámci Evropy zatím není možné používat, např. díky problémům s licencemi pásma, jedná se například o technologii SymphonyLink [203]. Parametry těchto technologií jsou navíc mnohdy pouze teoretické a není tedy možné je jednoznačně posoudit. Nejočekávanější technologií v rámci LPWAN je pak technologie NB-IoT (z angl. Narrowband Internet of Things), která je vyvíjena pod záštitou standardu 3GPP. NB-IoT je v tomto případě tedy hybridem, jelikož operuje na stejném principu jako celulární sítě a je i součástí 3GPP či využívá GSM/LTE spektra pro komunikaci [203].

Nicméně jinak jejich vlastnosti, trh a použití odpovídají oblasti LPWAN. Popišme si teď tedy jednotlivé technologie LoRaWAN, SigFox a NB-IoT z pohledu jejich vlastností a bezpečnosti:

- **LoRaWAN** zajišťuje důvěrnost pomocí algoritmů s velikostí parametrů 128 b (algoritmus AES-128, mód CTR) a autentizace probíhá pomocí AES-128 v módu CMAC. Nedostatkem v tomto případě je nevyřešený klíčový management [204]. Dalším problémem je v případě operátorem řízené sítě, stejně jako u celulárních sítí, nevyřešena kontrola nad klíči. Propustnost je u této technologie 0,3–50 kb/s, s možností obousměrné komunikace.
- **SigFox** řeší stejný bezpečnostní problém se správou klíčů, která je pod třetí stranou (operátorem). Technologie zajišťuje pouze autentizaci přenášených dat a to nepublikovanou technikou o neznámé délce parametrů [205]. Propustnost je u této technologie 100 b/s, s velmi omezenou možností obousměrné komunikace (obecně je komunikace u SigFox velice omezena na 140x 12 B zpráv pro odesílání a 4x 8 B zráv pro příjem).
- **NB-IoT** je tedy celulární technologie v oblasti LPWAN. Opět je zde problém se správou klíčů třetí stranou. Délka klíčů se předpokládá 128 bitů. Technologie by měla zajišťovat jak šifrování, tak i autentizaci dat. V případě 2G sítí se mají používat šifrovací/autentizační algoritmy GEA4/GIA4 (A5/4, postavené na šifře KASUMI) a GEA5/GIA5 (A4/5, postavené na šifře SNOW 3G). V případě LTE sítí se mají používat šifrovací/autentizační algoritmy 128-EEA1/128-EIA1 (postavené na šifře SNOW 3G), 128-EEA2/128-EEI2 (postavené na šifře AES) a 128-EEA3/128-EEI3 (postavené na šifře ZUC). Propustnost je u této technologie předpokládaná 35–170 kb/s (GSM) či 3–10 Mb/s (LTE), s obousměrným typem komunikace. Je nutno podotknout, že tento standard není prozatím dokončen a parametry jsou jen teoretické. Vycházet však lze z veřejně dostupných standardů definujících koncept CIoT („Cellular Internet of Things“), kde pro 2G sítě se jedná o dokument [206] (Annex H) a pro LTE sítě o dokument [207] („Control Plane CIoT EPS Optimisation“). Pro 3G sítě zatím rámec CIoT definován není. [206, 207].

Jak můžeme vidět v rámci LPWAN sítí je tedy největším problémem klíčový management a pokud uvažujeme operátorskou variantu, pak i tedy zajištění důvěrnosti, autenticity a dalších bezpečnostních principů pro uživatele. V rámci LPWAN technologií byla autorem také provedena řada evaluačních měření a analytických rešerší vhodnosti těchto technologií pro inteligentní sítě. Výsledky byly mj. publikovány na tuzemské uznávané odborné konferenci CK CIRED společně s firmou MEgA a E.ON [171, 172], a vhodnost LPWAN pro telemetrické systém diskutována v rámci

aplikace chytrého svozu odpadu v autorem publikovaném článku na mezinárodní vědecké konferenci CSNDSP 2016 indexované ve WoS/Scopus [208].

### 3.2.4 Rádiové technologie typu MESH

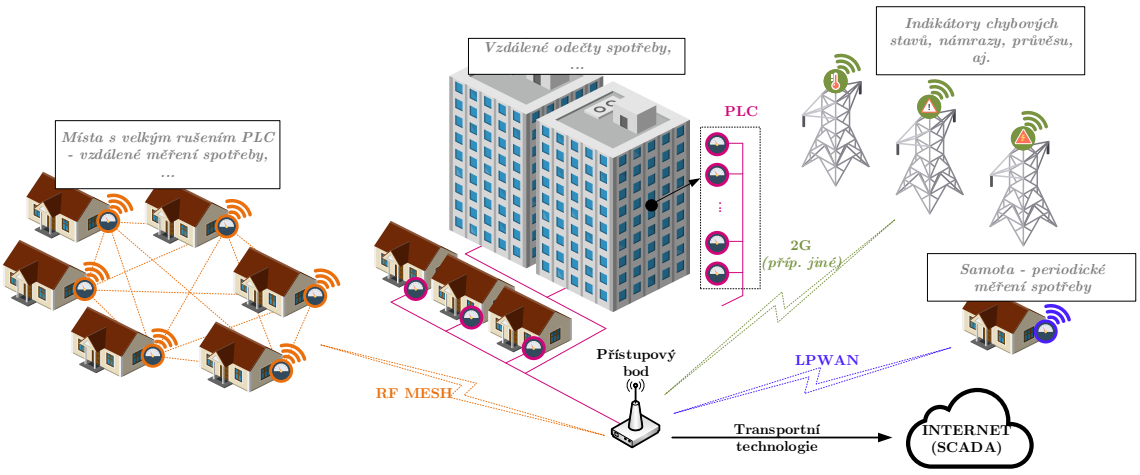
Rádiové technologie typu RF MESH (z angl. Radio Frequency MESH) jsou technologie, které používají rádiové prostředí pro komunikaci a topologii sítě MESH. Většina těchto technologií je proprietární a tak nelze přímo generalizovat vlastnosti této technologie. Nicméně jejich vlastnosti jsou si napříč spektrem velice podobné. Jedná se o vzájemně propojené komunikační body do topologie MESH s nízkou propustností i výpočetním výkonem, ale velkou energetickou efektivitou, kdy rozsah sítě bývá převážně MAN a uživatel buduje síť sám (nejedná se o operátorskou technologii jako v případě LPWAN či celulárních technologií).

Uvažujme např. technologii IQRF. Jedná se o technologii od firmy MICRORISC [209]. Klíče a parametry mají neznámou délku a jsou pod správou uživatele. Technologie zajišťuje pouze důvěrnost šifrováním proprietárním algoritmem. Velkým nedostatkem technologie je chybějící infrastruktura pro distribuci tajných klíčů, pokud bychom uvažovali více zařízení, bylo by již téměř nemožné pravidelně měnit tajné klíče v jednotlivých zařízení. Pokud navíc neuvažujeme prozatím neintegrovaný způsob šifrování pomocí AES-128, pak i důvěrnost není zajišťována bezpečným způsobem.

V rámci IQRF technologie byla provedena hloubková analýza vhodnosti této technologie pro inteligentní sítě, kde mj. byly posuzovány komunikační parametry technologie, ale i bezpečnost a soulad s dosavadními normami a legislativou. Výsledky byly publikovány na konferenci vážené tuzemské odborné konferenci v oboru CK CIRED 2016 [171, 172],

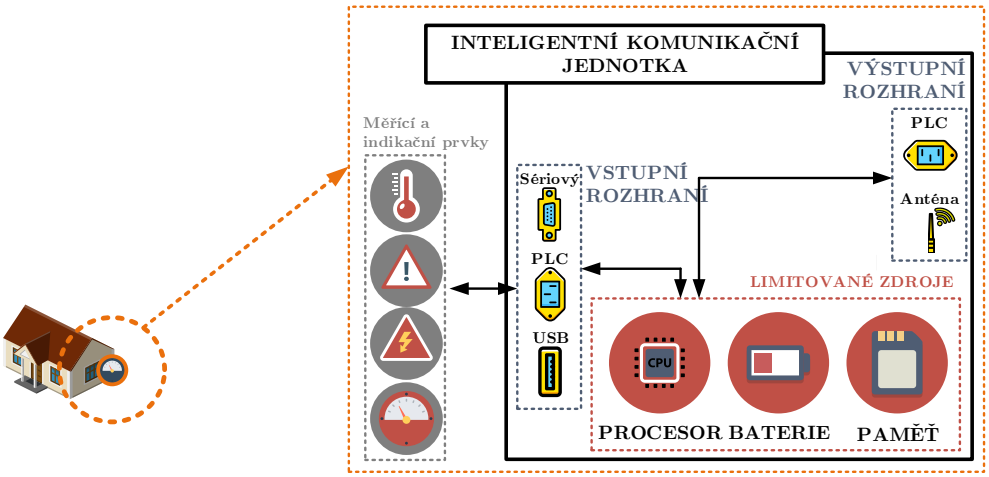
# 4 NÁVRH VLASTNÍHO HYBRIDNÍHO KRYPTOSYSTÉMU

V rámci kapitoly 1.1 byl na Obr. 1.1 definován základní model inteligentní sítě. V této práci se převážně věnujeme však pouze přístupové část, kde v kapitole 3.2 byly definovány nejpoužívanější komunikační technologie, tj. PLC či bezdrátové komunikační technologie (model inteligentní sítě, společně s diskuzí komunikačních možností, byly úspěšně publikovány autorem v impaktovaném časopise [183]). Výsledná přístupová část telemetrického systému (inteligentní sítě) je na zobrazena na Obr. 4.1.



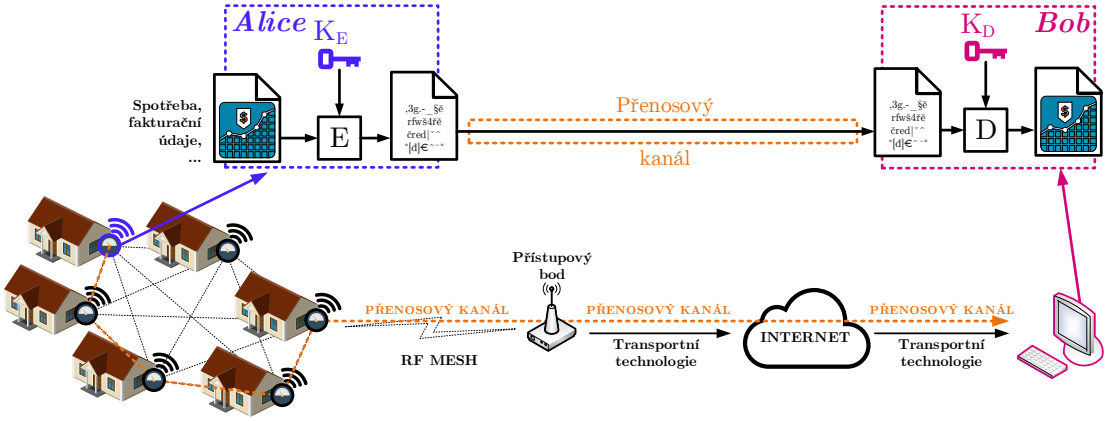

Obr. 4.1: Ukázka uvažované přístupové část inteligentní sítě.

Přístupový body je většinou tvořen data koncentrátorem, základnovou stanicí nebo bránou, kde na jednom konci je připojen do internetu (či dohledovému centru SCADA) a na druhém konci pak umožňuje připojení koncových prvků. Koncový prvek zde bude představovat indikátor, senzor či měřící zařízení připojené pomocí různých periferií např. USB, sériový port RS232/RS485, USB, aj. k výpočetní a komunikační jednotce opatřené anténou, mikroprocesorem, pamětí a baterií či trvalým napájením. Výkon mikroprocesoru i paměť bývají v těchto zařízeních omezeny, aby nedocházelo při velkém počtu zařízení k nadměrným netechnickým ekonomickým ztrátám, ale také z důvodu, že jsou tyto zařízení mnohdy pouze bateriově napájeny a je nutno u nich udržet životnost baterie v řádech jednotek let. Ukázka inteligentní komunikační jednotky je zobrazena na Obr. 4.2.




Obr. 4.2: Příklad inteligentní komunikační jednotky.

V rámci námi představovaného modelu přístupové části inteligentních sítě se dále z pohledu komunikačních technologií vyskytuje různá podoba vícecestné komunikace, kde je jí např. RF MESH, ale i například celulární sítě či sítě typu LPWAN, kde uživatel nemá navíc plnou kontrolu nad danou infrastrukturou a komunikační cestou. Pro zajištění informační bezpečnosti nebude uvažovat spojení bod-bod (P2P, z angl. point-to-point), ale konec-konec (E2E, z angl. End-to-end). Znamená to tedy, že například, i když v rámci RF MESH, LPWAN či celulární technologie jsou uvažovány komunikační skoky mezi jednotlivými zařízeními, ve výsledku se však bude jednat o jednu komunikační cestu z koncového prvku až do konečného serveru (např. dohledové centrum SCADA), viz Obr. 4.3.




Obr. 4.3: Příklad uvažovaného komunikačního řetězce pro zajištění informační bezpečnosti (na obrázku případ RF MESH).

Navržené řešení vychází z logiky definice bezpečnostních principů a tedy pro koho

(mezi kým) se zajišťují. V tomto případě je nutno zajistit bezpečnostní principy mezi Alicí (inteligentní jednotkou) a Bobem (dohledovým centrem, datovým úložištěm, cloudem, aj.). Komunikační spojení mezi Alicí a bobem je zde tedy mnohdy alespoň z části poskytováno třetí stranou a nebylo by tak možné s jistotou bezpečnostní principy zajistit pouze pro Alici a Boba. Pokud uvažujeme definované principy z kapitoly 1.2, pak dle tabulky 3.1 by teoreticky bylo možné řešit všechny definované principy algoritmy z oblasti asymetrické kryptografie s aditivními prvky pro zajištění čerstvosti dat. Nicméně jak ukazují např. práce [210, 211, 212], tak asymetrické algoritmy jsou oproti symetrickým algoritmům velice pomalé a to i při zachování stejně velkého klíče. Navíc jsou náročnější na velikost kryptografických parametrů (paměťová náročnost) i složitější (časová a výpočetní náročnost), viz kapitola 3.1. Z tohoto pohledu jsou tedy pro zařízení s limitovanými zdroji nevhodné. V rámci asymetrických algoritmů však dále existují ještě algoritmy s mnohem menšími nároky na velikost kryptografických parametrů, tedy algoritmy využívající eliptické křivky. Využití eliptických křivek pak zmenšuje náročnost na velikost kryptografických parametrů a dosahuje se tím v některých specifických oblastech (například generování či sestavení klíče) lepších výsledků než u klasických asymetrických algoritmů [213]. Avšak tyto algoritmy jsou vhodné pouze pro některé úlohy kryptografie (elektronický podpisy, přenos či dohoda klíčů) a není možné uvažovat např. pro šifrování [214]. Z těchto důvodů by bylo tedy vhodnější využít pro zabezpečení komunikace symetrické algoritmy. Ty však nezajišťují nepopiratelnost a čerstvost dat. Čerstvost dat musí být zajištěna separátně, u kteréhokoliv kryptografického algoritmu, a tak se nejedná o nevýhodu oproti asymetrickým algoritmům. Nezaručení nepopiratelnosti však může mít v rámci inteligentních sítí kritické dopady např. ve velkých ekonomických ztrátách, díky např. černým odběrům [215, 216, 217]. Nicméně největší nedostatek je pro symetrické algoritmy nutnost bezpečné distribuce tajných klíčů před započetím komunikace a šifrování. Je očividné, že zajištění všech definovaných bezpečnostních principů není primitivní úlohou a je nutné najít vhodnou i efektivní kombinaci všech kryptografických algoritmů.

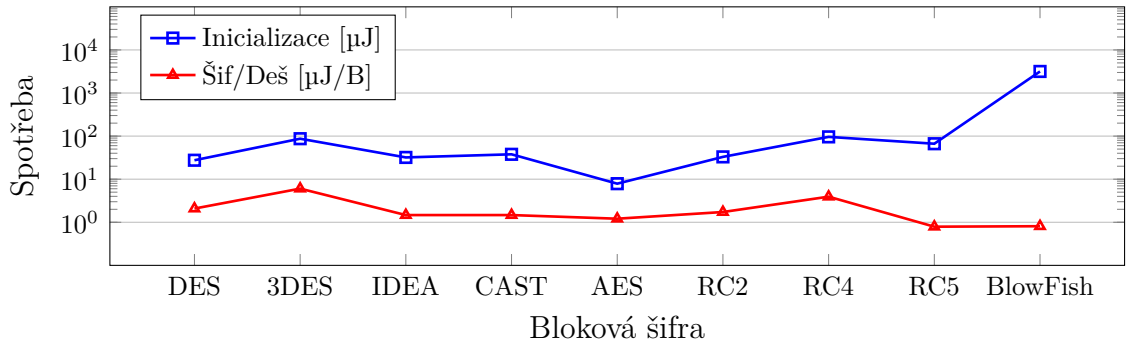
Tato kapitola se dále věnuje návrhu dílčích částí vlastního hybridního kryptosystému z pohledu jednotlivých definovaných bezpečnostních principů: (i) důvěrnost (Kapitola 4.1), (ii) integritu (Kapitola 4.2), (iii) autenticitu (Kapitola 4.3), (iv) nepopiratelnost (Kapitola 4.4) a (v) čerstvost dat (Kapitola 4.5). V neposlední řadě v kapitole 4.6 je následně představen kompletní vlastní návrh hybridního kryptosystému.

## 4.1 Evaluace a výběr řešení k zajišťení důvěrnosti

Jeden z nejklíčovějších nástrojů pro zajištění důvěrnosti je v současné době šifrování (viz kapitola 3.1). V rámci šifrovacích algoritmů jsou známy symetrické algoritmy a klasické asymetrické algoritmy (eliptické křivky momentálně není možné pro šifrování uvažovat [214]). Jelikož tedy není možné uvažovat asymetrické algoritmy, pak je nutno důvěrnost zajistit některým symetrickým algoritmem. Jak jsme si již uvedli v kapitole 3.1, tak existují dva základní druhy symetrických algoritmů [125]: (i) proudové, a (ii) blokové.

Jak jsme si uvedli, tak proudové algoritmy jsou obecně rychlejší jak blokové, nejsou tolik náchylné na chyby v přenosu a potřebují i mnohem méně paměti [127]. Inteligentní sítě jsou však z pohledu bezpečnosti velice náročná oblast a proudové šifry jsou nejen náročné na samotnou správnou implementaci, ale poskytují bohužel pouze důvěrnost bez možnosti zajistit integritu či autenticitu [124]. V neposlední řadě jsou proudové šifry vhodné spíše do oblasti kontinuálních toků a nikoliv do oblasti periodicky zasílaných zpráv [127]. Vhodnější jsou v tomto případě tedy algoritmy blokové.

Z analýzy symetrických algoritmů [218] plyne, že AES (Advanced Encryption Standard) je jeden z výpočetně i paměťově nejefektivnějších symetrických algoritmů a také algoritmus s nejvyšší bezpečností bez (prozatím) žádné známé slabiny (tedy v porovnání s ostatními nejznámějšími symetrickými algoritmy jako např. DES, 3DES, Blowfish, IDEA, TEA, CAST5, AES, RC6, Serpent, Twofish a MARS). Potvrzují to i rozsáhlá měření v [219], kde jejich shrnutí můžeme vidět na Obr. 4.4




Obr. 4.4: Srovnání jednotlivých blokových algoritmů z pohledu energetické náročnosti (data převzata z [219]).

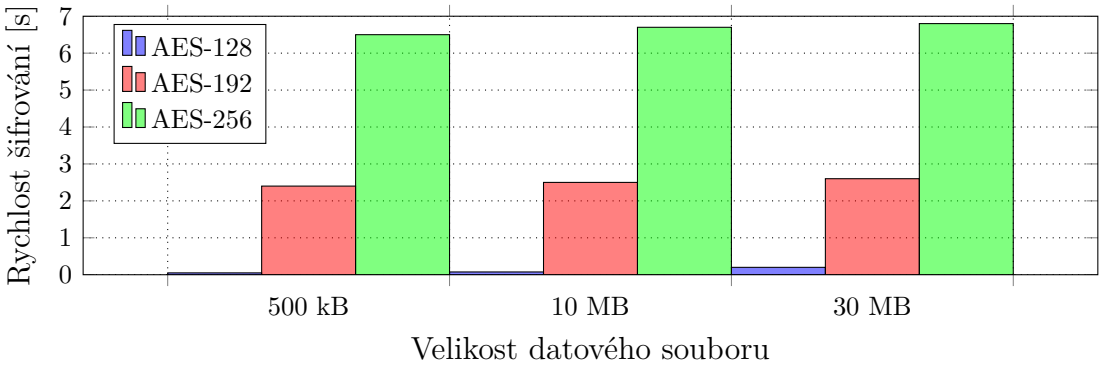
Jak můžeme vidět tak v rámci inicializace je AES algoritmus nejefektivnější (nastavení inicializačního vektoru, aj.), kde navíc při procesu šifrování či dešifrování, pokud neuvažujeme velké objemy dat (RC5/Blowfish) se jeví také jako jeden z nejefektivnějších algoritmů. AES standardizuje parametry pro symetrický blokový

algoritmus Rijndael. Rijndael algoritmus byl standardizován institutem National Institute of Standards and Technology (NIST) jako AES v roce 2001, kdy vyhrál veřejnou soutěž o náhradní algoritmus za tehdy již nebezpečný algoritmus Data Encryption Standard (DES) [220]. Algoritmus AES byl mj. v roce 2002 dále schválen jako federální standard pro utajené informace v USA. Dále je AES doporučován řadou národních i mezinárodních standardů [123, 131, 132, 109]. Z výše uvedených důvodů tedy uvažujeme pro zajištění principu důvěrnosti jako nejvhodnější symetrickou blokovou šifru AES, která bude dále blíže popsána v následující kapitole. Existují základní tři typy algoritmu AES-$n$ dle délky soukromého klíče $K_S$, kde $n$ je délka klíče 128, 192 či 256 bitů (tedy AES-128, AES-192 a AES-256). Tabulka 4.1 ukazuje předpokládanou dobu, do kdy jednotlivé typy AES budou bezpečné.

Tab. 4.1: Bezpečnost jednotlivých typů algoritmu AES (data převzata z [221]).

| **Algoritmus** | **Rok** | **Vysvětlení** |
|---|---|---|
| AES-128 | $>$ 2030 | Dostačující min. 20 let po roce 2030 |
| AES-192 | $\gg$ 2030 | Dostačující min. 40 let po roce 2030 |
| AES-256 | $\ggg$ 2030 | Dostačující v daleké budoucnosti po roce 2030 |

AES-128 by měl být dostatečný v blízké budoucnosti, nicméně delší klíče nabízí vyšší bezpečnost. V rámci výběru klíče byl proveden vlastní test porovnáním časové náročnosti šifrování jednotlivými velikostmi klíčů. Pro účely testování byly vytvořeny tři textové soubory o velikostech 500 kB, 10 MB a 30 MB. Velikost těchto souborů byla odvozena na základě analýzy komunikace PQ monitoru [222], který měří parametry kvality napětí v nn, vn i vvn sítích dle ČSN EN 50160 [223]. Analýza byla provedena pomoci programu Wireshark. Při analýze dat se lze setkat s daty malých velikostí (jednotky až stovky kB) až po velké velikosti (jednotky a desítky MB). Na základě této analýzy byl prvním testovaným souborem malý soubor o velikosti 500 kB, který slouží k testu spojení mezi měřicím přístrojem a PC. Dalším testovaným souborem (10 MB) byl soubor se záznamem kvality elektrické energie získaný při krátkodobém měření. Posledním testovaným soubor byl soubor o velikosti 30 MB se záznamem kvality elektrické energie získaný při dlouhodobém měření. Pomocí programu Cryptool 2.0 [224] byl pak sestaven komunikační model pro testování algoritmu AES. Pro různé délky klíče bylo provedeno šifrování a dešifrování všech tří textových souborů, přičemž byla měřena doba, za kterou AES zvládne šifrování. Program CrypTool 2.0 je schopen měřit tuto dobu s přesností na 1 ms. Testování probíhalo na PC s procesorem Intel s frekvencí 1600 MHz a s 1 GB RAM pamětí. Pro přesnější výsledky bylo každé měření provedeno třikrát a následně byl vypočítán medián těchto měření, viz Obr. 4.5.




Obr. 4.5: Srovnání časové náročnosti šifrování pro jednotlivé velikosti klíčů.

Jak můžeme vidět časová náročnost větších klíčů než je AES-128 je zcela jednoznačně mnohonásobně vyšší a tak z pohledu zařízení s limitovanými zdroji bude nejefektivnější využít AES-128. Odborné práce se dnes také zaměřují převážně na algoritmus AES-128, který by měl být dostačující do blízké budoucnosti (viz Tab 4.1). Tyto práce se snaží o minimalizaci vyzařovaného výkonu zařízení (což by mělo zabránit útoku postranními kanály) a také o optimalizaci některých z vnitřních výpočetně či paměťově náročných operací [210, 211, 212]. Novodobý výzkum se zabývá dále hardwarovou optimalizací AES a vytvářením mikročipů či aditivních speciálních zařízeních pro algoritmus AES ([225, 226, 227]), které jsou optimalizovány právě pro algoritmus AES-128. K daným zařízením však již chybí techniky na výměnu klíčů či popis jakým způsobem klíče doručovat. Je to z toho důvodu, že většina těchto čipů je integrována do nelimitovaných zařízeních či větších celků, kde výměnu klíče aj. úkony řeší jiné zařízení či jiná část (nebo se výměna klíčů neuvažuje). Z tohoto pohledu se pak jedná o pouze částečná řešení, kdy v rámci uvažované části inteligentních sítí nelze aditivní zařízení na každý úkon v rámci inteligentní komunikační jednotky (viz úvodní kapitola).

Softwarovou implementaci a optimalizaci pak řeší některé další práce ([228, 229, 230]), které však mají nejednotné měřící postupy, jejich výsledky nejsou jednoznačné a tedy nejsou zcela porovnatelné. Některé z nich uvádějí rychlosti pouze dílčích částí, nicméně komplexní měření hlavních funkcí chybí, nebo je nejednoznačná frekvence procesoru či co znamenají jednotlivé cykly (zda jsou to cykly procesoru, kroky či pouze jednotlivé operace). Dále není zcela jasné, zda se tyto práce soustředili na optimalizaci pro paměť, rychlost či bezpečnost. Nicméně většina z nich s jistotou prokazuje funkčnost a vhodnost algoritmu AES na zařízeních či mikrokontrolérech s limitovanými zdroji.

### 4.1.1 Algoritmus Advanced Encryption Standard

Advanced Encryption Standard (AES) je tedy standardem, který vznikl v roce 2001 a nahradil standard DES (standard AES byl popsán v dokumentu FIPS-197) [220]. Jedná se tedy také o symetrický blokový algoritmus, který je dnes již velice často používaný v celé řadě oblastí [220]. Používá se délky bloku $m = 128\,b$, délka klíče je pak volitelná (volí se z klíčů o délce 128 bitů, 192 bitů či 256 bitů) a počet rund závisí na vybrané velikosti klíče (pro vypsané klíče tedy 10, 12 či 14 rund). AES používá matici 4x4 byty (tzv. stav), těleso $GF\left(2^8\right)$:

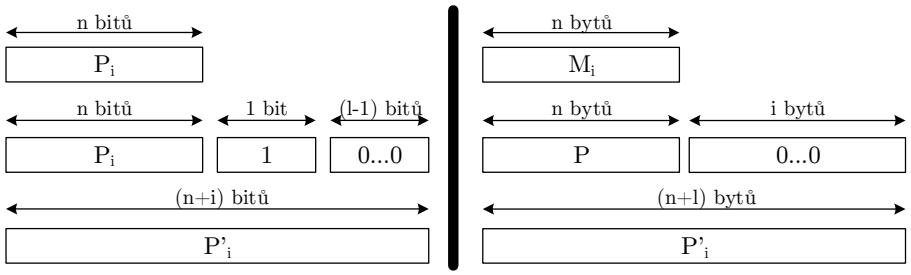
$$g\left(x\right) = \left(x^8 + x^4 + x^3 + x^1 + 1\right). \tag{4.1}$$

Velikost klíče určuje také bezpečnost daného systému, ale i paměťovou a výpočetní náročnost. Počet samotných iterací pak také ovlivňuje bezpečnost šifry, kdy mezi nejznámější útoky na Rijndaelův algoritmus (nestandardizovaná verze AES) pak patří útoky, kdy bylo použito 7 iterací se 128-bitovými klíči, 8 iterací se 192-bitovými klíči a 9 iterací s 256-bitovými klíči) [231]. AES však používá pevně dané parametry [220]. Parametrizace AES je znázorněna v tabulce 4.2.

Tab. 4.2: Parametrizace AES (počítáno v 32-bitových slovech) [220].

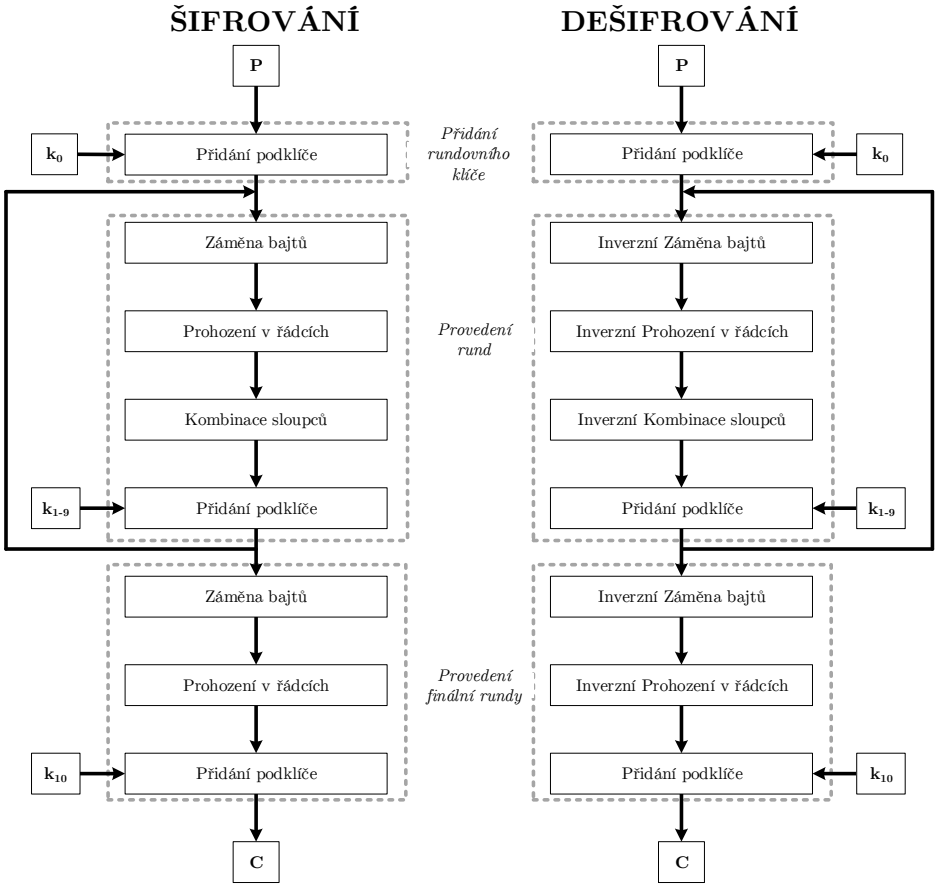
| **Algoritmus** | **Velikost klíče** ($N_k$) | **Vstupní a výstupní blok** ($N_b$) | **Počet rund** ($N_r$) |
|---|---|---|---|
| AES-128 | 4 | 4 | 10 |
| AES-192 | 6 | 4 | 12 |
| AES-256 | 8 | 4 | 14 |

Parametr $N_k$ značí počet 32-bitových slov samotného k-bitového klíče (například tedy $N_{128} = 4$). Vstupní blok otevřeného textu je pak vždy stejný tedy $N_b = 128$ bitů (tedy čtyři 32-bitové bloky). Počet iterací je pak jasně znázorněn pomocí parametru $N_r$. Pokud by např. poslední blok již neměl 128 bitů, dochází pak k tzv. padingu neboli doplnění (pouze pro určité módy, např. CBC či ECB), tedy bitovému (bajtovému) doplnění, viz Obr. 4.6.




Obr. 4.6: Ukázka techniky padingu, vlevo bitového doplnění a vpravo bajtové doplnění.

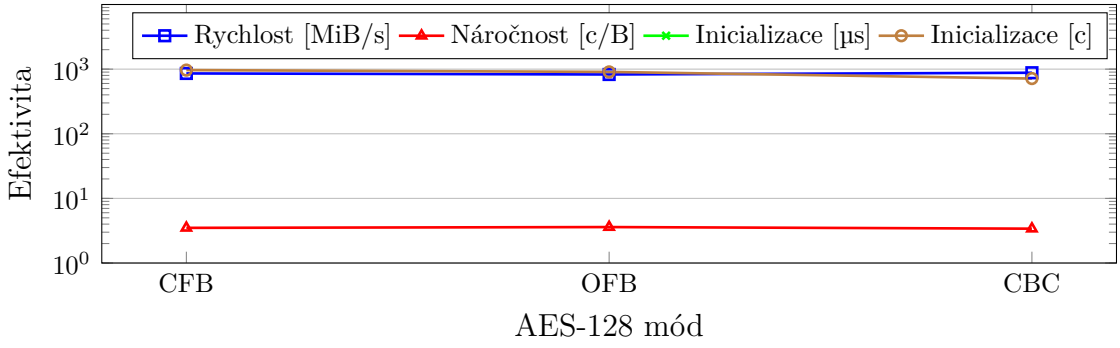
Jak můžeme vidět, existují tedy dva druhy padingu, tedy (i) doplňování bajtů a (ii) doplňování bitů. Pading i výběr typu záleží na dané implementaci, kdy např. můžeme zprávy doplňovat o kontrolní součet, apod. Funkčnost algoritmu AES je pak znázorněna přehledně na Obr. 4.7.




Obr. 4.7: Ukázka základního principu symetrického blokového algoritmu AES.

Popis jednotlivých bloků a operací využívaných v AES lze nalézt ve standardizaci v [220]. V rámci symetrických blokových algoritmů je pak nutno zvolit samozřejmě vhodný mód. Většina známých módů byla přiblížena v rámci kapitoly 3.1.3, tedy ECB, CTR, CFB, OFB a CBC společně s módy autentizačního šifrování CCM, EAX, GCM či OCB. Uvažujme nejdříve klasické symetrické blokové módy, vycházejme z odborných analýz [232, 233, 234]. Prvně tedy mód ECB, tento mód je nejjednodušší a nejrychlejší. Nicméně převádí stejný blok otevřeného textu vždy na stejný blok šifrovaného textu (šifrovaný text není náhodný), což může mít za následek narušení důvěrnosti jen pouhým odposlechem. Některé práce proklamují tento algoritmus za ideální šifrovací mód [235], nicméně mód ECB byl již mnohokrát úspěšně napaden, viz např. [236, 232] a současný názor považuje tento mód za nevhodný pro klasickou

komunikaci. Tento algoritmus je tedy spíše vhodný tam, kde otevřený text má charakter náhodných dat, nikoliv pro šifrování klasických dat, kde tedy může docházet k opakujícím se řetězcům a následně i narušení důvěrnosti. Mód CTR převádí blokový algoritmus na proudový a je vytvořen převážně pro multi-procesorové zařízení, tedy kde mohou být jednotlivé bloky šifrovány paralelně. Nicméně v rámci inteligentních sítí a oblasti telemetrických systému využívajících zařízení s limitovanými zdroji nelze uvažovat multi-procesorová zařízení či tzv. multi-tasking (zpracování více úloh naráz) na straně inteligentní jednotky. Zůstávají tak módy CFB, OFB a CBC, kde módy CFB a OFB si velice podobné, také převádí blokový algoritmus na proudový. Tyto módy se hodí spíše na hardwarovou implementaci a i jejich výkonnost je pak hardwarově závislá, což v rámci interoperability a uvažovaného velkého počtu různých zařízení není vhodné. Příkladem můžou být i naprosto odlišné výsledky v rámci dvou analýz módu CTR, kdy jedna proklamuje na specifickém hardwaru nejlepší výsledky ze všech módů [237] a druhá naopak podprůměrné výsledky srovnatelné s ostatními módy [238]. Pokud navíc srovnáme obecně rychlost a efektivitu módů OFB, CFB a CBC, pak CBC vykazuje srovnatelné výsledky (viz např. rozsáhlé výkonnostní testy Crypto++ [239] provedené na 3,1 GHz procesoru šesté generace Skylake a 64-bitovém operačním systému Fedora, shrnutí viz Obr. 4.8).




Obr. 4.8: Srovnání výkonnosti módů CFB, OFB a CBC (data převzata z [239]).

Všechny uvažované módy (CTR, CFB, OFB i CBC) jsou náchylné na tzv. malleable útoky, kdy útočník může využít jakékoliv $t$ a vztahu:

$$E\left(P\right) \oplus t = m \oplus t \oplus K_S = E\left(m \oplus t\right), \tag{4.2}$$

k následnému částečnému odkrytí otevřeného textu a možnosti ho dle potřeby změnit, např. “Spotřeba pro byt #2A je 0005,12 kWh” na “Spotřeba pro byt #2A je 5000,12 kWh”, apod. Navíc je velice lehké manipulovat s otevřeným textem tak, aby útočník docílil cíleného efektu. Tento nedostatek však můžeme jednoduše řešit kvalitní autentizací. V neposlední řadě mód CBC je považován za jeden z nejbezpečnějších

módů z výše uvedených, což je to i díky faktu, že výsledný šifrovaný text má náhodný charakter díky využívání předchozích bloků při šifrování, více jak jedna zpráva může být šifrována stejným klíčem a pokud je poskytnuta kvalitní autentizace, jedná se o velice efektivní algoritmus pro šifrování. Z tohoto pohledu je tedy z námi uvažovaných klasických módů nejvhodnější mód CBC.

Autentizační šifrování na druhé straně by řešilo nejen problém s důvěrností, ale zároveň i s integritou a autentizací. Vycházejme např. z [240], srovnání jednotlivých módu pak můžeme vidět v Tab. 4.3.

Tab. 4.3: Srovnání jednotlivých módu autentizačního šifrování v cyklech na bajt (data převzata z [240]).

| **Algoritmus** | **Velikost zprávy [B]** | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | 16 | 20 | 40 | 64 | 128 | 256 | 1024 | 8192 |
| OCB | 118,91 | 125,63 | 78,29 | 58,87 | 48,83 | 43,85 | 39,87 | 38,77 |
| CCM | 161,47 | 181,57 | 116,26 | 87,59 | 76,24 | 70,74 | 66,48 | 65,25 |
| EAX | 227,90 | 235,43 | 145,21 | 105,38 | 85,01 | 75,12 | 67,52 | 65,20 |
| GCM (4 kb) | 166,41 | 188,57 | 119,49 | 90,27 | 79,17 | 79,17 | 69,04 | 67,73 |
| GCM (8 kb) | 154,41 | 154,41 | 154,41 | 82,91 | 82,91 | 67,06 | 65,29 | 61,46 |
| GCM (64 kb) | 118,91 | 125,63 | 78,29 | 58,87 | 48,83 | 43,85 | 39,87 | 38,77 |

Měření proběhlo na zařízení s procesorem AMD Athlon 2500+ (Barton) a ukazuje, jakým způsobem byly jednotlivé algoritmy schopny zpracovávat různě velký otevřený text (data). Rychlost je pak uváděna v cyklech na jeden bajt (c/B), tedy nižší hodnota je rychlejší algoritmus (spotřeba méně cyklů na zpracování jednoho bajtu). Z porovnání plyne nejrychlejší mód OCB, ten mód je obecně považován za nejefektivnější i dalšími prameny např. [241], bohužel tento mód je zatížen patentem [242]. Díky problémům s poskytováním licence u módu OCB, byla vytvořena jeho nelicencovaná verze CCM, bohužel jak můžeme vidět, tak je znatelně pomalejší. Ideálním algoritmem by z pohledu rychlosti byl algoritmus GCM, ten však pro rychlejší chod potřebuje 64 kB paměti a více, navíc využívá Galoisova pole $F^{128}$ (místo 127 bitového celočíselného pole) a modulárních operací pro polynomiální hašovací funkci [243]. To klade nároky nejen na paměť, ale také hardwarovou strukturu a výpočetní výkon (z pohledu paměťových nároků je mód GCM ze všech uvažovaných módů nejnáročnější [241]). Z tohoto pohledu tedy GCM není vhodný pro obecné použití na limitovaných zařízeních, protože jeho efektivita je silně hardwarově závislá. Mód EAX je spíše vhodnější na větší datové toky, kde již od 128 B začne být srovnatelně výkony s módy CCM a GCM, pro malé datové toky je neefektivní a velice pomalý. V neposlední řadě mód CCM, jedná se o mód kombinující jednoduchý mód CTR s CBC-MAC ve variantě MtE (tedy nejdřív provede MAC a následně šifruje). MAC pak může mít velikost 4, 6, 8, 10, 12, 14 nebo 16 bajtů. Nevýhodou je, že CTR mód je vytvořen převážně na multi-procesorové zařízení, což není případ námi uvažované

oblasti inteligentních sítí a zařízeních s limitovanými zdroji. Dále pak metoda MtE není zatím prokazatelně bezpečná a není považována za zcela bezpečnou [244], i když mnoho implementací tento mód využívá v reálných podmínkách [245]. V neposlední řadě CBC-MAC není bezpečný, pokud není délka zpráv fixní, toto může být vyřešeno jednoduše např. padingem [246]. Nicméně dvě za sebou jdoucí zprávy by spolu neměly ani souviset [247], což u periodických měření či obecně telemetrických sítí, kde data mají stejný charakter nelze zcela dodržet. Tedy z pohledu důvěrnosti se jeví jako nejlepší varianta mód CBC (AES-128-CBC), pokud pokud bychom však našli bezpečnou a efektivní náhradu autentizace vůči AE (jinak je nutno použít mód AES-128-CCM a zajistit efektivní pading a ochranu proti známým útokům).

Hlavní nevýhodou symetrického algoritmu AES však zůstává, jako u všech symetrických algoritmů, nutnost řešit distribuci tajného klíče. Z aktuálních doporučení [221] plyne, že symetrické klíče by se měly měnit v periodě 1–3 let, kdy hranice 2 (3) roky se považuje za hraniční a nedoporučuje se. S každoroční rostoucí teoretickou maximální výpočetní silou pak dle těchto doporučení je nutno zvážit zmenšení periody. Při uvažovaném hromadném sběru dat ze stovek až tisíců inteligentních jednotek je nemožné, aby byl tajný klíč měněn fyzickým zásahem do jednotky. Z tohoto důvodu je nutno uvažovat o elektronické distribuci klíčů. Pokud uvažujeme tedy velké počty zařízení, která mají být nasazeny na jednotky let, je nutno u nich vytvořit efektivní systém klíčové distribuce (výměny klíčů), čímž se tedy dále zabývá následující kapitola.

### 4.1.2 Distribuce symetrického soukromého klíče

U symetrického algoritmu AES je tedy, jako u každého symetrického algoritmu, nutno vyřešit distribuci či sestavení klíče. K tomu máme několik možností, vytvoření separátního bezpečného kanálu, využití certifikačních autorit, využití asymetrického algoritmu nebo využití asymetrického algoritmu s eliptickými křivkami. Separátní kanál je nevhodný kvůli množství uzlů, kdy navíc např. při využití PLC bychom odstranili jednu z velkých výhod, tedy kdy nejsme nuceni vystavovat nové infrastruktury. Asymetrické algoritmy jsou velice výpočetně náročné a také paměťově náročné (viz kapitola 3.1.4), je tedy vhodnější se zabývat spíše asymetrickými algoritmy využívající eliptické křivky.

Použití eliptických křivek v kryptografii se datuje k roku 1986, kdy Victor S. Miller [157] a posléze nezávisle na sobě i Neal Kobliz v roce 1987 [156] poprvé navrhli jejich použití, nicméně k velkému rozšíření eliptických křivek v kryptografii došlo až později v letech 2004 až 2005, kdy byla vydána tzv. Suite B organizací NIST [248], kde bylo doporučeno používat převážně algoritmů využívající eliptických křivek, kde pro výměnu klíče tedy algoritmu Diffieho-Hellmana s využitím eliptických křivek

(Elliptic Curve Diffie Hellman - ECDH) a pro elektronický podpis algoritmu Digital Signature Algorithm s využitím eliptických křivek (ECDSA).

Uvažujme tedy pro dohodu klíčů doporučený algoritmus ECDH. Tento algoritmus lze popsat následujícími kroky:

1. Mějme opět dva účastníky Alici a Boba, jeden z nich vygeneruje velké prvočíslo $p$; základní (generující) bod $G[x_G; y_G]$; koeficienty $a, b$, tak aby splňovali diskriminant $\Delta = 4a^3 + 27b^2 \neq 0 \pmod{p}$; následně dle volby křivky je nutno zvolit ještě také další doménové parametry tj. řád bodu $G$ $n$, kofaktor $h$ a případně neredukovatelný polynom $f(x)$, pokud se jedná o křivku řádu 2. Tyto parametry mohou být následně veřejně sdíleny s druhým účastníkem.

2. Následně každá strana zvolí svůj privátní klíč, Alice $K_{E_a} = d_a$ a Bob $K_{E_b} = d_b$, kde $d_a$ a $d_b$ jsou náhodně volená celá čísla z intervalu $[1, 1 - n]$. Dále obě strany počítají svůj veřejný klíč, Alice $K_{D_a} = Q_a = dG$ a Bob $K_{D_b} = Q_b = dG$. Poté jsou zveřejněny veřejné klíče $Q_a$ a $Q_b$.

3. Alice i Bob můžou počítat sdílené tajemství $(x_k, y_k)$. Alice jako $(x_k, y_k) = d_a Q_b$ a Bob jako $(x_k, y_k) = d_b Q_a$. To je umožněno díky vzájemnému vztahu $d_A Q_B = d_A d_B G = d_B d_A G = d_B Q_A$.

4. V neposlední řadě sdílené tajemství $(x_k, y_k)$ může být využito např. jako tajný symetrický klíč (nejčastěji se využívá $x_k$). Ten je možné použít buď přímo či ještě z něj vytvořit haš pro zvýšení bezpečnost [249].

Algoritmus ECDH zajišťuje dohodu klíče přes nezabezpečený kanál [250, 251, 248]. Dle námi vybraného algoritmu pro zajištění důvěrnosti AES-128 bude nutné uvažovat o křivkách o velikosti 256 b (viz Tab. 3.4). Novinkou v rámci kryptografie eliptických křivek je pak zcela nová křivka Curve25519 od Daniela Bernsteina [252], která dosahovala v různých implementací vysokých rychlostí (v rámci velikost 256 b). Zjednodušení a zrychlení je také díky vypuštění souřadnice $y$, tedy využívá se pouze souřadnice $x$ a $z$ [253]. Tato křivka vychází z tzv. Edwardových křivek (Ed25519) [254], jedná se o nejrychlejší eliptické křivky prvočíselného řádu [255]. Curve25519 je tedy křivka prvočíselného řádu (Elliptic Curve over finite field, $\mathbb{F}_p$), nicméně prozatím nebyla žádnou organizací ověřena či prokázána její bezpečnost a ani nebyla žádnou organizací standardizována. Křivky s prvočíselným řádem by měly být rychlejší na procesorech s hardwarovou násobičkou oproti křivkám o řádu 2, které jsou na druhou stranu rychlejší v hardwarových implementacích, díky jejich jednoduchosti. ECDH je doporučován také mnoha dalšími standardy [256, 257, 248], které doporučují užití již ověřených křivek s ověřenými parametry, z tohoto důvodu není uvažována nejnovější křivka Curve25519, ale pouze soubor standardizovaných křivek.

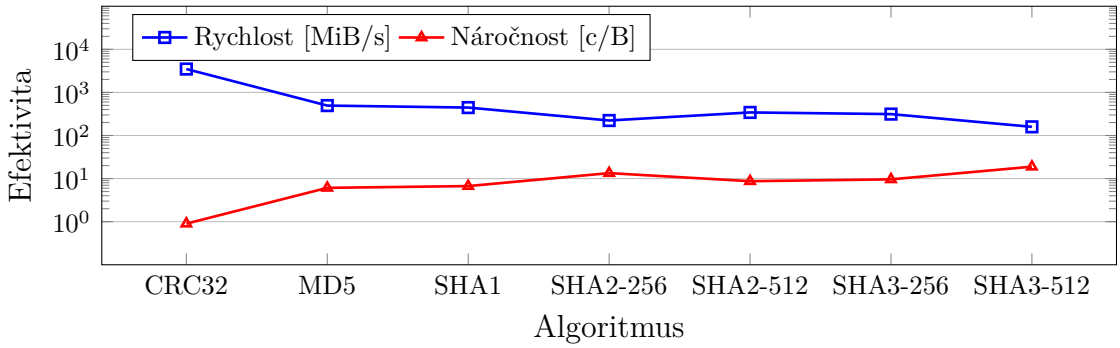
Eliptické křivky jsou podrobně matematicky popsány, implementace známých

křivek je řešena v mnoha pracích, hlavně tedy z důvodu, že se jedná o velmi aktuální problematiku. V této oblasti však chybí bližší popis výběru parametrů křivek, generování nových křivek, vliv parametrů na entropii či jejich bezpečnost obecně. Dále pro limitovaná zařízení chybí dostatek řešení, které by dosahovala velikost klíče 256 bitů, která je dnes společně s algoritmem AES-128, vyžadována většinou standardů v běžných oblast. Problematikou efektivní implementace křivek o velikosti 256 bitů se zabývá pouze několik prací [258, 259, 260, 261, 262], kde práce [258, 259] se zabývají pouze jedinou křivkou Curve25519 a ostatní tři pak obecnou implementací křivek do limitovaných zařízeních (v těchto pracích však chybí hlubší popis měření a výsledků, paměťové nároky či propojení implementace s nějakým dalším algoritmem do hybridního kryptosystému). Implementace větších křivek než je 256 bitů již, dle současného přehledu autora, řešena na limitovaných zařízeních doposud není.

## 4.2 Evaluace a výběr řešení k zajišťení integrity

V rámci zaručení integrity se dá uvažovat o několika algoritmech [127]: (i) kontrolní součet, (ii) cyklický redundantní součet (CRC), (iii) haš funkce (popř. kryptografická haš funkce), (iv) MAC kód (popř. HMAC). Typ dat v našem případě představuje velmi malé bloky dat, které obsahují většinou měřící údaje, či pouhé stavové informace (1/0). Dále je v našem scénáři použito limitovaných zařízení, které mají limitovanou paměť, ale i výkon a je tedy nutno poskytnout zabezpečení resp. naplnění jednotlivých principů, co nejrychleji. V rámci vybraného šifrovacího algoritmu máme min. 128 b blok dat, kdy je možné předpokládat doplnění bloku pomocí padingu aditivními informacemi. Pokud uvažujeme první způsob tedy kontrolní součet, tak se jedná o nejjednodušší způsob ochrany integrity dat [124]. Jedním ze základních příkladů kontrolního součtu je např. zaslání kopie dat, kdy následně příjemce může obě zprávy porovnat na změnu (spočítat změnu). Tato metoda je však silně redundantní (přenáší se dvojnásobný počet dat, jen pro zajištění integrity) a není vhodná do reálných komunikačních podmínek. Z tohoto důvodu se využívá matematických metod, jako například bitového součtu apod. Tato jednoduchá metoda však zabrání pouze velice specifickým chybám, která navíc byli zapříčiněny chybou přenosu, nikoliv sofistikovaným aktivním útokem na integritu dat [125]. Např. mějme zprávu 0x0002 (hexadecimální zápis), její kontrolní součet je 0x02, pokud změníme jednotlivé bajty na 0x0101 či 0x2000, tak kontrolní součet zůstane stejný. V tomto případě nejsme schopni odhalit chybu a budeme považovat zprávu za validní. Jedná tedy o velice jednoduchou ukázku, jak je bezpečnost kontrolního součtu nedostatečná při zaručování integrity vůči již jednoduchým chybám či útokům. Pokud uvažujeme CRC a haš funkce, lze obecně říci, že CRC jsou jednodušší, rychlejší a méně bezpečné a haš funkce naopak [124]. Nicméně při bližším pohledu není tento pohled zcela správný a pravdivý.

Kontrolní součty jsou obecně navrženy jako ochrana proti chybám přenosu, nikoliv proti sofistikovaným útokům na integritu. Velice podobně byly vyvinuty haš funkce, které měly sloužit např. pro rychlé prohledávání rozsáhlých databází apod., kdy se z relativně velkých objemů dat tvořil relativně malý unikátní haš [125]. Tedy lze tvrdit, že CRC mohou být použity jako jednoduchá haš funkce. Kryptografické hašovací funkce na druhou stranu jsou tvořeny jako jednosměrné funkce a tedy i přesto, že útočník získá samotný haš, není jednoduše schopen z něj získat žádné další aditivní informace (viz kapitola 3.1.2), což u CRC lze, protože se o jednosměrnou funkci nejedná. Dnes některé hašovací algoritmy jsou již považovány za nebezpečné např. MD5 či SHA-1 a je nutno je šifrovat společně se zprávou [263, 264, 265, 266, 267]. Doporučuje se tedy používání bezpečnější algoritmů jako např. SHA-2, který však již dnes také vykazuje značné nedostatky a je možné jej reálně napadnout [268, 269], tedy i verzi SHA-512, která používá výsledný 512 bitový haš [270]. Navíc CRC ani haš nebrání útočníkovi zprávu i haš následně změnit (pokud nejsou přenášeny šifrovaně), protože hašovací algoritmy i CRC algoritmy jsou veřejně známy. Z tohoto důvodu je nutno u všech těchto algoritmů použít šifrování. Dále pak jelikož uvažujeme limitovaná zařízení a malé objemy dat, není vhodné uvažovat komplexní a složitější haš funkce, které navíc tvoří redundantní data (pokud šifrujeme malé objemy dat např. 128 b, tak u SHA-512 bude výsledný haš vždy 512 b) a jsou znatelně pomalejší, viz Obr. 4.9 (CRC vykazuje nejrychlejší generování MiB a potřebu nejméně cyklů na vygenerovaný bajt c/B).




Obr. 4.9: Srovnání jednotlivých algoritmů pro zajištění integrity (data převzata z [219]).

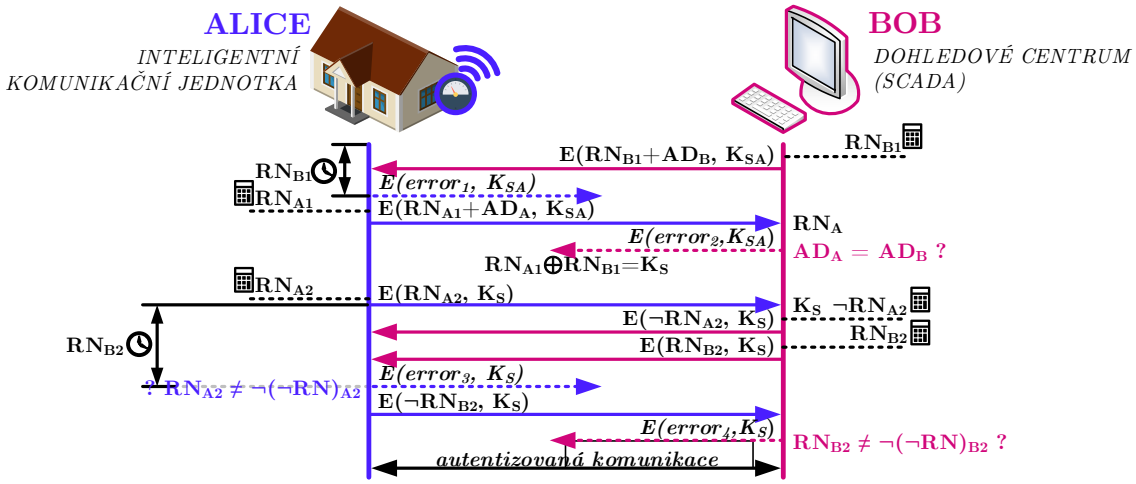
Z tohoto pohledu je tedy výhodnější použít CRC, který pokud bude využit např. v padingu a následně šifrován společně s otevřeným textem dostatečně zajistit integritu dat. CRC je navíc velice jednoduché implementovat pomocí operace XOR a volit z CRC-8/-16/-32/-64/-128 atd., kdy tedy číslo za pomlčkou značí velikost kontrolního součtu. Ta by měla být následně volena dle velikosti dat. Tedy, kdy stejně jako u haš

funkcí, čím menší velikost CRC kódu, tím více možností pro vznik kolizí (stejných CRC) a menší šance na odhalení chyb či změn. Z tohoto důvodu by volba CRC měla být volitelný parametr pro uživatele kryptosystému. V neposlední řadě pak samotný MAC tedy nejspíše není třeba uvažovat, ale budeme uvažovat rovnou kombinaci v AE, tento výběr jsme již provedli v rámci kapitoly 4.1.1, kde tedy jako jediný algoritmus z AE byl uvažován mód CCM, který však sám o sobě vykazuje pro naši oblast značné bezpečnostní nedostatky, viz kapitola 4.1.1. Tedy hlavní možností pro zajištění integrity je CRC, kde mnoho prací se zabývá využitím CRC pro zajištění integrity z pohledu informační bezpečnosti [271, 272, 273, 274, 275], nicméně spousta prací poukazuje na nebezpečnost CRC [276, 277, 278, 279, 280], a proto je nutno vždy zajistit šifrování a nezasílat CRC v otevřeném textu. CRC je nutné, i pokud by byl pro zajištění důvěrnosti použit mód CCM, protože jak ukazují normy [281, 282], tak u CCM módu je také nutno použít kontrolní součet, který následně zaručí integritu zprávy.

## 4.3 Evaluace a výběr řešení k zajišťení autentizace

Z pohledu autentizace máme několik možností: (i) asymetrická kryptografie, (ii) asymetrická kryptografie nad eliptickými křivkami, (iii) autentizační šifrování (AE), (iv) autentizační kódy zprávy (MAC). V rámci kapitol 4.1 a 4.2 i obecného úvodu v rámci kapitoly 4 jsme si dostatečně rozebrali nevhodnost asymetrické kryptografie a vyloučili jsme i možnost prostého MAC. Zůstávají tedy asymetrické algoritmy nad eliptickými křivkami (obecně vysvětleny již v rámci kapitoly 4.1.2) a AE CBC-MAC (dostatečně přiblíženo již v kapitolách 4.1.2 a 4.2). V rámci asymetrických algoritmů nad eliptickými křivkami je možno uvažovat o ECDSA, který však je velice redundantní pokud jde o poskytování pouze autentičnosti a hodí se spíše pro poskytování nepopiratelnosti v rámci transakcí na internetu apod. [124], kdy navíc některé jeho operace můžou, jako např. ověřování podpisu, být mnohem náročnější než u klasických asymetrických algoritmů [283], i když paměťová výhodnost ECDSA díky menším parametrům stále zůstává. Z tohoto pohledu je tedy jedinou možnost AE CBC-MAC, který však, jak jsme si ukázali v kapitolách 4.1.2 a 4.2 není příliš vhodné uvažovat. V práci [284] autoři představují autentizaci pomocí módu ECB, při užití náhodného tokenu. Symetrický blokový mód ECB jsme si již představili v rámci kapitoly 4.1.1, kde tedy ECB bylo definováno jako nevhodné pro důvěrnost a klasické komunikační prostředí. Nicméně pokud uvažujeme náhodný token, tak je ECB mód velice efektivní a to i s např. porovnáním módu CTR [239]. Vzhledem k uvedeným možnostem a nedostatkům se tak ECB autentizace (viz Obr. 4.10) jeví

jako nejlepší možnost pro zajištění autentizace.




Obr. 4.10: Ukázka možného zajištění autentizace pomocí symetrického blokového módu ECB (návrh převzat z [284]).

Kde tedy jednotlivé symboly znamenají: $RN_{A1}, RN_{A2}$ jsou náhodné proměnné generované Alicí; $RN_{B1}, RN_{B2}$ jsou náhodné proměnné generované Bobem; $\neg RN_{A2}$, $\neg RN_{B2}$ jsou invertované verze $RN_{A2}, RN_{B2}$; $K_{SA}$ je tajný (symetrický) autentizační klíč (pro první použití uložen v paměti, dále např. dohodnut pomocí ECDH); $AD_A, AD_B$ jsou adresy Alice (A) a Boba (B); $K_S$ je dohodnutý autentizovaný klíč určený pro šifrovanou komunikaci. Postup v rámci tohoto algoritmu je následující. Při navázání spojení (např. Bobem), je na straně Boba generováno náhodné číslo $RN_{B1}$, které je následně zašifrováno společně s jeho adresou $AD_B$ jako:

$$E_{AES-ECB}\left\{RN_{B1} + AD_B, K_{SA}\right\}, \tag{4.3}$$

pomocí sdíleného symetrického tajného autentizačního klíče $K_{SA}$. Ten je pro první použití nutno nahrát do paměti, kdy následně je možné využít například algoritmu ECDH pro jeho výměnu. Šifrovaný text je poté zaslán Alici. Alice čeká předdefinovaný čas na příjem šifrovaného textu od Boba. Pokud šifrovaný text nedorazí včas, pak je zaslána chyba typu $\text{Error}_1$ a přeruší se spojení. Alice se pak vrací do původního stavu, kdy čeká opět na navázání spojení. Pokud šifrovaný text přijde včas, pak Alice získává $RN_{B1}$ dešifrováním:

$$D_{AES-ECB}\left(E_{AES-ECB}\left(RN_{B1} + AD_B, K_{SA}\right), K_{SA}\right), \tag{4.4}$$

a dále volí své náhodné číslo $RN_{A1}$, které zasílá společně s její adresou šifrovaným textem Bobovi:

$$E_{AES-ECB}\left(RN_{A1} + AD_A, K_{SA}\right), \tag{4.5}$$

Bob po přijetí dešifruje šifrovaný text

$$D_{AES-ECB}\left(E_{AES-ECB}\left(RN_{A1}+AD_A, K_{SA}\right), K_{SA}\right), \tag{4.6}$$

a získává náhodné číslo Alice $RN_{A1}$ i její adresu $AD_A$. Zkontroluje, zda adresy nejsou shodné $AD_A = AD_B$?, což je jedna z možných ochran proti útoku přehráním. Pokud jsou shodné, Bob zasílá chybu typu $\text{Error}_2$ a ukončuje spojení. Pokud shodné nejsou, pak obě strany mají náhodná čísla $RN_{A1}$ a $RN_{B1}$ a mohou vypočítat sdílený tajný klíč $K_S = RN_{A1} \oplus RN_{B1}$, který je však nutno autentizovat a ověřit. Alice nyní generuje nové náhodné číslo $RN_{A2}$, které zašifruje pomocí nového tajného klíče $K_S$:

$$E_{AES-ECB}\left(RN_{A2}, K_S\right), \tag{4.7}$$

a šifrovaný text zašle následně Bobovi. Alice čeká stanovenou předem definovanou periodu než Bob zašle šifrovaný text s invertovaným $\neg RN_{A2}$. Bob dešifruje přijatý šifrovaný text:

$$D_{AES-ECB}\left(E_{AES-ECB}\left(\left(RN_{A2}, K_S\right), K_S\right)\right), \tag{4.8}$$

a získané náhodné číslo $RN_{A2}$ invertuje $RN_{B2} \rightarrow \neg RN_{A2}$ a zašifruje:

$$E_{AES-ECB}\left(\neg RN_{A2}, K_S\right). \tag{4.9}$$

Zároveň generuje své druhé náhodné číslo $RN_{B2}$, které také šifruje pomocí $K_S$:

$$E_{AES-ECB}\left(RN_{B2}, K_S\right), \tag{4.10}$$

oba šifrované texty jsou Bobem zaslány Alici. Pokud invertované $\neg RN_{A2}$ nedorazí včas, Alice zasílá $\text{Error}_3$ a ukončuje spojení. Pokud příjem šifrovaného textu proběhne správně, pak Alice nejprve dešifruje přijatý šifrovaný text s invertovaným $\neg RN_{A2}$:

$$D_{AES-ECB}\left(E_{AES-ECB}\left(\neg RN_{A2}, K_S\right), K_S\right), \tag{4.11}$$

a zkontroluje zda $RN_{A2} = \neg\left(\neg RN_{A2}\right)$, pokud ne zasílá chybu typu $\text{Error}_3$ a ukončuje spojení. Pokud podmínka platí, pak je druhý šifrovaný text také dešifrován:

$$D_{AES-ECB}\left(E_{AES-ECB}\left(RN_{B2}, K_S\right), K_S\right), \tag{4.12}$$

a získané náhodné číslo $RN_{B2}$ je invertováno $RN_{B2} \rightarrow \neg RN_{B2}$, zašifrováno:

$$E_{AES-ECB}\left(\neg RN_{B2}, K_S\right), \tag{4.13}$$

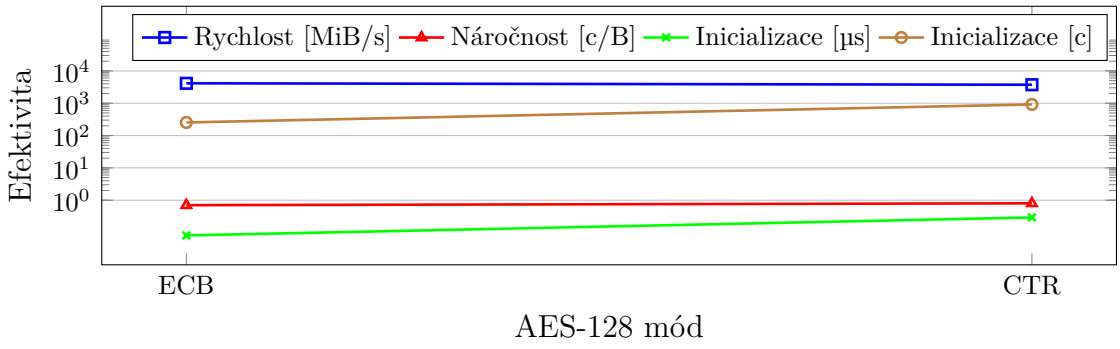
a zasláno Bobovi. Ten dešifruje přijatý text:

$$D_{AES-ECB}\left(E_{AES-ECB}\left(\neg RN_{B2}, K_S\right), K_S\right), \tag{4.14}$$

a zkontroluje zda $RN_{B2} = \neg\left(\neg RN_{B2}\right)$, pokud ne zasílá chybu typu $\text{Error}_4$ a ukončuje spojení. Pokud podmínka platí, pak je klíč $K_S$ autentizován a ověřen a může

být použit například v další fázi na šifrování dat a zaručení důvěrnosti. Stanovené čekací periody jsou ochranou proti chybám v síti, tedy aby bylo umožněno např. opětovného zaslání zprávy při chybě, ale také ochrana proti útoku přehráním, tak, aby útočník neměl neomezenou dobu pro výpočet důležitých parametrů komunikace a možnost komunikaci napadnout. Tímto způsobem je tedy možné velice efektivně řešit autentizaci pomocí módu ECB.

Pokud tedy nyní ještě porovnáme mód CCM (CTR+CBC) a ECB+CBC, pak nás tedy převážně zajímá rychlost CTR a CBC (protože CBC je obsažena v obou variantách), srovnání jejich efektivity je zobrazeno na Obr. 4.11.




Obr. 4.11: Srovnání výkonnosti módů CTR a ECB (data převzata z [239]).

Jak můžeme vidět tak rychlost šifrování je téměř stejná, nicméně inicializace u módu CTR trvá déle než u módu ECB, tedy v rámci efektivity je vhodnější mód ECB. Z těchto a i dalších výše popsaných důvodů je nejvhodnějším řešením pro autentizaci mód ECB.

## 4.4 Evaluace a výběr řešení k zajištění nepopiratelnosti

Nepopiratelnost je zobecněně zákonný koncept, kdy nejsme schopni popřít provedený akt, kde z technického pohledu se může jednat například přístup do databáze, zaslání zprávy, aj. Může se zdát, že tato priorita není podstatná z pohledu komunikace dvou zařízení, kdy nemůžeme navíc požadovat zodpovědnost od daného zařízení. Nicméně v rámci konceptu inteligentních sítí a vzdáleného měření spotřeby se tento princip mění např. na tzv. "odpovědnost" (z angl. accountability) [285]. Tedy, abychom byli schopni nejen zpoplatnit uživatele naší služby (dodávka energie, aj.), ale hlavně s jistotou odhalit, zaznamenat i prokázat nežádoucí manipulaci v jakékoliv podobě [286]. V tomto případě klasickými kryptografickými algoritmy nejsme schopni efektivně takto

komplexní a sofistikovanou úlohu řešit, už jen z principu, kdy uvažujeme i možnost napadení samotného zařízení. Jedná se o velmi komplexní algoritmy, které je nutno řešit spíše na straně dohledového centra pomocí behaviorálních modelů uživatele, statistických a pravděpodobnostních funkcí či analýz, aj. pokročilých moderních monitorovacích algoritmů [287]. Téma je tak spíše spjato s tzv. data miningem (tedy získávání informací z velkého objemu dat) a systematickou analýzou těchto informací než se samotným principem kryptografie či informační bezpečnosti [288]. Navíc většina těchto analýz vychází z principu MAN sítě a analýzy všech uživatelů v ní [215]. Zaručení nepopiratelnosti (odpovědnosti) přesahuje odborné zaměření a náplň této práce. Z tohoto důvodu se dále na tento princip již zaměřovat nebudeme. Nicméně bude to jeden z předpokladů pro správnou funkcionalitu výsledného kryptosystému, společně se zajištěním procesní bezpečnosti.

## 4.5 Evaluace a výběr řešení k zajištění čerstvosti

Čerstvost dat byla definována mnoha analýzami bezpečnosti senzorických sítí, inteligentních sítí, internetu věcí i telemetrických systému jako jedna z hlavních a důležitých priority pro informační bezpečnost [289, 290, 291, 292]. Jedná se o princip, který zaručuje, že data jsou aktuální a zajišťuje jednu ze základních ochran proti typům útoku přehrání (z angl. replay attack) [293]. Útok přehráním je diskutován v celé řadě odborných prací a je velmi dobře znám [294, 295, 296, 297]. V rámci systému, který nemá ochranu proti útoků přehráním, si útočník může nahrát jednotlivé reálné incidenty a dle potřeby je následně opakovaně přehrávat v síti, čímž může tvořit plané poplachy, vytvářet dvojí zúčtování, a další [298, 299].

Zajištění čerstvosti je možné za pomocí tzv. časového razítka (z angl. timestamp), nicméně je v tomto případě zaručit synchronizaci vysílače a přijímače, či dostatečnou toleranci chyby [300]. Dalšími možnostmi pak jsou použití tzv. čítače pro zprávu, relaci či oboje, nicméně i v rámci čítače musí být dodržena určitá míra tolerance a synchronizace na obou stranách [301]. Pro vhodné zvolení nejefektivnější techniky si nejdříve přibližme samotnou komunikaci v rámci telemetrických systémů a senzorických sítí. Samotná komunikace zde probíhá periodicky, nikoliv v kontinuálně v reálném čase, rozdělme si ji do dvou skupin [302]:

- **komunikaci na fixní bázi** (FS, z angl. Fixed-Scheduling) tedy přesně v daný čas dle plánu či rozvrhu. Pokud uvažujeme tedy například vysílání každou hodinu (perioda $t = 1\,\text{hod}$), pak za den zašle zařízení 24 zpráv. Pokud z pohledu časového razítka bude tolerance několik sekund či minut, tak i stejný čas bude mít útočník na zaregistrování komunikace a její napadení (tolerance v tomto případě bude vždy menší než perioda $t$ a útočníkův čas také). Pokud uvažujeme čítač, pak

tolerance musí být alespoň +-1 (často však bývá více), aby se zabránilo např. nepřijetí opakované zprávy z důvodu chyby. V tomto případě už teoretická doba útoku je rovna $2t$ a více. Tedy v tomto případě by útočník měl mnohem větší prostor pro napadení komunikace. Z tohoto pohledu se jeví jako efektivnější časové razítko, které dovoluje efektivnější kontrolu správně přijatých zpráv.

- **událostmi řízenou komunikaci** (ED, z angl. Event-Driven), tedy pouze pokud je splněna podmínka. V tomto případě si již nemůžeme být jisti přesným časem zasílání zpráv a časové okno je v tomto případě mnohem větší než u FS. Tyto zařízení však v rámci komunikace mnohdy musí vysílat tzv. keep-a-live zprávy, tedy informaci, že jsou v pořádku. Tyto zprávy pak lze využít na časovou synchronizaci či synchronizaci čítače. Pokud si však uvědomíme, že událostmi řízená komunikace může probíhat např. jednou za minutu, jednou za hodinu, ale mnohem pravděpodobněji např. jednou za rok při poruše, aj. Pak lze opět stanovit periodu $t$, kdy díky časovému razítku jsme schopni přesně rozlišit staré a nové zprávy, oproti čítači, který díky toleranci v tomto případě může dát útočníkovi i mnohem více času než v předchozím případě FS.

Z tohoto pohledu se tedy jeví časové razítko jako ideální varianta. Problémem však je časová synchronizace, která bývá mnohdy mnohem náročnější na implementaci než pouhý čítač, mj. i díky různým frekvencím interních hodin mikrokontroléru, uspávacím módům, aj. [303]. Jak ukazuje práce [304], tak časová synchronizace může být řešena různými způsoby, kdy největší problém tvoří autentizace jednotlivých stran. Pokud není zaručena autentizace, je nutno vždy využívat odhadů, které však nejsou přesné, kdy se navíc časová desynchronizace v čase roste [305]. V kapitole 4.3 je ukázán způsob autentizace, který lze využít i pro časovou synchronizaci. Nicméně navržený systém využívá jednorázového hesla tzv. tokenu pro inicializaci a následně je možno toto jednorázové heslo využít i pro šifrování [284]. Tento náhodný token je tak možné použít mj. i pro ochranu proti útoku přehráním [306], jelikož jednoznačně identifikuje danou relaci a každá další relace využívá jiný opět náhodně vygenerovaný token. Tento způsob ochrany čerstvosti dat, tedy ušetří případné místo v datové části, kterou by jinak zabralo časové razítko nebo čítač.

## 4.6 Vlastní návrh hybridního kryptosystémů

V rámci kapitol 4.1–4.5 byla provedena hloubková analýza a evaluace jednotlivých kryptografických možností pro zajištění definovaných principů informační bezpečnosti. Výsledky této analýzy jsou přehledně zobrazeny v Tab. 4.4.

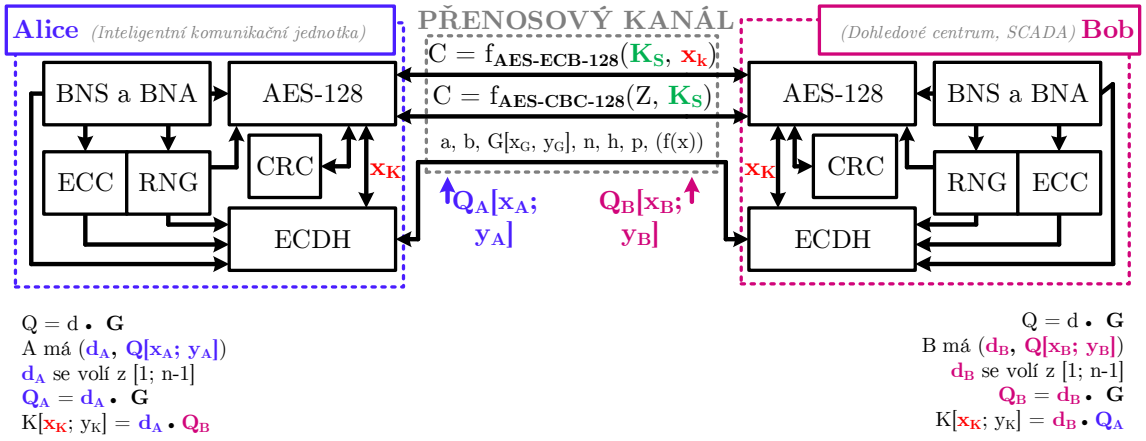
Tab. 4.4: Výsledky provedené hloubkové analýzy a evaluace jednotlivých kryptografických algoritmů.

| **Princip** | **Zvolený nejvhodnější algoritmus - popis** |
|---|---|
| Důvěrnost | V rámci zajištění důvěrnosti bylo zjištěno, že ideálními algoritmy jsou pro zařízení s limitovanými zdroji symetrické algoritmy. Byli hodnoceny jednotlivé blokové i proudové algoritmy z pohledu jejich bezpečnosti a efektivity, kde jako ideální algoritmus byl zvolen algoritmus **AES-128**. Následně byly posuzovány vhodné blokové módy, kde při vhodném zajištění autentizace, byl zvolen jako nejvhodnější **mód AES-CBC**, případně mód AES-CCM, pokud by nebylo možné zajistit efektivním způsobem autentizaci. Jako poslední v této části byly analyzovány možnosti pro distribuci symetrického tajného klíče, kde jako ideální a téměř jediná možnost pro námi definovanou oblast se jeví **algoritmus ECDH**. |
| Integrita | Analýza možností pro zajištění integrity kontrolní součty, CRC, kryptografické i klasické hašovací funkce a další. V rámci zajištění integrity bylo nutné přistoupit ke kompromisu, který však dle dosavadních znalostí a představené literatury je bezpečnou variantou, pokud bude toto řešení poskytováno společně s důvěrnosti. Jedná se o **algoritmus CRC-16(C)**, kdy jeho výsledek je nutno šifrovat společně s kontrolovanou zprávou. |
| Autentizace | V rámci autentizace proběhla hloubková analýza dnešních klasických možností, které nebyly shledány jako vhodné pro námi definovanou část telemetrických systémů. V rámci odborné literatury pak vzešla možnost zajištění integrity pomocí blokového **módu AES-ECB**, který se oproti ostatním řešením jeví jako nejefektivnější varianta z pohledu bezpečnosti i náročnosti. |
| Nepopiratelnost | Nepopiratelnost ve své podstatě byla identifikována jako nepotřebná pro definovanou oblast. Nicméně vznikla nová oblast tzv. *Odpovědnosti*, která již důležitá je. Nicméně tato oblast je řešena spíše procesními kroky a následně velice odlišnými algoritmy od těch kryptografickým, kdy většinou se jedná o analytické a statistické nástroje. Z tohoto důvodu je zajištění nepopiratelnosti (odpovědnosti) ponecháno jako procesní krok a je to jedna z podmínek, pro bezpečnou implementaci navrhovaného systému do reálného prostředí. |
| Čerstvost | Zajištění čerstvosti také není zcela možno zajistit kryptografickými algoritmy. Z provedené analýzy však plyne, že je možné čerstvost zajistit pomocí **jednorázového náhodného tokenu**, který se používá **v módu ECB**. Což je ideální z pohledu nepotřebnosti žádného aditivního mechanismu pro zajištění čerstvosti, synchronizace aj. |

Samotný vlastní hybridní kryptosystém bychom mohli popsat následovně. Před samotnou instalací zařízení do reálného prostředí do něj bude nahrán prvotní náhodný symetrický autentizační klíč. Ten bude využit algoritmem AES-128-ECB (viz Obr. 4.10) k dohodnutí a autentizaci jednorázového náhodného tajného šifrovacího klíče. Následně bude možno šifrovat komunikaci pomoci dohodnutého jednorázového klíče algoritmem AES-128-CBC (viz kapitola 4.1.1). Pro zajištění integrity pak budou před šifrováním doplňovány 2 B kódu pomocí CRC-16(C) (viz kapitola 4.2). Algoritmus ECDH bude následně využíván periodicky vždy, když bude nutno dohodnout nový tajný autentizační klíč (viz kapitola 4.1.2).

Dále pak v ramci komplexního systému je nutno uvažovat i modul, který bude řešit problematiku velkých čísel a modulární aritmetiku velkých čísel. Dalším požadavkem, které kryptografické algoritmy mají jsou náhodné parametry (např. při generování

náhodného tokenu pomocí AES-128-ECB, viz kapitola 4.3). Tedy jako další modul navrhovaného kryptosystému je nutno uvažovat i náhodný generátor, který poskytne vstupní parametry do kryptografických algoritmů. Výsledné řešení navrhovaného kryptosystému je pak zobrazeno na Obr. 4.12.




Obr. 4.12: Zjednodušené blokové schéma vlastního návrhu hybridního kryptosystému, zajišťující definované principy informační bezpečnosti.

Jednotlivé moduly jsou: (i) struktura velkých čísel (BNS, z angl. Big Number Structure), (ii) aritmetika velkých čísel (BNA, z angl. Big Number Arithmetic), (iii) náhodný generátor (RNG, z angl. Random Number Generator), (iv) modul pro cyklický redundantní součet (CRC, z angl. Cyclic Redundancy Check), (v) struktura pro kryptografii eliptických křivek (ECC, z angl. Elliptic Curve Cryptography), (vi) struktura pro algoritmus Diffieho-Hellmana založeném na eliptických křivkách (ECDH, z angl. Elliptic Curve Diffie-Hellman), a (vii) symetrický šifrovací algoritmus Advanced Encryption Standard (AES) s velikostí klíče 128 a podporou módu pro šifrování CBC (z angl. Cipher Block Chaining)a autentizaci ECB (z angl. Clectronic Codebook). Představený model byl úspěšně prezentován autorem v řadě odborných a vědeckých publikací, mj. mezinárodní konference (WoS/Scopus) [307, 308, 309] a v impaktovaných časopisech [310, 311].

# 5 VÝVOJ, VERIFIKACE A OPTIMALIZACE NAVRŽENÉHO KRYPTOSYSTÉMU

Tato kapitola se věnuje praktické validaci jednotlivých dílčích částí vlastního navrženého kryptosystému, experimentálním měřením a výzkumu zaměřeného na optimalizaci využívaných kryptografických algoritmů. Kapitola je rozdělena dle jednotlivých bloků hybridního kryptosystému. Jako první však bylo nutno vybrat vhodnou hardwarovou platformu, která by představovala uvažovanou inteligentní komunikační jednotku s limitovanými zdroji z oblasti telemetrických systémů, což shrnuje kapitola 5.1. Dále v kapitole 5.2 jsou již rozebrány funkce pro práci s velkými čísly z vlastní vytvořené knihovna kryptografických algoritmů. Jsou rozebrána algoritmizace jednotlivých algebraických operací v návaznosti na definované vztahy v předchozích kapitolách a následně jsou přiblíženy jednotlivé funkce knihovny. Nakonec jsou představeny výsledky vlastních experimentálních měření s účelem validovat navržené algoritmy z pohledu jejich efektivity. Následuje kapitola 5.3, která se věnuje výzkumu náhodných generátorů, jejich návrhu a vlastní realizaci. V této kapitole jsou provedeny mj. rozsáhlé experimentální i evaluační testy náhodnosti a výkonnosti jednotlivých generátorů. Poté v kapitole 5.4 je přiblížena realizace AES-128, která využívá knihovny [312] a knihovny [313]. V této kapitole je věnována značná část optimalizaci těchto metod a experimentálním měřením s danými knihovnami v reálném prostředí telemetrických sítí. V neposlední řadě je v kapitole 5.5 přiblížena vlastní knihovna kryptografie eliptických křivek pro distribuci tajných symetrických klíčů metodou ECDH (knihovnu je dostupná z [314]). Tato knihovna představuje odlehčenou derivaci funkcí z velmi rozšířené knihovny OpenSSL [315]. Významná část těchto funkcí byla optimalizována a pozměněna pro větší vhodnost ve vybraném MCU s limitovanými zdroji jako např. standardizace datových typů, změna dynamické alokace proměnných, upraven paměťový management pro lepší energetickou efektivitu, byli přidány chybové stavy, byly vyloučeny hardwarově závislé funkce a proměnné, aj. Ponechali jsme však jména proměnných a notaci funkcí pro přehlednost a transparentnost.

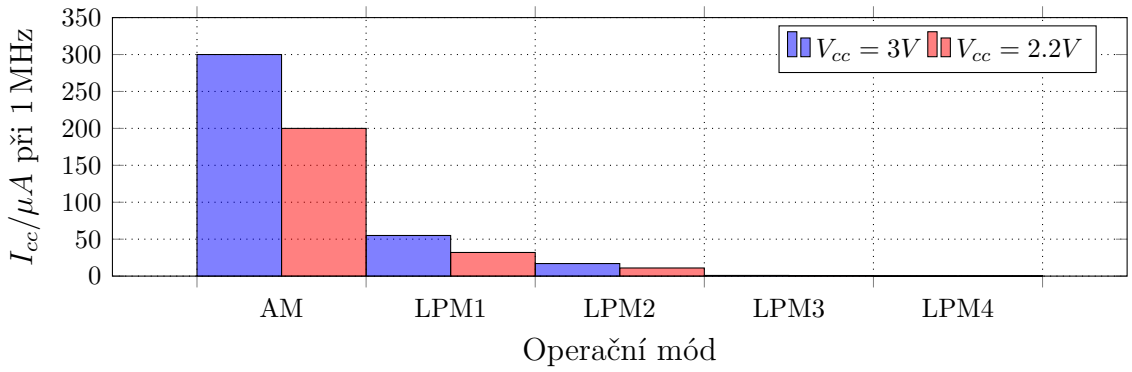
## 5.1 Výběr komunikační a výpočetní jednotky

Inteligentní komunikační jednotka je postavena na vybraném mikrokontroleru (MCU, z angl. Microcontroller Unit) od firmy Texas Instruments, MSP430F5438A [316]. MSP430F5419 je procesor z rodiny MSP430 od Texas Instruments (dále budeme námi vybraný typ označovat pouze jako MSP430). Tyto procesory se vyznačují velmi nízkou spotřebou a cenou na úkor menšího výkonu, paměti aj., tedy splňuje

aplikační definici zařízení s limitovanými zdroji. Architektura těchto procesorů je optimalizovaná k zvětšení životnosti baterie v přenositelných aplikacích. Tento MCU byl vybrán z těchto důvodů:

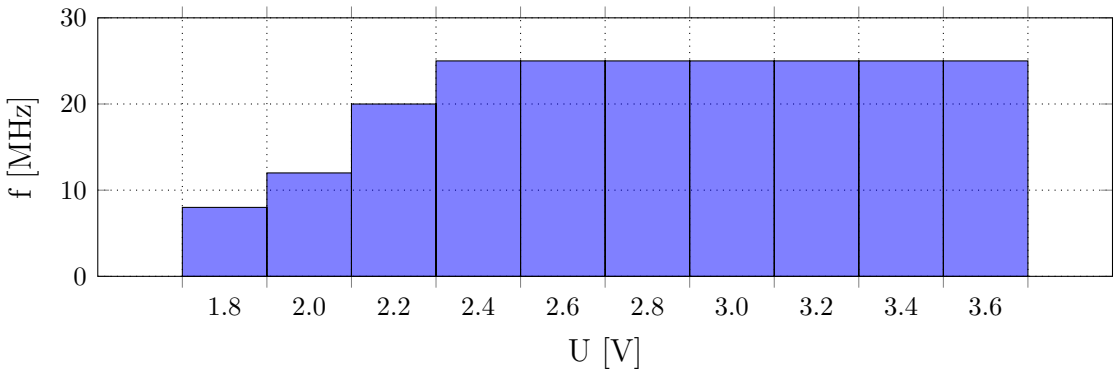
- Vlastní CPU, možno užít vysokofrekvenčního (digitálně řízený oscilátor, 32 MHz) i nízkofrekvenčního zdroje (fyzický krystal, 32 kHz),
- integrovaná 32-bitová hardwarová násobička,
- nízké napájecí napětí (1,8–3,6 V) a nízký odběr (řádově v jednotkách až stovkách µA),
- rychlé probuzení ze spacího režimu (3.5 µs),
- řešení hardwarového generátoru náhodných čísel (viz např. [148]),
- dostatečně paměť (Flash 256 kB + RAM 16 kB) a kvalitní softwarová optimalizace.

Další výhodou tohoto MCU, jsou různé módy (přednastavené spuštěné a vypnuté periferie), které mění velikost spotřeby, tyto módy je pak možné ještě dle požadavků měnit a tak použít jen opravdu nejnutnější prvky a tím idealizovat spotřebu. Módy MCU a jejich spotřeba je na zobrazena na Obr. 5.1, kde AM je aktivní mód (z angl. Active Mode) a LPM jsou nízkonapěťové módy 1–4 (z angl. Low Power Mode).



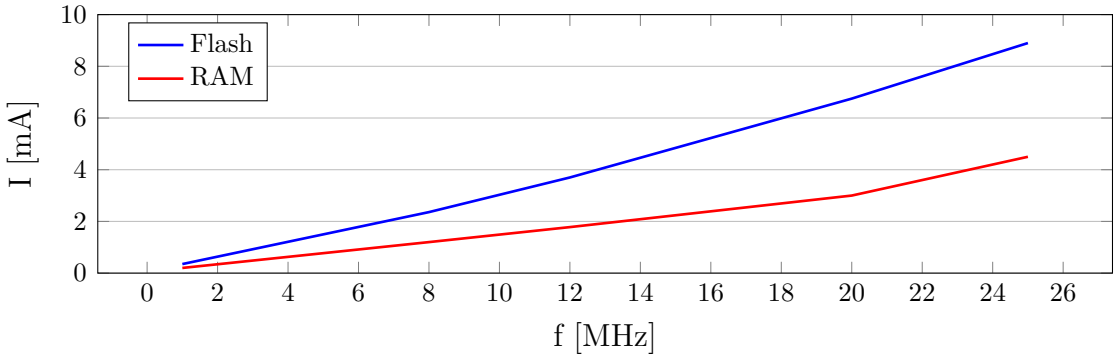

Obr. 5.1: Srovnání energetické efektivity operačních módů vybraného MCU.

Jak je vidět v LPM4 módu je spotřeba MCU téměř nulová (v tomto módu je většina částí MCU vypnutá, je to tzv. hluboký spánek). S tímto MCU byly provedeny také prvotní měření závislosti taktovací frekvence na napájecím napětí, viz Obr. 5.2.




Obr. 5.2: Závislost taktovací frekvence na napájecím napětí vybraného MCU.

Jak můžeme vidět v rámci nejmenší možné taktovací frekvence MCU 8 MHz je napájecí napětí 1,8 V a na nejvyšší frekvenci 25 MHz. Při realizaci uvažovaného kryptosystému bude tedy vhodné snažit se o řešení, které by bylo možné využít na frekvenci $\leq 8\,MHz$, aby se omezili netechnické ztráty a zvýšila výdrž baterie. Dále jak je patrné z Obr. 5.3, tak je možné snížit proudový odběr MCU využitím paměti RAM namísto paměti Flash, což znamená minimalizovat nároky na paměť, protože Flash je 256 kB, ale RAM pouhých 16 kB.




Obr. 5.3: Závislost odběru vybraného MCU na taktové frekvenci a typu paměti.

Největší výhodou tohoto MCU je, že externí mikroprocesorové periferie vybraného MCU mají již moderní koncepce automatického přechodu do spánkového módu, pokud není periferie využívána a opětovného přechodu do provozního stavu, je-li třeba periferii využít. U ostatních periferií přechod do úsporného režimu zajistí zásah řídícího procesoru. Toto řízení je vhodné použít nejen k přechodům do stavů snížené spotřeby, ale je účelné je použít také pro přechod těchto periferií do stavu plného provozu, kdy jsou tyto periferie zapínány postupně. Tato činnost při náběhu zmenší

nárazovou spouštěcí vlnu energie, která by nastala při současném zapnutí všech periferií. Taková koncepce pak celkově snižuje nároky na napájecí zdroj a sníží dimenzování jeho výkonu. Jak je vidět v rámci vybraného MCU je umožněno maximální možné dynamičnosti v úpravě spotřeby elektrické energie. To je jedna z dalších výhod, která nám dává prostor vytvořit efektivní algoritmy, které nenaruší dlouhodobý běh MCU na baterii. V neposlední řadě jsou tyto MCU využívány celou řadou průmyslových subjektů k dálkovým měřením, např. společnost MEgA – Měřící Energetické Aparáty, a.s., vyrábí GPRS komunikační jednotky MEg202.2 a komunikační jednotky MEg201.2 se čtyřnásobným dálkovým rozhraním ETHERNET. Tyto komunikační jednotky používají právě tento mikroprocesor a jsou využívány v inteligentních sítích a telemetrických systémech. Jak je vidět jedná se tedy o MCU, která splňuje veškeré požadavky pro námi uvažovanou inteligentní komunikační jednotku. V rámci experimentálních měření představených v této kapitole bylo na tomto MCU vždy použito frekvence $f_{CPU} = 1\,\text{MHz}$ a $V_{cc} = 3000\,\text{mV}$. $I_{cc}$ bylo $300\,\mu\text{A}$ pro vybrané $f_{CPU}$ a $V_{cc}$. Byl použit aktivní operační mód.

## 5.2 Vývoj modulu reprezentace velkých čísel a funkcí modulární aritmetiky

### 5.2.1 Algoritmizace operací modulární aritmetiky

V rámci kapitoly 3.1 byly definovány velká čísla, základní aritmetické operace, modulární aritmetika a konečná pole. Tento teoretický základ, společně se získanými znalostmi ze studované literatury [124, 127, 125], byly využity k vývoji uvažovaného modulu reprezentace velkých čísel, základních aritmetických operací i modulární aritmetiky pro potřeby navrženého vlastního hybridního kryptosystému. V této kapitole je přiblížena provedená algoritmizace jednotlivých operací do pseudo-funkcí. V rámci přehlednosti jsou tučně značeny v představených algoritmech logické operace a symboly značící velká čísla.

#### I. Operace sčítaní a odčítání

Operace sčítání a odčítání dvou celých čísel o stejné bázi $b$. Pokud mají čísla různou velikost, tak je menší z nich doplněno pomocí padingu nulami “zleva”, tedy od pozice MSB. Algoritmus 1 popisuje sčítání dvou velkých celých čísel $x + y$, kde výsledkem je celé velké číslo $w$ o stejné bázi $b$.

**Algorimus 1** Sčítání velkých čísel

**Require:** Kladná celá čísla $\mathbf{x}$, $\mathbf{y}$ o velikost $n$ a bázi $b$
**Ensure:** $\mathbf{w} = \mathbf{x} + \mathbf{y}$, kde $\mathbf{w} = (w_n, w_{n-1}, ..., w_0)$
1: $c \leftarrow 0$
2: **for** $(i \leftarrow 0)$ **to** $n - 1$ **do**
3: $\quad w_i \leftarrow (x_i + y_i + c) \bmod b$
4: $\quad$ **if** $((x_i + y_i + c) < b)$ **then**
5: $\quad\quad c \leftarrow 0$
6: $\quad$ **else**
7: $\quad\quad c \leftarrow 1$
8: $\quad$ **end if**
9: $\quad w_n \leftarrow c$
10: **end for**
11: **return w**

Algoritmus 2 představuje pro dvě velká celá čísla $x, y$ algoritmizovanou operaci odčítání $x - y$ pro $x \geq y$. Čísla $x, y$ mají opět stejnou bázi $b$ a výsledek je opět celé velké číslo $w$ o stejné bázi $b$.

**Algorimus 2** Odčítání velkých čísel

**Require:** Kladna celá čísla $\mathbf{x}$, $\mathbf{y}$ o velikosti $n$ a bázi $b$, $\mathbf{x} \geq \mathbf{y}$
**Ensure:** $\mathbf{w} = \mathbf{x} - \mathbf{y}$, kde $\mathbf{w} = (w_n, w_{n-1}, ..., w_0)$
1: $c \leftarrow 0$
2: **for** $(i \leftarrow 0)$ **to** $n - 1$ **do**
3: $\quad w_i \leftarrow (x_i - y_i + c) \bmod b$
4: $\quad$ **if** $((x_i - y_i + c) \geq b)$ **then**
5: $\quad\quad c \leftarrow 0$
6: $\quad$ **else**
7: $\quad\quad c \leftarrow -1$
8: $\quad$ **end if**
9: $\quad w_n \leftarrow c$
10: **end for**
11: **return w**

## II. Operace násobení

Algoritmus 3 představuje pro dvě celá čísla $x, y$ o velikosti $n + 1, t + 1$ a bázi $b$ algoritmizovanou operaci násobení $x \cdot y$, kde výsledkem je celé číslo $w$ s maximální velikostí $n + t + 2$ o stejné bázi $b$.

**Algorimus 3** Násobení velkých čísel

**Require:** Kladná celá čísla $\mathbf{x}$ o velikosti $n + 1$ a $\mathbf{y}$ o velikosti $t + 1$, $\mathbf{x}$, $\mathbf{y}$ mají bázi $b$
**Ensure:** $\mathbf{w} = \mathbf{x} \cdot \mathbf{y}$, kde $\mathbf{w} = (w_{n+t}, w_{n+t+1}, ..., w_0)_b$
1: **for** $(i \leftarrow 0)$ **to** $(n + t + 1)$ **do**
2: $\quad w_i \leftarrow 0$
3: **end for**
4: **for** $(i \leftarrow 0)$ **to** $(t)$ **do**
5: $\quad c \leftarrow 0$
6: $\quad$ **for** $(j \leftarrow 0)$ **to** $(n)$ **do**
7: $\quad\quad (u, v)_b = w_{i+j} + x_j \cdot y_i + c$, for $w_{i+j} \leftarrow v$ a $c \leftarrow u$
8: $\quad$ **end for**
9: $\quad w_{i+n+1} \leftarrow u$
10: **end for**
11: **return** $\mathbf{w}_b$

### III. Operace dělení

Algoritmus 4 představuje pro dvě celá čísla $x, y$ o velikosti $n, t$ a bázi $b$, kde $n \geq t \geq 1$ a $y_t \neq 0$ algoritmizovanou operaci násobení $x/y$, kde výsledkem je celé číslo $q$ (podíl) a celé číslo $r$ (zbytek) se stejnou bází $b$, tedy $(q, r)_b$.

**Algorimus 4** Dělení velkých čísel

**Require:** Kladná celá čísla $\mathbf{x} = (x_n, x_{n-1}, ..., x_0)_b$, $\mathbf{y} = (y_t, y_{t-1}, ..., y_0)_b$ s bází $b$, pro $n \geq t \geq 1$ a $y_t \neq 0$
**Ensure:** $\mathbf{q} = \lfloor \mathbf{x}/\mathbf{y} \rfloor$ a zbytek $\mathbf{r}$, kde $\mathbf{q} = (q_{n-t}, q_{n-t-1}, ..., q_0)_b$, $\mathbf{r} = (r_t, r_{t-1}, ..., r_0)_b$, $\mathbf{x} = \mathbf{q}\mathbf{y} + \mathbf{r}$ a $0 \leq \mathbf{r} \leq \mathbf{y}$
1: **for** $\{i \leftarrow 0)$ **to** $(n - t)$ **do**
2: $\quad q_i \leftarrow 0$
3: **end for**
4: **while** $\left(\mathbf{x} \geq \mathbf{y}b^{n-t}\right)$ **do**
5: $\quad q_{n-t} \leftarrow q_{n-t} + 1$ a $\mathbf{x} \leftarrow \mathbf{x} - \mathbf{y}b^{n-t}$
6: **end while**
7: **for** $(i \leftarrow n)$ **to** $(t + 1)$ **do**
8: $\quad$ **if** $(x_i = y_t)$ **then**
9: $\quad\quad q_{i-t-1} \leftarrow b - 1$
10: $\quad$ **else**
11: $\quad\quad q_{i-t-1} \leftarrow \lfloor (x_i b + x_{i-1})/\, y_t \rfloor$
12: $\quad$ **end if**
13: $\quad$ **while** $\left(q_{i-t-1}\,(y_t b + y_{t-1}) > \left(x_i b^2 + x_{i-1} b x_{i-2}\right)\right)$ **do**
14: $\quad\quad q_{i-t-1} \leftarrow q_{i-t-1} - 1$
15: $\quad$ **end while**
16: $\quad \mathbf{x} \leftarrow \mathbf{x} - q_{i-t-1}\mathbf{y}b^{i-t-1}$
17: $\quad$ **if** $(\mathbf{x} < 0)$ **then**
18: $\quad\quad \mathbf{x} \leftarrow \mathbf{x} + \mathbf{y}b^{i-t-1}$ a $q_{i-t-1} \leftarrow q_{i-t-1} - 1$
19: $\quad$ **end if**
20: **end for**
21: $\mathbf{r} \leftarrow \mathbf{x}$
22: **return** $(\mathbf{q}, \mathbf{r})_b$

### IV. Modulární operace sčítání a odčítání

Modulární sčítání a odčítání jsou nejjednodušší modulární operace. Nechť $x, y$ jsou kladná celá čísla definovaná jako $x, y < m$. Pak platí, že: (i) $x + y < 2m$; (ii) pokud je $x \geq y$, pak platí $0 \leq x - y < m$; a (iii) pokud je $x < y$, pak platí $0 \leq x + m - y < m$. Dále pak pokud jsou $x, y \in \mathbb{Z}_m$, pak modulární sčítání $(x + y \pmod m)$ lze řešit pomocí algoritmu 1, jako vícenásobné sčítání s aditivním krokem odečtení $m$ (pouze a jedině tehdy, když $x + y \geq m$). Modulární odečítání $(x - y \pmod m)$ pak můžeme řešit přesně pomocí algoritmu 2 za předpokladu, že $x \geq y$.

### V. Modulární operace sčítání a odčítání

Modulární násobení je mnohem více používáno než klasické násobení (viz algoritmus 3) lze řešit pomocí kombinace algoritmů 3 (násobení) a 4 (pro výpočet tzv. "redukce"), tedy máme opět celá čísla $x, y$ a modulo $m$, všechna tato čísla mají bázi $b$, pak kombinací algoritmu 3 a 4 jsme schopni vypočítat modulární násobení $x \cdot y \pmod m$, viz algoritmus 5.

**Algorimus 5** Základní modulární násobení velkých čísel

**Require:** Kladna celá čísla $\mathbf{x}$, $\mathbf{y}$ a modul $\mathbf{m}$
**Ensure:** $\mathbf{x} \cdot \mathbf{y} \bmod \mathbf{m}$
1: $\mathbf{i} = \mathbf{x} \cdot \mathbf{y}$ pomocí 3
2: $\mathbf{r} = \mathbf{i}/\mathbf{m}$ pomocí 4
3: **return r**

Tento algoritmus však není příliš efektivní a tak bylo využito další optimalizace v kroku (1) a (2) pomocí mnohem efektivnějších metod násobení. V sekci (IV.) je popsána využitá metoda Montgomeryho redukce a v sekci (V.) pak Montgomeryho násobení, které jsou v rámci funkcí modulární aritmetiky využity také ve vlastní knihovně.

## VI. Operace Montgomeryho redukce

Mongomeryho redukce je technika umožňující efektivní implementaci modulárního násobení. Pokud máme velká kladná celá čísla $m$, $R$ a $T$, kde $R > m$, $f_{gcd}(m, R) = 1$ a $0 \leq T < mR$. Funkce $gcd\,()$ je funkce výpočtu největšího společného dělitele (z angl. Greatest comon divisor). Hlavní myšlenka je v převedení operace dělení, která slouží k získání zbytku, na mnohem jednodušší operaci bitového posuvu (viz 6). Operace bitového posuvu či obecně bitové operace jsou nejrychlejší operace na většina hardwarových platforem a také méně náročné oproti klasickému dělení. V rámc další optimalizace byla Montgomeryho redukce využitá také pro optimalizaci algoritmu 4.

**Algorimus 6** Montgomeryho redukce velkých čísel

**Require:** Kladná celá čísla $\mathbf{m} = (m_{n-1}, m_n, ..., m_0)$ s bází $b$, kde $gcd(\mathbf{m}, b) = 1$, $\mathbf{R} = b^n$, $\mathbf{m'} = -\mathbf{m}^{-1} \bmod b$ a $\mathbf{T} = (t_{2n-1}, t_{2n}, ..., t_0) < \mathbf{mR}$
**Ensure:** $A = \mathbf{TR}^{-1} \bmod \mathbf{m}$
1: $\mathbf{A} \leftarrow \mathbf{T}$, for $\mathbf{A} = (a_{2n-1}, a_{2n}, ..., a_0)$
2: **for** $(i \leftarrow 0)$ **to** $(n-1)$ **do**
3: $\quad u_i \leftarrow a_1 \mathbf{m'} \bmod b$
4: $\quad \mathbf{A} \leftarrow \mathbf{A} + u_i \mathbf{m} b^i$
5: **end for**
6: $\mathbf{A} \leftarrow \mathbf{A}/b^n$
7: **if** $(\mathbf{A} \geq \mathbf{m})$ **then**
8: $\quad \mathbf{A} \leftarrow \mathbf{A} - \mathbf{m}$
9: **end if**
10: **return A**

## VII. Operace Montgomeryho násobení

Montgomeryho násobení je tedy kombinací algoritmu 6 (Montgomeryho redukce) a algoritmu 3 (klasického násobení). Výsledný algoritmus 7 je pak znázorněn níže.

**Algorimus 7** Montgomeryho násobení pro velká čísla

**Require:** Kladná celá čísla $\mathbf{m} = (m_{n-1}, m_n, ..., m_0)$, $\mathbf{x} = (x_{n-1}, x_n, ..., x_0)$, $\mathbf{y} = (y_{n-1}, y_n, ..., y_0)$ s bází $b$, for $0 \leq \mathbf{x}, \mathbf{y} < \mathbf{m}$, $\mathbf{R} = b^n$, $gcd(\mathbf{m}, b) = 1$ and $\mathbf{m'} = \mathbf{m}^{-1} \bmod b$
**Ensure:** $A = \mathbf{xyR}^{-1} \bmod \mathbf{m}$
1: $\mathbf{A} \leftarrow 0$, for $\mathbf{A} = (a_n, a_{n-1}, ..., a_0)$
2: **for** $(i \leftarrow 0)$ **to** $(n-1)$ **do**
3: $\quad u_i \leftarrow (a_0 + x_i x_0)\,\mathbf{m'} \bmod b$
4: $\quad A \leftarrow \mathbf{A} + x_i\mathbf{y} + u_i\mathbf{m}/b$
5: **end for**
6: **if** $(\mathbf{A} \geq \mathbf{m})$ **then**
7: $\quad \mathbf{A} \leftarrow \mathbf{A} - m$
8: **end if**
9: **return A**

### 5.2.2 Ověření funkcí modulární aritmetiky

V rámci této části jsou již popsány jednotlivé funkce modulární aritmetiky z vlastní knihovny [314] kryptografických funkcí. Jednotlivé funkce jsou opatřeny identifikátorem #, který je pak použit v rámci experimentálních měření. První je nutno představit vytvořenou struktura pro velký čísla `bignum_st`:

```
Struct bignum_st {BN_ULONG *d, int top; int dmax; int neg; int flags; } BIGNUM;
```

Proměnná $d$ je ukazatel specifické pozice v paměti, kde je velké číslo uloženo, *top* představuje pozici MSB v poli $d$ a *dmax* je maximální velikost pole $d$. Dále pak *neg* je příznak určující zda je číslo záporné a $flags$ slouží pro případné další příznaky. Dále pak jsou zde funkce sčítání dvou velkých celých čísel dle $r = a + b$ (`BN_add`, #1) vycházející z algoritmu 1:

```
int BN_add {BIGNUM *r, const BIGNUM *a, const BIGNUM *b};
```

a odčítání dvou velkých celých čísel dle $r = a - b$ (`BN_sub`, #2) vycházející z algoritmu 2:

```
int BN_sub {BIGNUM *r, BIGNUM *a, const BIGNUM *b};
```

Dále byla realizována funkce klasického násobení dvou velkých celých čísel dle $r = a \cdot b$ (`BN_mul`, #8) vycházející z algoritmu 3:

```
int BN_sub {BIGNUM *r, BIGNUM *a, const BIGNUM *b};
```

a dělení dvou velkých celých čísel $r = a / b$ (`BN_div`, #7) vycházející z algoritmu 4.

```
int BN_sub {BIGNUM *r, BIGNUM *a, const BIGNUM *b};
```

Tyto funkce byly dále modifikovány pro jejich modulární varianty, k těmto účelům byla vytvořena pomocná funkce modulárních operací `BN_mod`, která zajišťuje $r = a \pmod m$ (#6):

```
int BN_mod {BIGNUM *r, const BIGNUM *a, const BIGNUM *m, BN_CTX *ctx };
```

Struktura `BN_CTX` je pomocná struktura využívána pro vedlejší výpočty. Dále byla vytvořena funkce modulárního sčítání dvou velkých celých čísel `BN_mod_add` (#3), která počítá $r = a \ + b \pmod{m}$, kde výsledek $r$ musí splňovat:

$$(r \neq a) \wedge (r \neq b) \wedge (r \neq m), \tag{5.1}$$

jedná se o funkci vycházející z 1, která je následně upravena dle kapitoly 5.2.1 sekce (IV.):

```
int BN_mod_add {BIGNUM *r, const BIGNUM *a, const BIGNUM *b, const BIGNUM *m, BN_CTX *ctx };
```

pokud je vznikne chyba, funkce vrací hodnotu 0. Následně byla vytvořena operace modulárního odečítání dvou velkých celých čísel `BN_mod_sub` (#4), která počítá $r \ = \ a \ - b \pmod{m}$. Výsledek $r$ musí splňovat rovnici 5.1. Syntaxe funkce je následující:

```
int BN_mod_sub {BIGNUM *r, const BIGNUM *a, const BIGNUM *b, const BIGNUM *m, BN_CTX *ctx };
```

Následuje vytvořená funkce `BN_mod_mul` (#5), sloužící pro modulární násobení dvou velkých celých čísel $r = a \ \cdot b \pmod{m}$ vycházející z algoritmu 3. Výsledek $r$ musí opět splňovat rovnici 5.1. Syntaxe je následující:

```
int BN_mod_mul {BIGNUM *r, const BIGNUM *a, const BIGNUM *b, const BIGNUM *m, BN_CTX *ctx };
```

Tato funkce, jak již bylo řečeno v kapitole 5.2.1 sekci (VI.), není zcela ideálním efektivním řešením. Z tohoto důvodu byly dále vytvořeny Montgomeryho funkce, zajišťující Montgomeryho redukci (`BN_from_montgomery`), vycházející z algoritmu 6:

```
int BN_from_montgomery {BIGNUM *ret, const BIGNUM *a, BN_MONT_CTX *mont, BN_CTX *ctx };
```

Tato funkce není používána samostatné, ale slouží k zajištění Montgomeryho násobení (`BN_mod_mul_montgomery`, #10) vycházející z algoritmu 7):

```
int BN_mod_mul_montgomery {BIGNUM *r, const BIGNUM *a, const BIGNUM *b,
    BN_MONT_CTX *mont, BN_CTX *ctx };
```

Komentovaný příklad jednotlivých funkcí a jejich použití je názorně ukázán v příloze A. Algoritmizace, následná realizace i experimentální měření a validace představených metod je nyní podána na konferenci ICUMT 2017 [307] (indexováno ve Scopus/Wos, *článek je nyní v recenzním řízení*).

### 5.2.3 Experimentální validace funkcí modulární aritmetiky

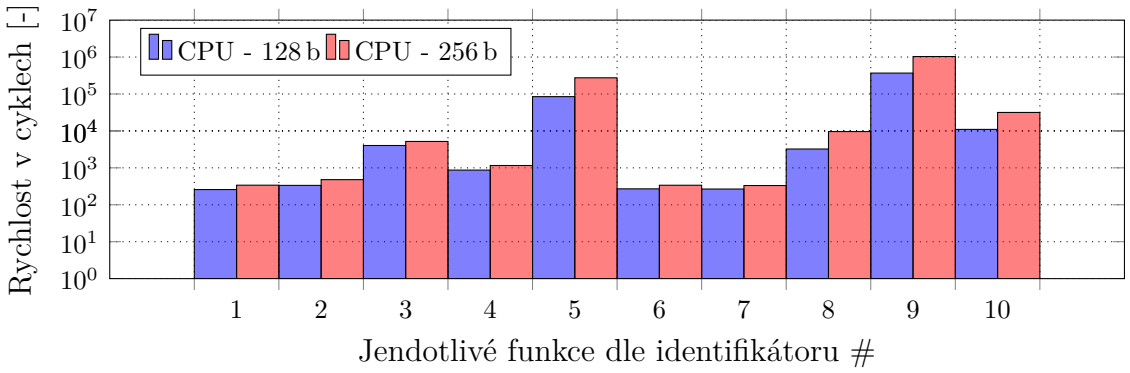
V rámci zařízení s limitovanými zdroji jsou paměť a výkon, které mj. dále pak ovlivňují i spotřebu, viz Obr. 5.2 a 5.3. Z tohoto důvodu musí být jakýkoliv reálný systém dostatečně efektivní. Z tohoto důvodu byly provedeny experimentální měření navržených funkcí sloužících pro algebraické operace s velkými čísly a modulární aritmetiku s velkými čísly. Vytvořili jsme tři velká čísla $a$, $b$ a $m$, kde $m > a > b$ s velikostí 128 a 256 b (tyto velikosti vychází z analýzy provedené v kapitole 3). Čísla $a$ a $b$ reprezentují operandy testovaných funkcí a číslo $m$ pak modulo. Tabulka 5.1 pak zobrazuje přehledně jednotlivé výsledky procesorové a paměťové náročnosti (CPU tedy značí počet cyklů), kde paměť zařízení je tedy 256 kB.

Tab. 5.1: Časová a výkonnostní náročnost jednotlivých implementovaných funkcí pro výpočty s velkými čísly.

| # | **Jméno funkce** | **Flash [B]** | **CPU - 128 b [-]** | **CPU - 256 b [-]** |
|---|---|---|---|---|
| *Funkce bez pomocných struktur* | | | | |
| 1 | `BN_add` | 5 686 | 258 | 339 |
| 2 | `BN_sub` | 5 736 | 335 | 479 |
| | Všechny funkce | 5 856 | - | - |
| *Funkce s pomocnou strukturou BN_CTX* | | | | |
| 3 | `BN_mod_add` | 8 310 | 869 | 1 157 |
| 4 | `BN_mod_sub` | 8 310 | 4 028 | 5 183 |
| 5 | `BN_mod_mul` | 9 552 | 84 730 | 274 088 |
| 6 | `BN_mod` | 4 176 | 270 | 338 |
| 7 | `BN_div` | 4 204 | 264 | 332 |
| 8 | `BN_mul` | 6 748 | 3 237 | 9 603 |
| | Všechny funkce | 9 816 | - | - |
| *Funkce s pomocnou strukturou BN_CTX a BN_MONT_CTX* | | | | |
| 9 | `BN_MONT_CTX_set` | 11 104 | 367 994 | 1 033 268 |
| 10 | `BN_mod_mul_montgomery` | 8 948 | 11 000 | 31 641 |
| | Všechny funkce | 12 010 | - | - |

Výsledné porovnání všech funkcí je pak názorně zobrazeno na Obr. 5.4. Z výsledků je patrná rostoucí tendence časové náročnosti jednotlivých funkcí s rostoucí velikostí velkého čísla. Pouze přechod ze 128 b na 256 b se projevil u některých funkcí značným nárůstem počtu cyklů, např. modulární násobení `BN_mod_mul` více jak 300 % nárůst. Nicméně u některých modulárních funkcí lze pozorovat značně rychlejší operace, tedy hlavně u funkce `BN_mod_add`. Je to hlavně díky tomu, že ve funkci není žádná funkce dělení, pokud by byla, odpovídala by rychlost této funkce přibližně rychlosti funkci `BN_mod_sub`. Dále díky optimalizované funkci bitového posuvu je funkce *BN_div* také znatelně rychlejší než ostatní funkce. Funkce `BN_MONT_CTX_set` je pak funkce pro inverzní modulo operace $m$ a je nejvíce náročná. Pokud porovnáme Montgomeryho násobení `BN_mod_mul_montgomery` s klasickou implementací modulárního násobení `BN_mod_mul`, pak Montgomeryho násobení vykazuje mnohem lepší výsledky. Nicméně

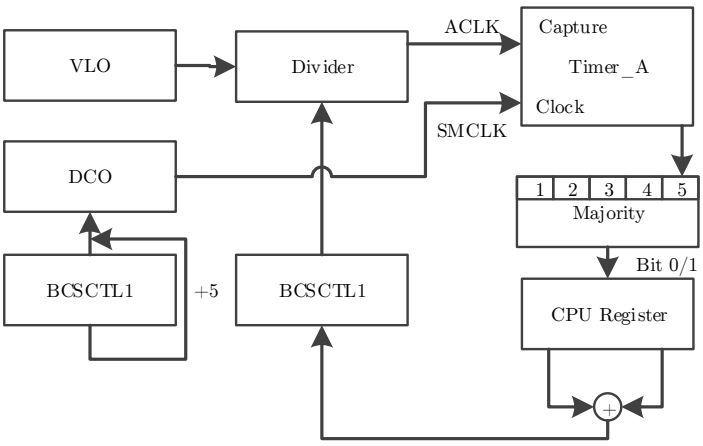
funkce Montgomeryho násobení využívá pomocné struktury `BN_MONT_CTX_set`, která je sice volána pouze jednou, ale je nutno brát toto v potaz. Tedy pokud používáme operaci násobení více jak pětkrát, jinak je efektivnější Montgomeryho násobení oproti klasickému, jinak je nutno použít klasickou funkci. Celá část funkcí modulární aritmetiky pak zabírá méně než 5 % paměti (12 kB/256 kB), což tedy ukazuje na velmi efektivní implementaci, která ponechává prostor na implementaci dalších funkcí uvažovaného kryptosystému či komunikačních i jiných funkcionalit.




Obr. 5.4: Srovnání časové náročnosti šifrování pro jednotlivé velikosti klíčů.

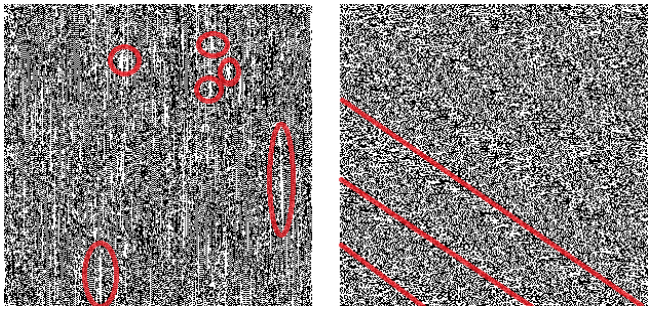
## 5.3 Generátor náhodných čísel

V rámci kapitoly 3.2 byla definována náhodná čísla a provedena analýza hlavních možností pro generování náhodných čísel. Kapitola 4.6 poukazuje na nutnost modulu náhodného generátoru v uvažovaném kryptosystému pro jednotlivé kryptografické algoritmy. Vybraný MCU má možnost využití jak externích periferií, tak interních hardwarových i softwarových periferií. Z tohoto důvodu byl započat výzkum v oblasti generování náhodných čísel. Nejprve byl vytvořen generátor založený na myšlence dvou protichůdných oscilátorů o různé frekvenci. Výsledná desynchronizace těchto oscilátorů pak tvoří náhodný děj, který je možné využít ke generování náhodných čísel. Myšlenka vychází z [148]. Prvotní návrh tohoto generátoru byl úspěšně publikován autory v odborném časopise [317] a následná rozšířená verze byla vyžádána mezinárodním vědeckým časopisem [318], kde je mj. podrobně vysvětlen i průběh implementace a základní funkčnost generátoru. Blokové schéma generátoru je zobrazeno na Obr. 5.5




Obr. 5.5: Blokové schéma navrženého náhodného generátoru čísel založeném na dvou oscilátorech (myšlenka pro návrh převzata z [148]).

Bloky VLO a DCO značí dané oscilátory, jedná se o vysoko-kmitočtový digitální oscilátor (DCO, z angl. Digitally controlled ocillator) o frekvenci 1 MHz a nízko-kmitočtový oscilátor (VLO, z angl. Very Low Oscillator) o frekvenci 12 kHz. Tyto oscilátory slouží jako zdroje pro interní hodiny ACLK/SMCLK, kde v časovači Timer_A je pak dána perioda pomalého oscilátoru. Po uběhnutí této periody se změří počet cyklů rychlého oscilátoru, který se v každé periodě mění. LSB je pak následně pomocí posuvného registru zapisován do paměti či proměnné, to tvoří hlavní myšlenku generátoru. Bloky BSCTL1 pak slouží pro vkládání různého startu oscilátorů pro zvětšení náhodnosti (viz [318], [317] a [148]). Knihovna obsahující generátor (ale i další implementované funkce popsané v tomto článku níže) je dostupné na [319]. Následně byla provedena evaluace generátoru z pohledu jeho náhodnosti a srovnání s klasickou matematickou funkcí `rand()` knihovny `math.lib` (s časovým vstupem jako seed). Jako první byl proveden jednoduchý vizuální test, kdy je nejprve vygenerována velká posloupnost "1" a "0", kterým je následně přiřazena bílá (pro 1) a černá (pro 0). Poté je vytvořen obrázek a následně je možné již pouhým okem rozeznat případnou pravidelnost a vzory. Výsledky vizuálního testu jsou zobrazeny na Obr. 5.6.



Obr. 5.6: Jednoduchý vizuální test vlevo vytvořený generátor a vpravo funkce `rand()` z knihovny math.

Jak je z obrázku patrné, tak matematická funkce `rand()` není zcela náhodná a objevují se zde jasné vzory. Oproti tomu námi vytvořený generátor dvou oscilátorů nemá pravidelné vzory (červené vyznačené příčné čáry), ale vyskytuje se u něj přílišný shluk jedniček a nul (červeně znázorněna bíla a černá místa tvořící vertikální čáry). Toto byl také mj. jeden z důvodů, proč bylo nutno pokračovat ve výzkumu a ověřování daného generátoru. V rámci dalšího testování byla testována statistická hypotéza $H_0$, zda je daný generátor náhodný či nikoliv. Hypotéza je testována pomocí pravděpodobnosti a je nutno tedy počítat s možnou chybou, tu tvoří: (i) chyba typu I a (ii) chyba typu II. V rámci chyby typu I je díky pravděpodobnosti rozhodnuto, že generátor není náhodný i přesto, že skutečně náhodný je. To je zapříčiněno podstatou generátoru, kdy je možné, aby TRGN generoval nějakou dobu sekvenci bitů, která se bude zdát náhodná, protože máme např. pouze malý vzorek, ale ve výsledném dlouhodobém testován je generátor náhodný. Druhá chyba typu II vzniká stejným způsobem, nicméně efekt je opačný. Tedy generátor se zdá být náhodný, i když je skutečně nenáhodný. Ukázku možný výsledků při testování hypotézy, společně s případnou chybou shrnuje Tab. 5.2.

Tab. 5.2: Ukázka možných výsledků statistických testů hypotéz.

| **Skutečnost** | **Závěr** | |
|---|---|---|
| | $H_0$ je přijata | $H_0$ je odmítnuta |
| $H_0$ je pravdivá | *Správný závěr* | *Chyba typu I* |
| $H_0$ není pravdivá | *Chyba typu II* | *Správný závěr* |

Pro testování námi stanovené hypotézy byl vybrán statistická baterie testů DIEHARD [320] a NIST [321] (v těchto příručkách jsou dále popsány mj. i podrobně využívané testy). V rámci těchto testů je tedy ověřována hodnota $p$ či $p - value$, která nabývá hodnot od 0,0–1,0 (tj. 0–100 %). V rámci testů pak volíme prahovou hodnotu $\alpha$, která určuje námi požadovanou hodnotu jistoty výsledného tvrzení (zda generátoru je náhodný či nikoliv). Tedy např. pokud zvolíme $\alpha = 1\,\%$, znamená

to, že můžeme s $p - \alpha$ jistotou říci, že test je pravdivý. Čím vyšší jistota, tím jsou následně vyšší nároky testů, kde pokud $\alpha = 0,01\,\%$ a požadujeme jistotu $99,99\,\%$, pak se blížíme téměř ideálnímu TRGN (a navíc zvyšujeme riziko chyby typu I). Z tohoto důvodu v dále provedených testech byla $\alpha = 1\,\%$ a pravděpodobnost tvrzení tedy $99\,\%$, v každém testu bylo generováno $10^{11}$ bitů, posloupnost následně byla rozdělena na 1 mil. bloky a bylo provedeno 100 tis. testů, což by mělo dostatečně omezit statistickou chybu. Z těchto hodnot byl následně vytvořen histogram rozložení pravděpodobnosti, kde černá čárkovaná horizontální čára bude představovat ideální rozložení pravděpodobnostní funkce. Prahová hodnota 0,01 % je pak začleněna do intervalu 0,0–0,1 (tedy tento sloupec mj. obsahuje i testy, které skončili neúspěšně). V rámci druhé fáze testů byl zvolen frekvenční monobitový test (z angl. Frequency Monobit Test), který kontroluje vyváženost generování "1" a "0". Testuje se tedy posloupnost $\epsilon$ o $n$ bitech ($\{\epsilon_1, ..., \epsilon_n\}$), kdy je nejprve transformována tato posloupnost do statistické proměnně $\epsilon \rightarrow S$:

$$S_n = \sum_{i=1}^{n} x_i, x_i = 2\epsilon_i - 1, \tag{5.2}$$

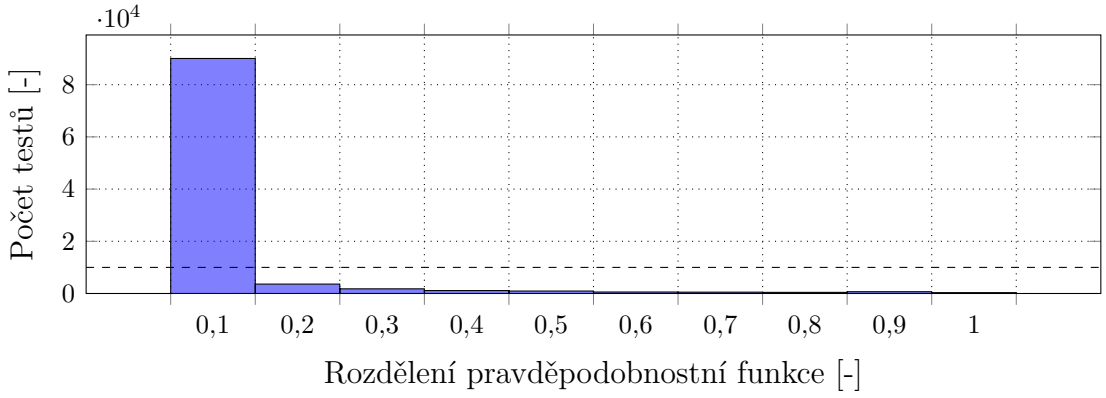
z které je následně počítán statistický test $s_{obs}$:

$$S_{obs} = \frac{|S_n|}{\sqrt{2}}, \tag{5.3}$$

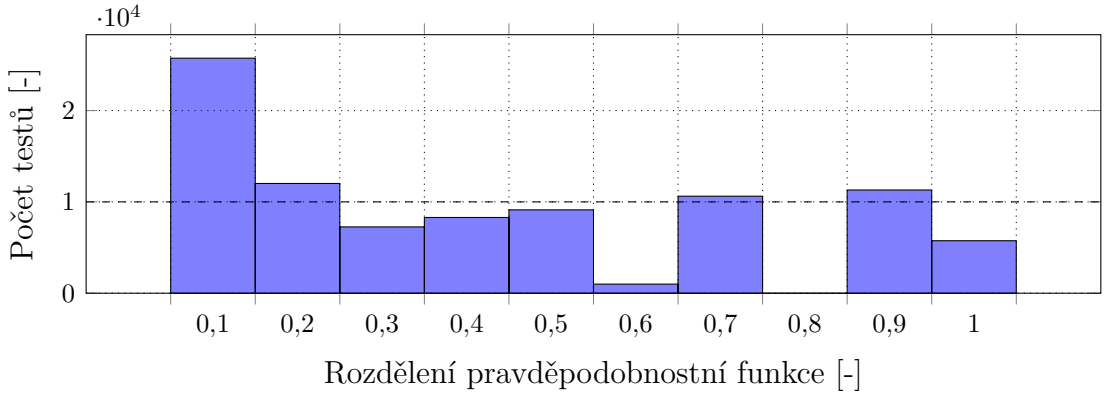
a následně í výsledná pravděpodobnostní hodnota $P - value$:

$$P\_value = erfc\{\frac{s_{obs}}{\sqrt{2}}\}, erfc(x) = \frac{2}{\sqrt{\pi}} \int_x^{\infty} e^{-t^2} dt, \tag{5.4}$$

kde $erfc()$ je komplementární chybová funkce. Následně je tedy aplikována kritická hodnota $\alpha$ a rozhodnuto zda je hypotéza zamítnuta ($P - value < \alpha$) či přijata ($P - value < \alpha$). Výsledky testu funkce *rand()* jsou zobrazeny na Obr. 5.7 (pseudonáhodná funkce `rand()`) a Obr. 5.8 (vyvinutý vlastní generátor). V histogramech je zjednodušeně značen interval $[X - -Y)$ pouze jako $Y$ a vždy je inkrementován o 0,1 (tedy 0,0–0,1; 0,1–0,2;...;0,9–1,0), tento způsob je dále využit v celé kapitole pro vytvořené statistické testy.

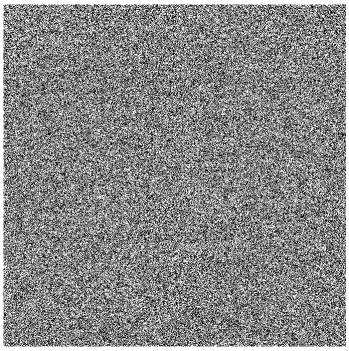



Obr. 5.7: Histogram rozložení výsledků pravděpodobnostní funkce pro pseudonáhodný generátor `rand()`.



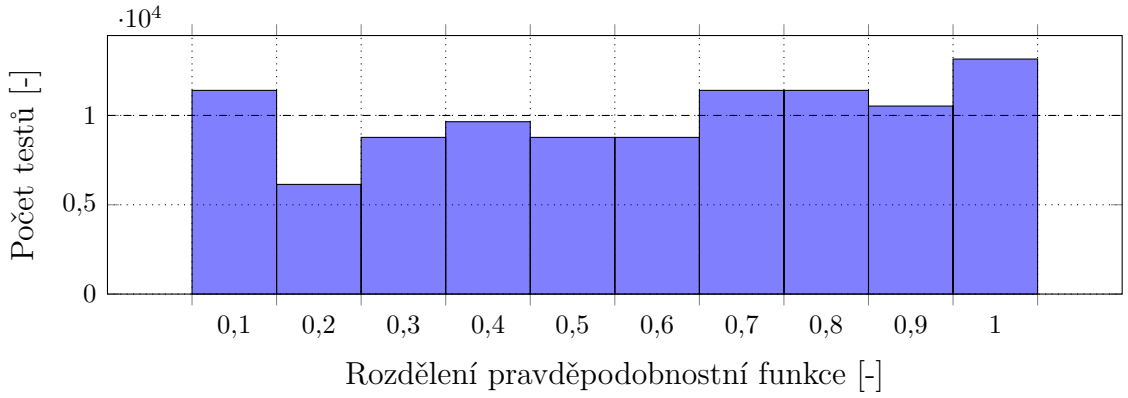

Obr. 5.8: Histogram rozložení výsledků pravděpodobnostní funkce pro vytvořený generátor založený dvou oscilátorech.

Generátor založený na funkci `rand()`, dle předpokladu, má většinu výsledků v rozsahu 0,0–0,1, což tedy znamená, že s velkou pravděpodobností většina testů zamítla hypotézu $H_0$. Naproti tomu námi navržený generátor má pouze mírně zvýšené hodnoty v intervalu 0,1 a vykazuje anomálie v oblasti 0,6 a 0,8. Generátor tedy není ideální, což však bylo potvrzeno již vizuálním testem. Výsledky jsou však mnohonásobně lepší oproti velmi nevyrovnanému generátoru `rand()`. Výsledky byly úspěšně publikovány autorem a diskutovány na mezinárodní vědecké konferenci TSP2014 [322]. Následně proběhla optimalizace práce s pamětí (vytvořená dynamická alokace a využití místo statických proměnných registrů mikrokontroléru), optimalizace nastavení módu Timeru (dříve count-up, nyní continuous mód přes hodnotu 0x 0FFFFh, o jednotlivých módech je diskutováno v dokumentaci MCU [316], aj.). Prvotní vizuální test generátoru je na Obr. 5.9.



Obr. 5.9: Jednoduchý vizuální test optimalizovaného generátoru dvou oscilátorů.

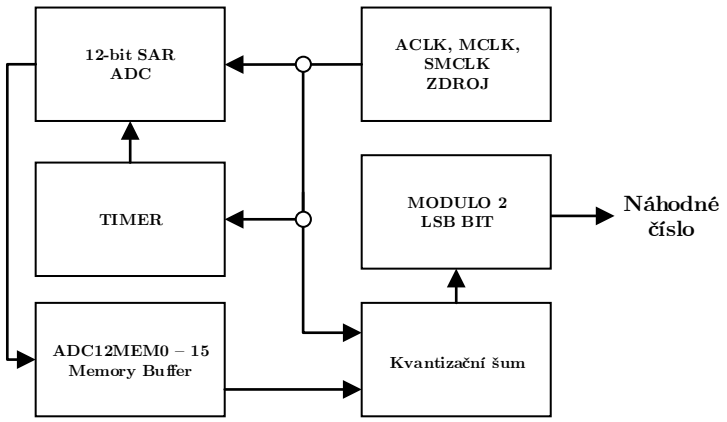
Jak můžeme vidět tak již z vizuálního testu můžeme vidět značné zlepšení rozložení “1” a “0”, kde výsledný vizuální efekt vypadá skutečně náhodně. Dále byl také proveden statistický test jako v prvním případě pro získání porovnatelných výsledků, které jsou zobrazeny na Obr.5.10




Obr. 5.10: Histogram rozložení výsledků pravděpodobnostní funkce pro optimalizovaný generátor dvou oscilátorů.

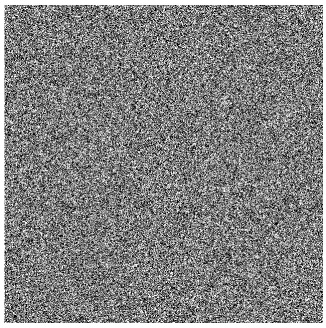
Jak můžeme vidět, tak proběhlo vyrovnání jednotlivých statistických testů, kdy generátor se nyní velice blíží ideálním hodnotám. Výzkum v této oblasti pokračoval návrhem dalšího generátoru založeném na bázi šumu. Využití jevu šumu není zcela novinkou, naopak se jedná o klasický jev, který je využíván v mnohých generátorech, např. [323, 324, 325], ale i spousty dalších. Vlastní myšlenka zde spočítá v návrhu a využití specifických hardwarových prvků MCU, které jsou většinou obsaženy také v jiných MCU využívaných v oblasti inteligentních sítí či telemetrických systémů. V rámci telemetrických systému je často využíváno analogových měřících zařízení [326]. Z tohoto důvodu jednotky MCU většinou obsahují převodníky analogového signálu na digitální signál (ADC, z angl. Analogue-to-Digital Converter). Převod analogového signálu na digitální signál však bývá vždy doprovázen jistou ztrátou

užitečného signálu, zapříčiněn citlivostí převodník, ale také parazitními šumy [327]. Z tohoto důvodu je v této oblasti prováděn rozsáhlý výzkum potlačení šumu u ADC převodníků, tak aby se výsledný signál blížil ideálnímu, tj. analogovému (viz např. [328, 329, 330], aj.). Pokud však nevyužijeme prvků pro odstranění parazitního šumu u ADC převodníku, pak výsledný signál výstupu ADC obsahuje i náhodnou složku šumu. Vlastní návrh generátoru pak spočívá ve využití tohoto signálu (kvantizačního šumu, tedy chyba vzniklá převodem analogového signálu na digitální) ke generování náhodné bitové posloupnosti. Blokové schéma generátoru je zobrazeno na Obr. 5.11.



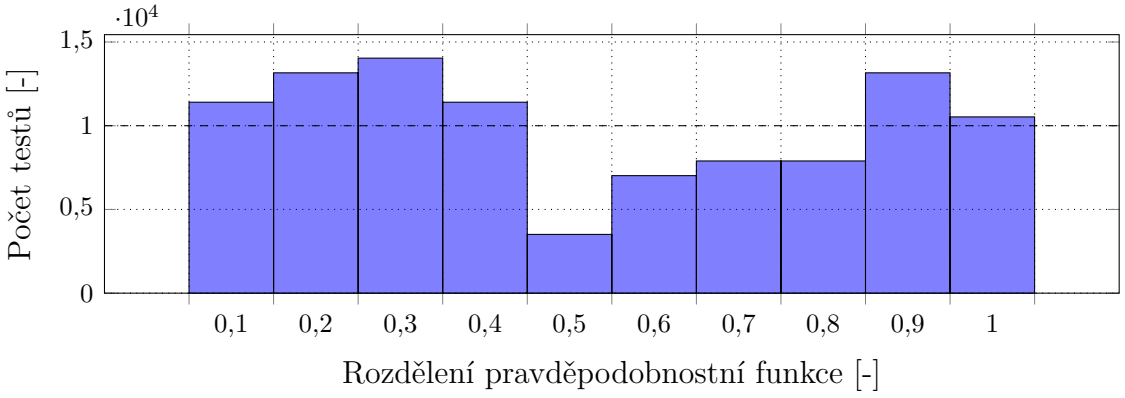

Obr. 5.11: Blokové schéma navrženého náhodného generátoru čísel založeném kvantizačním šumu.

Blok ADC představuje tedy konvertor analogového signálu (získaného z reálného nízkofrekvenčního oscilátoru VLO, který je zdrojem pro interní hodiny ACLK/MCLK/SMCLK, které slouží jako vstup ADC). Signál je mj. také přiveden do časovače, který následně ovlivňuje hodnotu kvalitu kvantování (je to další aditivní prvek náhodnosti), a do bloku Kvantizační šum, který slouží k porovnání reálného signálu s digitálním (pro získání složky šumu, resp. kvantizační chyby). ADC následně převede signál a uloží jej do Memory bufferu (paměť MCU), kde tento signál je následně srovnáván v bloku kvantizační šum s předchozím. Jako poslední je pak využit LSB bit z kvantizační chyby, který představuje vygenerovaný náhodný bit generátorem. Prvotní vizuální test generátoru je na Obr. 5.12.



Obr. 5.12: Jednoduchý vizuální test generátoru kvantizačního šumu.

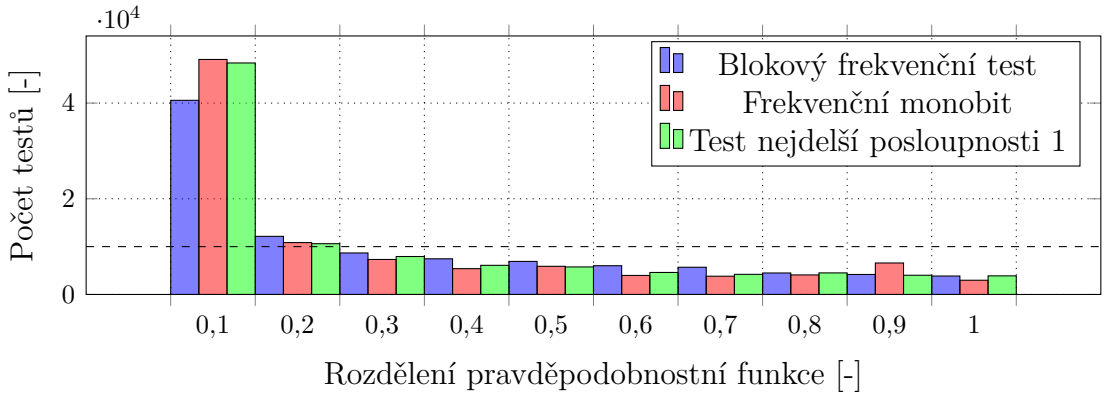
Jak můžeme vidět tak výsledek je srovnatelný s optimalizovaným generátorem dvou oscilátorů. Opět zde nejsou žádné znatelné vzory či velké shluky “1” či “0”. Dále byl také proveden statistický monobitový test, kde jeho výsledky jsou zobrazeny na Obr. 5.13.



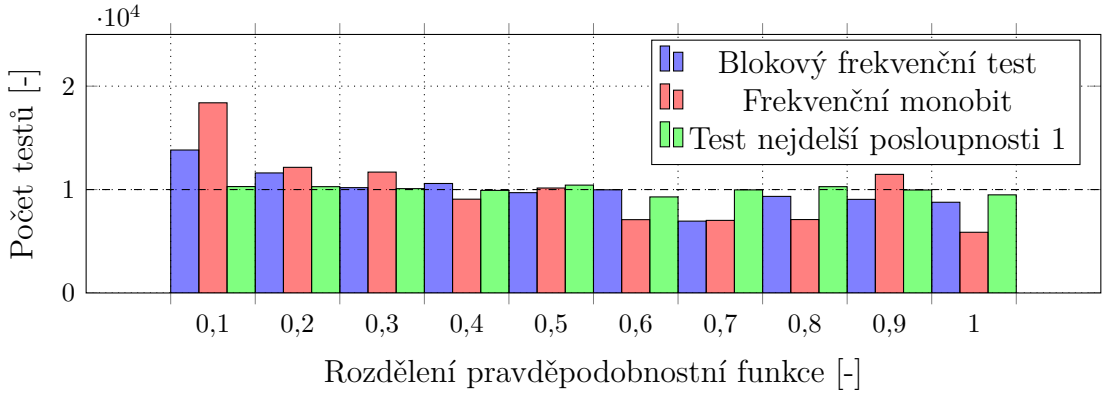

Obr. 5.13: Histogram rozložení výsledků pravděpodobnostní funkce pro vytvořený generátor kvantizačního šumu.

Jak můžeme vidět, tak námi vytvořený druhý generátor založený na kvantizačním šumu vykazuje oproti optimalizovanému generátoru méně kvalitní výsledky, kdy jednotlivé rozsahy histogramu se vzdalují od ideální hodnoty. Toto však nemusí znamenat menší náhodnost, pouze, že v rámci sekvence $10^{11}$ vykázal horší výsledky v rámci statistického rozložení. Idea, návrh a prvotní ověření generátoru kvantizačního šumu byly úspěšně prezentovány na mezinárodní vědecké konferenci TSP 2016 [331]. V rámci ověření generátorů byly provedeny další sady testů tedy blokový frekvenční test, kdy se testují tedy předem dané bloky “1” a 0”, které jsou ověřovány stejně jako u monobitového testu jejich % počet v rámci bloku. Dále pak test nejdelší posloupnosti “1” (“0”), tedy testování shluků jednotlivých bitů. Jedná se o nejčastěji používané testy v rámci testování náhodnosti. Pro tyto testy byla vygenerována nová posloupnost $10^{11}$, velikost bloku u blokového testu byla 100 b. Výsledky jednotlivých

generátorů jsou pak na Obr. 5.14 (optimalizovaný generátor dvou oscilátorů) a 5.15 (generátor kvantizačního šumu).




Obr. 5.14: Rozsáhlé pravděpodobnostní testy pro optimalizovaný generátor dvou oscilátorů.




Obr. 5.15: Rozsáhlé pravděpodobnostní testy pro generátor kvantizačního šumu.

V tomto testu se jeví jako mnohem ideálnější generátor kvantizačního šumu, kde křivka hladin histogramu více odpovídá hladině ideálního generátoru. Je nutno říci, že odchylka od předpokládané ideálnosti je dobrou vlastností kvalitního generátoru, jelikož přesné kopírování ideální hodnoty poukazuje na nenáhodnost generátoru (což je paradox). V neposlední řádě parametrizace obou generátorů shrnuje Tab. 5.3.

Tab. 5.3: Shrnutí parametrizace jednotlivých vlastních generátorů.

| **Typ generátoru** | **Rychlost [kB/s]** | **Gen. 128 b [ms]** | **Flash [B]** | **RAM [B]** |
|---|---|---|---|---|
| Opt. G. dvou oscilátorů | 1,75 | 73,142 | 4608 | 1628 |
| G. kvantizačního šumu | 19,175 | 6,675 | 4312 | 1774 |

Všimnout si můžeme mnohonásobně vyšší rychlosti kvantizačního generátoru oproti generátoru dvou oscilátorů. Je to převážně dáno tím, že generátor není zpožďován periodou VLO, jako u generátoru dvou oscilátorů. Dále pak tento generátoru pracuje více s pamětí RAM, aby se dosáhlo nejvyšších úspor elektrické energie, viz 5.3. Výzkum v této oblasti pokračuje, nicméně v nynější fázi je zvolen generátor ADC pro generování náhodných parametrů ostatních bloků, jako vhodnější oproti generátoru dvou oscilátorů z pohledu rychlosti i náhodnosti. Energetická spotřeba je pak přímo úměrná rychlosti generování a velikosti generované posloupnosti (v AM módu byl pro oba generátory teoretický odběr $I_{cc} = 300\mu A$ a $V_{cc} = 3V$). Z tohoto pohledu je tedy rychlejší generátor kvantizačního šumu efektivnější i z pohledu energetické náročnosti. Z pohledu komunikace je pak rychlejší generování parametrů také žádoucí, jelikož každý prvek následně přispívá k zvyšování výsledného komunikačního zpoždění.

## 5.4 Modul pro autentizaci a šifrování

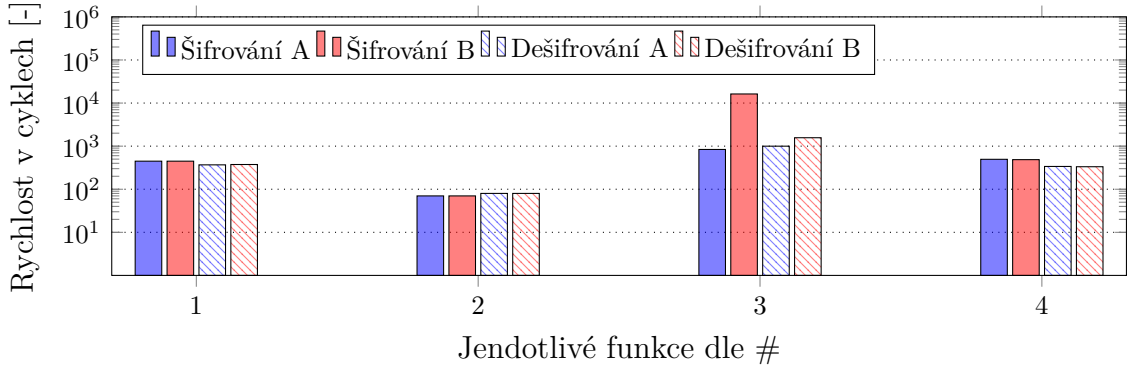
V rámci implementace algoritmu AES BC/ECB byly uvažovány tedy dvě knihovny [313] (v textu značeno jako metoda A) a [312] (v textu značeno jako metoda B). Obě tyto knihovny byly implementovány do navrženého kryptosystému. V rámci ověření těchto knihoven a výběru nejlepší z nich bylo provedeno první srovnávací měření na vybraném MCU. Výsledky prvotního měření jsou v Tab. 5.4, tabulka je rozdělena dle jednotlivých operací prováděných v rámci algoritmu AES (více o jednotlivých operací viz standardizace AES [220]) a dle šifrování a dešifrování. Výsledky uvedené v tabulce jsou vždy mediánem z 10 měření (byl využit klíč o velikosti 128 b). Pro přehlednost zavádíme opět identifikátor jednotlivých operací #. V neposlední řadě měření jsou prováděny pro AES-128 v módu CBC, který je z vybraných dvou módů nejnáročnější.

Tab. 5.4: Prvotní porovnání různých knihoven symetrického blokového algoritmu AES-128.

| | | **AES - Metoda A** | | **AES - Metoda B** | |
|---|---|---|---|---|---|
| | | **Šifrování** | **Dešifrování** | **Šifrování** | **Dešifrování** |
| Bajtová substituce (#1) | Cykly | 448 | 448 | 368 | 375 |
| Prohození řádků (#2) | Cykly | 70 | 70 | 80 | 80 |
| Kombinace sloupců (#3) | Cykly | 838 | 16259 | 999 | 1568 |
| Přidání podklíče (#4) | Cykly | 495 | 486 | 338 | 333 |
| Celá runda | Cykly | 1851 | 17263 | 1806 | 2384 |
| Poslední runda | Cykly | 1004 | 1003 | 817 | 815 |
| **Cyklů celkem** | Cykly | 19035 | 157743 | 17520 | 26161 |
| **FLASH paměť celkem** | B | 7586 | | 2226 | |
| **RAM paměť celkem** | B | 2034 | | 160 | |

Prvotní měření ukázalo velké rozdíly v efektivitě, kde metoda B tedy byla značně

rychlejší. Metoda A měla zanedbatelně efektivnější operaci prohození řádků, což se však ve výsledné náročnosti téměř neprojevilo (i díky mnohem pomalejším ostatním metodám). Výsledky experimentálního měření a validace knihoven symetrické kryptografie byly úspěšně publikovány autorem na vědecké konferenci EEICT 2015 v rámci doktorandské soutěže, kde práce získala ocenění 2. místa [332] (článek byl následně také podstatně rozšířen o popisy jednotlivých funkcí AES a publikován v odborném časopise [333]). Obr. 5.16 již ukazuje grafické srovnání jednotlivých operací.




Obr. 5.16: Srovnání vybraných šifrovacích algoritmů - metoda A, metoda B.

Jak můžeme vidět operace dešifrování u metody A vykazuje značně velký rozdíl u operace prohození řádků oproti šifrování a obecně se zde jedná o nejnáročnější funkci. Byla provedena analýza kódu jednotlivých implementací, aby bylo jasné, jaký je důvod těchto anomálií. V rámci metody A je se využívá tzv. před-počítacího makra pro násobení, což by mělo ve výsledku zefektivnit výslednou rundu. Dále se využívá struktur čtyř *unsigned_char* pro jednotlivé proměnné a dvou rozměrné pole pro matici stavu S 4x4. Naproti tomu metoda B využívá před-počítací funkci násobení v konečném poli, dále třech *unsigned_char* struktur a pouze jednorozměrného pole pro matici stavu S 4x4 (tedy transformace do 1x16). Srovnání počtu jednotlivých operací je v Tab. 5.5.

Tab. 5.5: Počet jednotlivých operací v rámci vybraných metod AES.

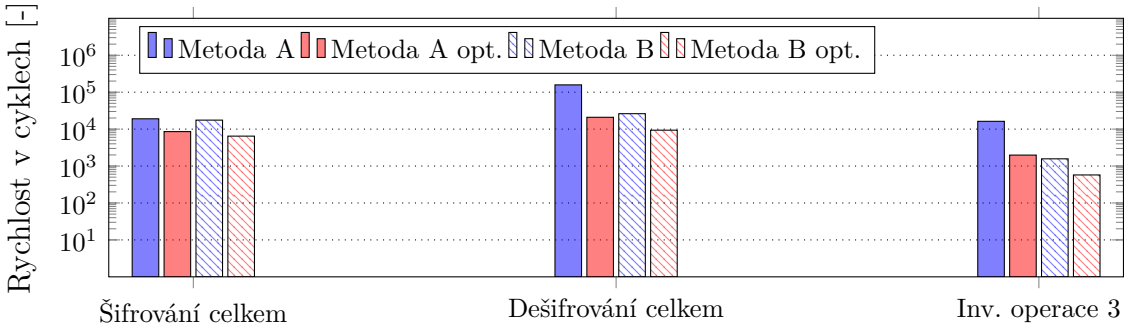
| **Operace** | **Metoda A** | **Metoda B** |
|---|---|---|
| cyklus for | 1 | 1 |
| operace násobení | 60 | 0 |
| operace sčítání | 0 | 20 |
| bitové posuvy | 384 | 10 |
| logické AND | 240 | 0 |
| logické XOR | 76 | 30 |
| bitové operace celkem | 700 | 40 |

Jak můžeme vidět tak z analýzy jednotlivých implementací jednoznačně plyne, proč je operace inverzního kombinace sloupců (tedy kombinace sloupců při dešifrování) tak markantně pomalejší. Operace násobení jsou mnohokrát pomalejší než operace sčítání, kde metoda B využívá převážně sčítacích operací. Dále v rámci metody A je použito nadměrné množství bitových operacích a také dvourozměrné pole, což jsou další faktory zpomalující chod dané knihovny. Následně byla provedena implementace vlastních aritmetických i modulárních funkcí představených v kapitole 5.2, zakomponována vlastní struktura velkých čísel a provedena softwarová optimalizace. Následně proběhlo další měření stejných funkcí obou knihoven, kde výsledky jsou zobrazeny v následující Tab. 5.6.

Tab. 5.6: Výsledky experimentálního měření optimalizovaných knihoven symetrického blokového algoritmu AES-128.

| | | **AES - Metoda A** | | **AES - Metoda B** | |
|---|---|---|---|---|---|
| | | **Šifrování** | **Dešifrování** | **Šifrování** | **Dešifrování** |
| Bajtová substituce (#1) | Cykly | 124 | 124 | 111 | 111 |
| Prohození řádků (#2) | Cykly | 56 | 56 | 48 | 50 |
| Kombinace sloupců (#3) | Cykly | 591 | 1980 | 344 | 574 |
| Přidání podklíče (#4) | Cykly | 99 | 99 | 105 | 91 |
| Celá runda | Cykly | 870 | 2259 | 659 | 869 |
| Poslední runda | Cykly | 279 | 279 | 410 | 283 |
| Cyklů celkem | Cykly | 8561 | 20912 | 6460 | 9357 |
| FLASH paměť celkem | B | 5284 | | 2628 | |
| RAM paměť celkem | B | 2034 | | 160 | |

Srovnání neoptimalizované a optimalizované (značeno jako opt.) verze je graficky znázorněno na Obr. 5.17, kde je zobrazeno srovnání náročnosti pro celkový proces šifrování, celkový proces dešifrování a inverzní kombinace sloupců (#3).




Obr. 5.17: Srovnání vybraných šifrovacích algoritmů - metoda A, metoda B.

Jak můžeme vidět, provedená optimalizace znatelně snížila výpočetní náročnost jednotlivých metod, kdy metoda A je nyní téměř srovnatelná s metodou B. U metody

A došlo ke snížení výpočetní náročnosti o více než 80 % a povedlo se snížit i jednotlivé paměťové nároky, díky předchozí špatné práci s pamětí (neoptimalizované datové typy, aj.) a zahrnutí vlastních metod pro reprezentaci velkých čísel (Flash nároky o více než 30 % a RAM nároky zůstaly stejné). U metody B došlo k nárůstů o 400 B pro FLASH paměť cca 20 % (RAM paměťové nároky zůstaly stejné), ale snížení výpočetní náročnosti o více než 60 %. Vzhledem k velikosti Flash paměti 256 kB se jedná o nárůst 0,16 % za cenu snížení výpočetní náročnosti o více než 60 %, což lze považovat za efektivní. Softwarová analýza a optimalizace obou knihoven byla úspěšně publikována autorem v rámci konference CSOC 2017 [309] (indexováno ve Scopus a WoS).

## 5.5 Modul pro dohodu symetrického tajného klíče

V rámci poslední fáze tvorby hybridního kryptosystému byla vytvořena knihovna asymetrické kryptografie využívající eliptických křivek. Nejprve byl vytvořen návrh vycházející z klasického algoritmu Diffieho Hellmana, tento návrh byl autorem úspěšně publikován na vědecké konferenci EEICT 2013 [334]. Následně již byla vytvořena knihovna, obsahující funkce algebraických a modulárních operací s eliptickými křivkami a dále také funkce pro dohodu sdíleného tajemství (např. tajného symetrického klíče) pomocí algoritmu ECDH. Knihovnu je dostupná z [314], knihovna mj. obsahuje také funkce popsané v kapitole 5.2, které řeší modulární aritmetiku při práci s eliptickými křivkami. Jako první bylo implementováno celkem 34 eliptických křivek nad polem řádu 2 ($\mathbb{F}_{2^m}$) standardů NIST [335], SECG [336] a ANSI [337] o velikosti 113 b až 571 b. V době implementace se jednalo o jedinečnou softwarovou implementaci takto velkých křivek na limitovaném MCU (v dané době byla častá velikost křivek do 256 b a ojediněle 256 b), což jen prokazuje efektivnost navržených algoritmů. Jedná se o tyto křivky (jména křivek vychází ze standardizace, čísla 131–571 značí velikost křivky resp. $m$):

- $\mathbb{F}_{2^{113}}$–$\mathbb{F}_{2^{131}}$: `sect113r1`, `sect113r2`, `sect131r1`, `sect131r2`.
- $\mathbb{F}_{2^{163}}$–$\mathbb{F}_{2^{208}}$: `sect163k1`, `sect163r1`, `sect163r2`, `c2pnb163v1`, `c2pnb163v2`, `c2pnb163v3`, `c2pnb176v1`, `c2tnb191v1`, `c2tnb191v2`, `c2tnb191v3`, `sect193r1`, `sect193r2`, `c2pnb208w1`.
- $\mathbb{F}_{2^{233}}$–
- $\mathbb{F}_{2^{239}}$: `sect233k1`, `sect233r1`, `sect239k1`, `c2tnb239v1`, `c2tnb239v2`, `c2tnb239v3`.
- $\geq \mathbb{F}_{2^{272}}$: `c2pnb272w1`, `sect283k1`, `sect283r1`, `c2pnb304w1`,`c2tnb359v1`, `c2pnb368w1`, `sect409k1`, `sect409r1`, `c2tnb431r1`,`sect571k1`, `sect571r1`.

Knihovna má hlavní tři části. První je objekt (struktura):

```
EC_KEY *EC_KEY_new_by_curve_name(int nid);
```

ve které jsou uloženy veškeré potřebné parametry, se kterými se dále pracuje a to dle požadované křivky (parametr `nid`, jednotlivé křivky jsou pak popsány v dokumentaci). Následně funkce pro generování veřejného a soukromého klíče:

```
int EC_KEY_generate_key(EC_KEY *eckey,int priv_is_set);
```

Pokud je druhý parametr `priv_is_set` = 1 tak se očekává, že soukromý klíč je již vygenerován. Jako poslední funkce pro validaci ECDH:

```
int ECDH_compute_key(void *out,size_t outlen,const EC_POINT *pub_key,EC_KEY *eckey);
```

První parametr `out` představuje bufer, parametr `outlen` je hašovací funkce (může být `NULL`), parametr `pub_key` je veřejný klíč druhé strany a `eckey` je vlastní soukromý klíč. Jako první byly implementovány křivky nad polem řádu 2 ($F_{2^m}$). Tyto křivky jsou jednodušší na implementaci, nicméně jak ukázaly následné experimentální měření, tak pokud není provedena hardwarová akcelerace, tak jsou tyto křivky velice pomalé. Výsledky experimentálního měření jednotlivých křivek na vybraném MCU jsou v Příloze C (jedná se o jeden proces dohody symetrického klíče o velikosti 128 b, hodnoty jsou uvedeny pro jednu komunikační stranu bez uvažovaného komunikačního či jiného zpoždění).

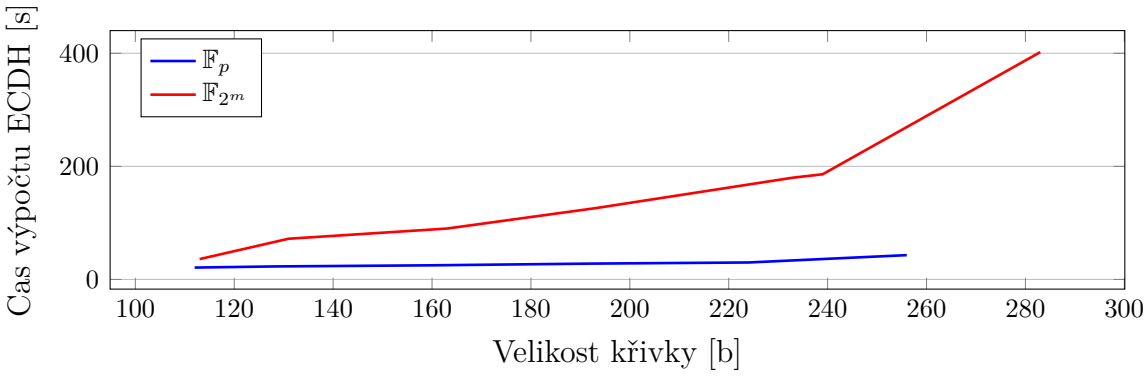
Jak můžeme vidět, tak implementace nabízí opravdu velké množství různorodých křivek, rozsáhlá experimentální měření pak prokázala funkčnost těchto křivek na vybraném MCU a ve vytvořené implementaci. Nicméně jak potvrdil teoretický rozbor tak eliptické křivky nad polem o řádu 2 jsou velice pomalé, pokud se nejedná o hardwarovou implementaci či není k dispozici hardwarová akcelerace. Jak můžeme vidět tak pro křivky, které by byly nutné použít v kombinaci s AES-128 (tj. křivky s $\mathbb{F}_{2^{256}}$ a více), je čas více než 10 m, což je velký problém z pohledu spotřeby, ale i v rámci samotné komunikace. Výsledky experimentálních textů a také jedinečná implementace eliptických křivek byla publikována v rámci konference TSP 2014 [308] (indexované ve Scopus a WoS).

Z důvodu malé efektivity eliptických křivek o řádu 2, byla hledána alternativa v podobě jiných křivek. Z teoretického rozboru pak vyplynula možnost křivek nad polem prvočíselného řádu $\mathbb{F}_p$. Tyto křivky jsou mnohem složitější na implementaci, nicméně nabízejí velkou variaci optimalizace a tak mohou být v softwarové implementaci mnohem rychlejší než eliptické křivky $\mathbb{F}_{2^m}$. V rámci implementace se pak povedlo implementovat 27 eliptických křivek nad polem prvočíselného řádu $\mathbb{F}_p$ o velikosti 112 b až 521 b. standardů NIST [335], SECG [336] a ANSI [337]. V době implementace se jednalo opět o velice jedinečnou softwarovou implementaci, kde implementaci eliptických křivek nad polem $\mathbb{F}_{256}$ se v danou dobu věnovalo pouze

velice omezené množství vědeckých prací. Jedná se o tyto křivky (jména křivek vychází ze standardizace:

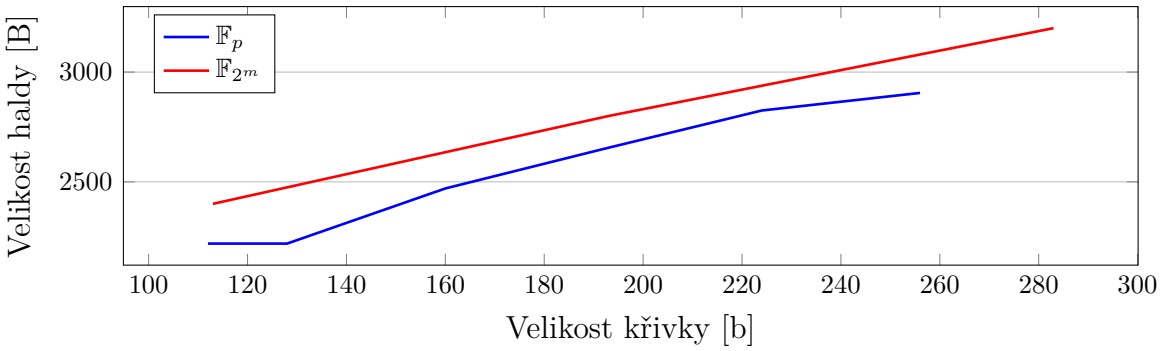
- $\mathbb{F}_{112}$–$\mathbb{F}_{128}$: `secp112r1`, `secp112r2`, `wtls6`, `wtls8`, `secp128r1`, `secp128r2`.
- $\mathbb{F}_{160}$–$\mathbb{F}_{192}$: `secp160k1`, `secp160r1`, `secp160r2`, `wtls7`, `wtls9`, `secp192r1`, `secp192k1`, `prime192v1`,`prime192v2`, `prime192v3`.
- $\mathbb{F}_{224}$–$\mathbb{F}_{239}$:: `secp224k1`, `secp224r1`, `secp224r2`, `wtls12`, `prime239v1`, `prime239v2`, `prime239v3`.
- $\geq \mathbb{F}_{256}$: `secp256k1`, `prime256v1`, `secp384r1`, `secp521r1`.

Křivky o velikosti 112 b až 256 b byly úspěšně ověřeny v rámci algoritmu ECDH, křivky o velikosti nad 256 b se bohužel dále nepodařilo dostatečně optimalizovat, tak aby je bylo možné využít pro algoritmus ECDH. Problémem byla nedostatečná paměť při modulárních operacích a příliš dlouhá doba výpočtu, kdy i následně ve většině případů přetékala paměť. Nicméně s úspěšně implementovanými křivkami byly provedeny experimentální testy a ověřena jejich efektivnost vůči předchozím křivkám $\mathbb{F}_{2^m}$. Výsledky srovnání časové náročnosti jednotlivých typů vybraných křivek jsou zobrazeny na Obr. 5.18.




Obr. 5.18: Srovnání jednotlivých typů křivek nad polem řádu 2 a prvočíselného řádu.

Jak můžeme vidět, tak časová náročnost z několika minut klesla na pouhých několik sekund, což v uvážení četnosti využití algoritmu ECDH je již reálně využitelné i v systémech s omezeným přístupem k elektrické energii. Z pohledu paměťové náročnosti pak křivky nad polem prvočíselného řádu vykazovaly také lepší výsledky cca o 100–200 B. Výsledky měření paměťové náročnosti jsou zobrazeny na Obr. 5.19.




Obr. 5.19: Srovnání jednotlivých typů křivek nad polem řádu 2 a prvočíselného řádu.

Implementace křivek nad polem prvočíselného řádu, společně s porovnáním obou typů křivek byla autorem úspěšně publikována v impaktovaném časopise [310]. Díky výsledkům experimentálního měření se dále výzkum zabýval různorodostí křivek a studováním jejich parametrů. Byly provedeny další experimentální testy rozsáhlé skupiny implementovaných eliptických křivek $\mathbb{F}_p$. Bylo zjištěno, že typ eliptické křivky má markantní vliv na efektivnost jednotlivých algoritmů. Výsledky experimentálních měření jsou zobrazeny v Tab. 5.7 (měřen byl opět proces ECDH).

Tab. 5.7: Výsledky experimentálního měření eliptických křivek nad polem prvočíselného řádu, dle jejich typu.

| Křivka | Velikost [b] | CPU [-] | Rozdíl [%] | Standard |
|---|---|---|---|---|
| `secp112r1` | 112 | 139276 | 0,00% | SECG |
| `wtls8` | 112 | 154206 | 10,72% | WTLS |
| `wtls6` | 112 | 155225 | 11,45% | WTLS |
| `secp112r2` | 112 | 161508 | 15,96% | SECG |
| `secp128r1` | 128 | 171116 | 0,00% | SECG |
| `secp128r2` | 128 | 183768 | 7,39% | SECG |
| `wtls7` | 160 | 184404 | 0,00% | WTLS |
| `secp160r1` | 160 | 184673 | 0,15% | SECG |
| `secp160r2` | 160 | 197593 | 7,15% | SECG |
| `secp160k1` | 160 | 213400 | 15,72% | SECG |
| `wtls9` | 160 | 277533 | 50,50% | WTLS |

Tabulka popisuje rychlost jednotlivých křivek (CPU) v cyklech. Měření v cyklech bylo zvoleno pro lepší transparentnost výsledků v rámci vědecké komunity (časová náročnost v sekundách/inutách byla v prvních měřeních zvolena z důvodu prokázání praktické využitelnosti křivek). Dále je v tabulce rozdíl v % (tedy poměr vůči nejrychlejší křivce daného řádu $p$, která je značena jako 0,00 %). Všimnout si můžeme, že správnou volbou křivky jsme v dané kategorii schopni získat 7–50 % procent výkonu. To může mít ve výsledku nezanedbatelný dopad na výslednou efektivitu uvažovaného systém. Pokud následně srovnáme nejpomalejší křivku daného řádu

s nejrychlejší křivkou řádu vyššího, dostaneme velice zajímavé výsledky, viz Tab. 5.8 (SL znamená nejpomalejší, tedy z angl. Slowest, a FA nejrychlejší z angl. Fastest).

Tab. 5.8: Srovnání nejpomalejší křivky s nejrychlejší křivkou vyššího řádu.

| Curves | Variances [%] |
|---|---|
| $112_{SL} : 128_{FA}$ | 5,61 % |
| $128_{SL} : 160_{FA}$ | 0,34 % |
| $160_{SL} : 192_{FA}$ | 12,72 % |
| $192_{SL} : 224_{FA}$ | 4,62 % |

Jak můžeme vidět, tak nejen, že můžeme díky volbě vhodné křivky získat mnohem rychlejší a efektivnější řešení, ale také bezpečnější. Tedy je možné použít v některých případech křivku o řádově vyšší, která bude výkonnostně odpovídat křivce o s nižším řádem. Systém výběru křivek byl autorem úspěšně prezentován a publikován na konferenci ICUMT 2015 [338]. Na základě prvotních úspěšných výsledků s křivkami prvočíselného řádu bylo následně proveden hlubší výzkum parametrizace křivek $\mathbb{F}_p$ i $\mathbb{F}_{2^m}$ (tedy závislosti jejich doménových parametrů) a jejich vlivu na výpočetní náročnost. Měřeno bylo nejen na vybraném MCU (vlastní implementace), ale také již na nelimitovaném zařízení RaspBerry Pi 2B (implementace OpenSSL [315] na PC). Bylo evaluováno více než 60 křivek, u kterých se posuzoval vliv jejich parametrů na výpočetní náročnost. Výsledky experimentálních měření křivek nad polem řádu 2 realizované na RaspBerry Pi 2B jsou zobrazeny v Příloze D.

Některé eliptické křivky totiž mají definované doménové parametry velmi malé či dokonce nulové. Prvotní myšlenka byla tedy vyjít z rovnic 3.33 a 3.36, kdy za předpokladu, že některý parametr je velmi malý či nulový, křivka by měla být znatelně rychlejší. Což můžeme vidět i v tabulce 5.7, kde jednotlivé křivky s nulovými či velmi malými parametry jsou podstatně rychlejší (řádově v jednotkách procent). Parametr No. značí tedy počet nulových či velmi malých parametrů. Tedy pokud například křivka wtls1 nad polem $\mathbb{F}_{2^{114}}$ má hlavní doménové parametry $(m_{114\,b}, a_{1\,b}, b_{1\,b}, x_{113\,b}, y_{112\,b}, n_{112\,b})$, pak je v tomto případě No. = 2. Parametr $t_{G1}$ pak značí rychlost ECDH v µs a $\Delta t_1$ je pak rozdíl vůči nejrychlejší křivce stejného řádu (index 1 značí měření na RaspBerry Pi 2B, později je zaveden ještě index 2 sloužící pro odlišení měření na MCU MSP430). Prvotní předpoklad se tedy potvrdil a z tohoto důvodu jsme se rozhodli dále ověřit i křivky nad polem prvočíselného řádu. Tyto výsledky jsou zobrazeny v Příloze E.

Měření proběhlo nejdříve pouze na platformě Raspberry Pi 2B, nicméně výsledky ukázaly anomálie v chování některých křivek s nulovými či malými parametry. Z tohoto důvodu bylo tedy přistoupeno na ověření výsledků na jiné platformě a implementaci. Přešlo se zpět k limitovanému MCU a vlastní implementaci (v tabulce značeny indexem 2). Výsledky prokázaly téměř stejný charakter. Anomálie v chování

eliptických křivek nad polem prvočíselného řádu spočívají v pomalosti křivek, které mají některý doménový parametr malý či nulový. Jedná se o ty nejpomalejší křivky, tedy naprosto opačné výsledky vůči křivkám nad polem řádu 2. V rámci křivek $\mathbb{F}_{2^m}$ byl výkonnostní rozdíl v řádu jednotek procent (tedy, kdy křivky s malým či nulovým doménovým parametrem byly rychlejší). Jak však vidíme z výše uvedené tabulky, tak křivky $\mathbb{F}_p$, které mají nulový či malý parametr vykazují zpomalení až o 50 %, což může být využito k následné optimalizaci výsledného systému. Tyto zajímavé výsledky, které mají nezanedbatelný vliv na optimalizaci eliptických křivek, byly autorem úspěšně publikovány v impaktovaném časopise [311] (*článek je momentálně v tisku*). V neposlední řadě srovnání výsledků s ostatními pracemi je v Tab. 5.9.

Tab. 5.9: Srovnání výsledků s vybranými pracemi.

| **Popis** | **Zrychlení** [%] | **Práve** |
|---|---|---|
| Práce se věnuje využití eliptických křivek v rámci zabezpečení senzorických sítí. Autoři prezentují novou operaci rychlejšího násobení. | 32–48 % | [339] |
| Práce zaměřena na algoritmus double-and-add pro násobení bodů na křivce a aplikaci Fibonačiho sekvence. | ca. 18 % | [340] |
| Autoři se soustředí na novou mnohem efektivnější formu Montgomeryho modulárního násobení. | 4–38 % | [341] |
| Autoři představují novou křivku Curve25519 v tomto případě se jedná o nejrychlejší křivku, která je velice efektivní na specifickém hardwaru. Nicméně finální data zatím v literatuře chybí pro porovnání křivky na vetší variacy hardwaru. | - % | [342] |
| Práce soustředící se na eliptické křivky využitelné pro internet věcí. Autoři implementují jejich vlastní návrh ECDSA na limtovaném procesoru a dosahují velkého zrychlení díky využití FPGA akcelerace. | 50 % | [343] |
| Další práce, která se soustředí na nové algoritmy založené na modifikovaném tradičním GCD. Autoři dosahují velice zajímavých výsledků, nicméně chybí zde hlubší popis hardwarové specifickace a postupu měření. | >50 % | [344] |

Představené práce se zabývají problematikou nových algoritmů či křivek a změny stávajících operací na křivkách dosahují horších či stejných výsledků než autorem představované řešení. Tedy i přesto, že se jedná o velmi komplexní a složitá řešení, která pro implementaci, optimalizaci i následný vývoj zaberou mnohonásobně více času. Navíc žádná dosavadní práce nepřináší tak komplexní a rozsáhlé testy jednotlivých dostupných křivek a jejich parametrů, jako jsou představeny v této práci autorem. Byla dále prokázána souvislost parametrizace křivek a vlivu doménových parametrů na efektivnost operací nad křivkou. Dále byl také představen efektivní způsob, jak je možné jednoduchým způsobem bez většího zásahu do HW či SW zefektivnit vlastní systém pouhým výběrem správných křivek. Výsledky přinesly také možnost nového směru výzkumu v parametrizaci křivek, kde autor s výzkumem v této oblasti stále pokračuje.

# 6 ZÁVĚR

V dnešní digitální době, kde informace se stává komoditou, vlastnictvím a data začínají nabývat citlivý a soukromý charakter, je informační bezpečnost jeden z nejrychleji se rozvíjejících oborů. Nové trendy a technologie nám krok po kroku pomáhají digitalizovat svět a připojovat i ty nejprimitivnější zařízení do sítě Internet. Tím však vzniká celá řada vědeckých výzev, které je a bude nutné řešit i v budoucnu. Tato dizertační práce se věnovala výzkumu v oblasti informační bezpečnosti inteligentních sítí, kde jsou užity zmíněná primitivní zařízení - zařízení s limitovanými zdroji. Tyto zařízení nám pomáhají díky moderním telemetrickým systémům optimalizovat každodenní činnosti a ulehčují práci v řadě oborů. Nicméně bezpečnost těchto zařízení je kritická otázka, kterou je nutno řešit. I přesto se dnes setkáváme s řadou implementací a aplikací, kde jsou tyto zařízení implementována bez jakékoliv bezpečnosti či jen s částečným řešením, což může mít až fatální následky v globální charakteristice.

V této práci jsme si definovali informační bezpečnost i dnešní výzvy (viz kapitola 1. Byly přiblíženy výzvy technologické, legislativní i problémy se standardizací. **Vlastním přínosem v kapitole 1 je převážně pohled na informační bezpečnost v poslední deseti letech, stanovení bezpečnostních principů vůči dnešním výzvám a představení nejnovějších regulací, legislativních změn v oboru a ucelení standardizací.** Následně byly definovány cíle této práce v kapitole 2. Hlavním cílem práce bylo navázat na nově vzniklé výzvy a vytvořit hybridní systém, který nepřinese pouze částečné řešení, ale komplexní řešení informační bezpečnosti v inteligentních sítí v oblasti energetiky, kde jsou využívány zařízení s limitovanými zdroji.

Nejprve byl proveden rozbor aktuální problematiky (viz kapitola 3), kde byly specifikovány dnešní možnosti pro zajištění informační bezpečnosti, rozděleny kryptografické algoritmy a představeny možná řešení. Byl definován vlastní komunikační model a představeny zkušenosti autora v rámci dnešních inteligentních sítí v energetice a zde používaných komunikačních technologií. Zkušeností vychází z řady představených vědeckých a odborných publikací. Nedostatky byly mj. diskutovány v rámci distribučních společnosti a to i na významném národním fóru (konferenci) ČK CIRED. **Přínos autora v kapitole 3 je nejen komplexní analýza dnešních možností zabezpečení, ale také vytvořený celkový přehled nedostatků dnešních progresivních technologií v dané oblasti.**

Kapitola 3 byla základem pro kapitolu 4 a vytvoření kritického pohledu na současná řešení a volby vhodných řešení, která budou efektivním a komplexním způsobem splňovat veškeré stanovené požadavky. Byly rozebrány metody pro jednotlivé stanovené bezpečnostní principy a byla kritickou analýzou stanovena jedna aktu-

ální možnost řešení z pohledu bezpečnosti, robustnosti, efektivnosti, ceny a dalších parametrů. Byl vytvořen model komunikace v inteligentních sítích, který byl mj. publikován v renomovaných časopisech a konferencích. Dále je v této části provedená kritická rešerše literatury, která přináší vlastní poznatky pro návrh systémů, ale také vlastní experimentální měření s technologiemi a algoritmy, které přinesly další důležité znalosti pro vytvoření bezpečného, komplexního a efektivního kryptosystému. Následně je vytvořeném vlastní model kryptosystému na základě představených a získaných znalostí. **Přínosem kapitoly 4 je samotná kritická rešerše dnešních algoritmů, vlastní experimentální měření potvrzující teoretické znalosti, vlastní analýzy technologií, ale hlavně vytvoření vlastního modelu hybridního kryptosystému, řešícího komplexním způsobem problematiku informační bezpečnosti v inteligentních sítí v energetice. Model byl mj. prezentován ve dvou impaktovaných časopisech a řadě mezinárodních konferencí. Celý modul pak následně zabírá méně než 5 % paměti a nechává tak prostor pro budování dalších modulů, funkcí a periferií.**

Kapitola 5 navazuje vývojem navrženého modelu a výzkumem v oblasti jeho dílčích částí. Je vybrán MCU na kterém následně probíhá výzkum, kdy nejprve jsou algoritmizovány navržené operace a následně jsou vytvořeny struktury pro velká čísla, společně s aritmetikou velkých čísel a funkcemi modulární algebry. Všechny vytvořené funkce jsou experimentálně validovány, kde výsledky testů prokázaly efektivnost navrženého řešení, které bylo publikováno v řadě vědeckých časopisů. Jako další bylo přistoupeno k modulu náhodného generátoru, kdy jsou vytvořeny dva vlastní generátory, jeden založený na známém jevu dvou oscilátorů a druhý zcela vlastního návrhu. Generátory jsou ověřeny pomocí testování hypotézy statistickou funkcí a baterií standardizovaných testů NIST a DIEHARDER. Validace ukázala anomálie a nenáhodné chování známého generátoru dvou oscilátorů, bylo přistoupeno k optimalizaci, která pomohla zefektivnit daný generátor. Následně byly provedeny opravdu rozsáhlé testy (ca. 300 tis. testů na jeden generátor) a vyhodnocena jejich náhodnost, efektivnost a rychlost. Ze všech parametrů tak následně vyšel nejlépe vlastní návrhu generátoru založeném na kvantifikačním šumu, který vykazoval mnohonásobně větší rychlost generování oproti známému řešení. Vlastní generátor i vývoj dle známého návrhu byl také publikován v řadě vědeckých konferencí a časopisů. Výzkum dále pokračoval v oblasti autentizace a šifrování, kde byly vybrány dvě (v dané době jediné) knihovny symetrické kryptografie, které jsou srovnány pomocí experimentálních testů výpočetní výkonnosti. Následně je proveden rozbor obou knihoven, zanalyzovány vnitřní funkce a obě knihovny jsou optimalizovány. Výsledky dalších měření ukázaly značné zlepšení obou knihoven, kde tedy rychlost AES byla zvýšena o více než 60 %. Výzkum v oblasti optimalizace symetrických šifer byl následně také úspěšně publikován autorem v řadě vědeckých konferencí a časopisů. Jako poslední

je pak asi nejvýznamnější část výzkumu eliptických křivek a modulu pro dohodu symetrického klíče. V rámci této části probíhal výzkumu v oblasti parametrizace křivek a efektivního výpočtu bodů. Vývoj skončil úspěšnou implementací více než 60 eliptických křivek různých standardů. V té době byly jedinečné implementace, na takto limitovaném hardwaru, křivek nad 256 b, což se úspěšně povedlo implementovat, tato velikost odpovídá úrovní bezpečnosti námi navrženému AES-128. Tyto jedinečné výsledky byly publikovány v řadě konferencích a také ve dvou impaktovaných článcích. **Hlavním přínosem kapitoly 5 jsou vlastní, v danou dobu jedinečné, výsledky výzkumu a vývoje, které byly uznány i vědeckou komunitou a publikovány v renomovaných časopisech.**

Z pohledu splnění stanovených cílů na dizertaci jsou všechny cíle splněny, je představen funkční kryptosystém, jeho dílčí části a to i s řešením pro velká čísla a náhodným generátorem. Takto komplexní řešení v dané době nebylo dostupné na uvažovaném limitovaném zařízení a pokud ano, většinou se jednalo pouze o řešení jednoho principu, které neřešilo další aspekty zabezpečení. Velkou výhodou daného řešení je hardwarová nezávislost (knihovny jsou řešeny v jazyce C a měly by být jednoduše převaditelné). Všechny výsledky byly pravidelně publikovány a recenzovány a disktovány vědeckou i odbornou komunitou.

# LITERATURA


[1] Naser Al-Falahy and Omar Y Alani. Technologies for 5g networks: challenges and opportunities. *IT Professional*, 19(1):12–20, 2017.

[2] Andrea Zanella, Nicola Bui, Angelo Castellani, Lorenzo Vangelista, and Michele Zorzi. Internet of things for smart cities. *IEEE Internet of Things journal*, 1(1):22–32, 2014.

[3] Vladimir Atanasovski and Alberto Leon-Garcia. *Future Access Enablers for Ubiquitous and Intelligent Infrastructures*. Springer, 2015.

[4] Stephen Ornes. Core concept: The internet of things and the explosion of interconnectivity. *Proceedings of the National Academy of Sciences*, 113(40):11059–11060, 2016.

[5] Li Da Xu, Wu He, and Shancang Li. Internet of things in industries: A survey. *IEEE Transactions on industrial informatics*, 10(4):2233–2243, 2014.

[6] Rodrigo Roman, Jianying Zhou, and Javier Lopez. On the features and challenges of security and privacy in distributed internet of things. *Computer Networks*, 57(10):2266–2279, 2013.

[7] Deepak Goyal and Malay Ranjan Tripathy. Routing protocols in wireless sensor networks: a survey. In *Advanced Computing & Communication Technologies (ACCT), 2012 Second International Conference on*, pages 474–480. IEEE, 2012.

[8] Jake Longo, Elke De Mulder, Dan Page, and Michael Tunstall. Soc it to em: electromagnetic side-channel attacks on a complex system-on-chip. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 620–640. Springer, 2015.

[9] Keith E Nolan, Wael Guibene, and Mark Y Kelly. An evaluation of low power wide area network technologies for the internet of things. In *Wireless Communications and Mobile Computing Conference (IWCMC), 2016 International*, pages 439–444. IEEE, 2016.

[10] Ala Al-Fuqaha, Mohsen Guizani, Mehdi Mohammadi, Mohammed Aledhari, and Moussa Ayyash. Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials*, 17(4):2347–2376, 2015.

[11] Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, and Marimuthu Palaniswami. Internet of things (iot): A vision, architectural elements, and future directions. *Future generation computer systems*, 29(7):1645–1660, 2013.

[12] Serbulent Tozlu, Murat Senel, Wei Mao, and Abtin Keshavarzian. Wi-fi enabled sensors for internet of things: A practical approach. *IEEE Communications Magazine*, 50(6), 2012.

[13] Yan Chen, Shunqing Zhang, Shugong Xu, and Geoffrey Ye Li. Fundamental trade-offs on green wireless networks. *IEEE Communications Magazine*, 49(6), 2011.

[14] Luigi Atzori, Antonio Iera, and Giacomo Morabito. The internet of things: A survey. *Computer networks*, 54(15):2787–2805, 2010.

[15] Luca Mainetti, Luigi Patrono, and Antonio Vilei. Evolution of wireless sensor networks towards the internet of things: A survey. In *Software, Telecommunications and Computer Networks (SoftCOM), 2011 19th International Conference on*, pages 1–6. IEEE, 2011.

[16] Petr Mlynek, Jiri Misurec, Martin Koutny, and Ondrej Raso. Design of secure communication in network with limited resources. In *Innovative Smart Grid Technologies Europe (ISGT EUROPE), 2013 4th IEEE/PES*, pages 1–5. IEEE, 2013.

[17] Ye Yan, Yi Qian, Hamid Sharif, and David Tipper. A survey on smart grid communication infrastructures: Motivations, requirements and challenges. *IEEE communications surveys & tutorials*, 15(1):5–20, 2013.

[18] Zhong Fan, Parag Kulkarni, Sedat Gormus, Costas Efthymiou, Georgios Kalogridis, Mahesh Sooriyabandara, Ziming Zhu, Sangarapillai Lambotharan, and Woon Hau Chin. Smart grid communications: Overview of research challenges, solutions, and standardization activities. *IEEE Communications Surveys & Tutorials*, 15(1):21–38, 2013.

[19] V Cagri Gungor, Dilan Sahin, Taskin Kocak, Salih Ergut, Concettina Buccella, Carlo Cecati, and Gerhard P Hancke. A survey on smart grid potential applications and communication requirements. *IEEE Transactions on Industrial Informatics*, 9(1):28–42, 2013.

[20] Vehbi C Gungor, Dilan Sahin, Taskin Kocak, Salih Ergut, Concettina Buccella, Carlo Cecati, and Gerhard P Hancke. Smart grid technologies: Communication

technologies and standards. *IEEE transactions on Industrial informatics*, 7(4):529–539, 2011.

[21] Rodrigo Roman, Pablo Najera, and Javier Lopez. Securing the internet of things. *Computer*, 44(9):51–58, 2011.

[22] Ye Yan, Yi Qian, Hamid Sharif, and David Tipper. A survey on cyber security for smart grid communications. *IEEE Communications Surveys & Tutorials*, 2012.

[23] Himanshu Khurana, Mark Hadley, Ning Lu, and Deborah A Frincke. Smart-grid security issues. *IEEE Security & Privacy*, 8(1), 2010.

[24] Thomas Eisenbarth and Sandeep Kumar. A survey of lightweight-cryptography implementations. *IEEE Design & Test of Computers*, 24(6), 2007.

[25] Asvin Gohil, Hardik Modi, and Shobhit K Patel. 5g technology of mobile communication: A survey. In *Intelligent Systems and Signal Processing (ISSP), 2013 International Conference on*, pages 288–292. IEEE, 2013.

[26] Wenye Wang, Yi Xu, and Mohit Khanna. A survey on the communication architectures in smart grid. *Computer Networks*, 55(15):3604–3629, 2011.

[27] Mohammad Hossein Javidi Dasht Bayaz et al. A review on transmission media in power systems. In *First Iranian Conference on Smart Grid*, 2010.

[28] Peter Bach Andersen, Einar Bragi Hauksson, Anders Bro Pedersen, Dieter Gantenbein, Bernhard Jansen, Claus Amtrup Andersen, and Jacob Dall. Smart grid applications, communications, and security. In *Smart Grid Applications, Communications, and Security*, pages 381–408. Wiley-VCH, 2012.

[29] Eric Sortomme and Mohamed A El-Sharkawi. Optimal charging strategies for unidirectional vehicle-to-grid. *IEEE Transactions on Smart Grid*, 2(1):131–138, 2011.

[30] Frederick Johannes Bruwer, Willem Smit, et al. Encoder and decoder microchips and remote control devices for secure unidirectional communication, January 16 2001. US Patent 6,175,312.

[31] Taneli Riihonen, Stefan Werner, and Risto Wichman. Hybrid full-duplex/half-duplex relaying with transmit power adaptation. *IEEE Transactions on Wireless Communications*, 10(9):3074–3085, 2011.

[32] Young-Bae Ko and Nitin H Vaidya. Geotora: A protocol for geocasting in mobile ad hoc networks. In *Network Protocols, 2000. Proceedings. 2000 International Conference on*, pages 240–250. IEEE, 2000.

[33] Divya Sharma, Sandeep Verma, and Kanika Sharma. Network topologies in wireless sensor networks: a review 1. 2013.

[34] Jie Chen, Cheng Li, and Paul Gillard. Network-on-chip (noc) topologies and performance: a review. In *Proceedings of the 2011 Newfoundland Electrical and Computer Engineering Conference (NECEC)*, pages 1–6, 2011.

[35] Nader Mehravari. Performance and protocol improvements for very high speed optical fiber local area networks using a passive star topology. *Journal of Lightwave technology*, 8(4):520–530, 1990.

[36] Srinivasan Venkataraman, Ramkumar Jayam, Anil Kapatkar, and Sivakumar Munnangi. Protocol stack for linking storage area networks over an existing lan, man, or wan, March 28 2006. US Patent 7,020,715.

[37] Chinh H Doan, Sohrab Emami, David Sobel, Ali M Niknejad, and Robert W Brodersen. 60 ghz cmos radio for gb/s wireless lan. In *Radio Frequency Integrated Circuits (RFIC) Symposium, 2004. Digest of Papers. 2004 IEEE*, pages 225–228. IEEE, 2004.

[38] Emil Jovanov, Aleksandar Milenkovic, Chris Otto, and Piet C De Groen. A wireless body area network of intelligent motion sensors for computer assisted physical rehabilitation. *Journal of NeuroEngineering and rehabilitation*, 2(1):6, 2005.

[39] David J Frerichs, Ian E McDowall, and Mark T Bolas. Method and system for adding advertisements over streaming audio based upon a user profile over a world wide area network of computers, January 27 2004. US Patent 6,684,249.

[40] Angus KY Wong. The near-me area network. *IEEE internet computing*, 14(2), 2010.

[41] Roy Want. Near field communication. *IEEE Pervasive Computing*, 10(3):4–7, 2011.

[42] Janaka B Ekanayake, Nick Jenkins, Kithsiri Liyanage, Jianzhong Wu, and Akihiko Yokoyama. *Smart grid: technology and applications*. John Wiley & Sons, 2012.

[43] Vinay M Igure, Sean A Laughter, and Ronald D Williams. Security issues in scada networks. *Computers & Security*, 25(7):498–506, 2006.

[44] Karl Maria Michael de Leeuw and Jan Bergstra. *The history of information security: a comprehensive handbook*. Elsevier, 2007.

[45] Sari Stern Greene. Security policies and procedures. *Principles and practices. Upper Saddle*, 2006.

[46] Peter Mell, Karen Scarfone, and Sasha Romanosky. A complete guide to the common vulnerability scoring system version 2.0. In *Published by FIRST-Forum of Incident Response and Security Teams*, volume 1, page 23, 2007.

[47] Adam Beautement and David J Pym. Structured systems economics for security management. In *WEIS*, pages 1–20, 2010.

[48] Donald L Pipkin. *Information security: protecting the global enterprise*. Prentice Hall PTR, 2000.

[49] James P McDermott. Attack net penetration testing. In *Proceedings of the 2000 workshop on New security paradigms*, pages 15–21. ACM, 2001.

[50] James M Anderson. Why we need a new definition of information security. *Computers & Security*, 22(4):308–313, 2003.

[51] HS Venter and Jan HP Eloff. A taxonomy for information security technologies. *Computers & Security*, 22(4):299–307, 2003.

[52] Thomas R Peltier. *Information security risk analysis*. CRC press, 2005.

[53] Glossary of terms. Glossary, ISACA.

[54] Information technology – security techniques – information security management systems – overview and vocabulary. Standard, ISO.

[55] Adéle Da Veiga and Jan Hp Eloff. A framework and assessment instrument for information security culture. *Computers & Security*, 29(2):196–207, 2010.

[56] Committee on national security systems. Glossary, ISO.

[57] Irene Maria Portela. *Organizational, Legal, and Technological Dimensions of Information System Administration*. IGI Global, 2013.

[58] Ralph Stair and George Reynolds. *Principles of information systems*. Cengage Learning, 2013.

[59] Committee on national security systems. Glossary, ISO.

[60] Hossein Bidgoli. *Handbook of Information Security, Information Warfare, Social, Legal, and International Issues and Security Foundations*, volume 2. John Wiley & Sons, 2006.

[61] Morris Sloman and Emil Lupu. Security and management policy specification. *IEEE network*, 16(2):10–19, 2002.

[62] Li Gong. Increasing availability and security of an authentication service. *IEEE Journal on Selected Areas in Communications*, 11(5):657–662, 1993.

[63] Aboosaleh Mohammad Sharifi, Saeed K Amirgholipour, Mehdi Alirezanejad, Baharak Shakeri Aski, and Mohammad Ghiami. Availability challenge of cloud system under ddos attack. *Indian Journal of Science and Technology*, 5(6):2933–2937, 2012.

[64] Fabian Fischer, Florian Mansmann, Daniel A Keim, Stephan Pietzko, and Marcel Waldvogel. Large-scale network monitoring for visual analysis of attacks. In *Visualization for Computer Security*, pages 111–118. Springer, 2008.

[65] Ajit Appari and M Eric Johnson. Information security and privacy in healthcare: current state of research. *International journal of Internet and enterprise management*, 6(4):279–314, 2010.

[66] H Jeff Smith, Tamara Dinev, and Heng Xu. Information privacy research: an interdisciplinary review. *MIS quarterly*, 35(4):989–1016, 2011.

[67] Jeffrey R Gulcher, Kristleifur Kristjánsson, Hákon Gudbjartsson, and Kári Stefánsson. Protection of privacy by third-party encryption in genetic research in iceland. *European journal of human genetics: EJHG*, 8(10):739, 2000.

[68] Qian Wang, Cong Wang, Kui Ren, Wenjing Lou, and Jin Li. Enabling public auditability and data dynamics for storage security in cloud computing. *IEEE transactions on parallel and distributed systems*, 22(5):847–859, 2011.

[69] Sung Hoon Kim, Bum Han Kim, Young Ki Kim, and Dong Hoon Lee. Auditable and privacy-preserving authentication in vehicular networks. In *Mobile Ubiquitous Computing, Systems, Services and Technologies, 2008. UBICOMM'08. The Second International Conference on*, pages 19–24. IEEE, 2008.

[70] Matthew K Franklin and Dahlia Malkhi. Auditable metering with lightweight security. In *International Conference on Financial Cryptography*, pages 151–160. Springer, 1997.

[71] Deyan Chen and Hong Zhao. Data security and privacy protection issues in cloud computing. In *Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on*, volume 1, pages 647–651. IEEE, 2012.

[72] Ross Anderson and Tyler Moore. The economics of information security. *Science*, 314(5799):610–613, 2006.

[73] Mohamed Al-Kuwaiti, Nicholas Kyriakopoulos, and Sayed Hussein. A comparative analysis of network dependability, fault-tolerance, reliability, security, and survivability. *IEEE Communications Surveys & Tutorials*, 11(2), 2009.

[74] S Massoud Amin and Bruce F Wollenberg. Toward a smart grid: power delivery for the 21st century. *IEEE power and energy magazine*, 3(5):34–41, 2005.

[75] Massoud Amin. Challenges in reliability, security, efficiency, and resilience of energy infrastructure: Toward smart self-healing electric power grid. In *Power and Energy Society General Meeting-Conversion and Delivery of Electrical Energy in the 21st Century, 2008 IEEE*, pages 1–5. IEEE, 2008.

[76] Matt Blaze, Whitfield Diffie, Ronald L Rivest, Bruce Schneier, and Tsutomu Shimomura. Minimal key lengths for symmetric ciphers to provide adequate commercial security. a report by an ad hoc group of cryptographers and computer scientists. Technical report, INFORMATION ASSURANCE TECHNOLOGY ANALYSIS CENTER FALLS CHURCH VA, 1996.

[77] Wullianallur Raghupathi and Someswar Kesh. Interoperable electronic health records design: towards a service-oriented architecture. *E-service Journal*, 5(3):39–57, 2007.

[78] T Kavitha and D Sridharan. Security vulnerabilities in wireless sensor networks: A survey. *Journal of information Assurance and Security*, 5(1):31–44, 2010.

[79] Paul C Drews. System and method for verifying the integrity and authorization of software before execution in a local platform, October 8 2002. US Patent 6,463,535.

[80] Costas Efthymiou and Georgios Kalogridis. Smart grid privacy via anonymization of smart metering data. In *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, pages 238–243. IEEE, 2010.

[81] Chung-Ping Wu and C-C Jay Kuo. Fast encryption methods for audiovisual data confidentiality. In *Proceedings of SPIE, the International Society for*

*Optical Engineering*, volume 4209, pages 284–295. Society of Photo-Optical Instrumentation Engineers, 2001.

[82] Yael Gertner, Sampath Kannan, Tal Malkin, Omer Reingold, and Mahesh Viswanathan. The relationship between public key encryption and oblivious transfer. In *Foundations of Computer Science, 2000. Proceedings. 41st Annual Symposium on*, pages 325–335. IEEE, 2000.

[83] Charanjit S Jutla. Encryption modes with almost free message integrity. In *Eurocrypt*, volume 2045, pages 529–544. Springer, 2001.

[84] Stuart G Stubblebine and Virgil D Gligor. On message integrity in cryptographic protocols. In *Research in Security and Privacy, 1992. Proceedings., 1992 IEEE Computer Society Symposium on*, pages 85–104. IEEE, 1992.

[85] William Stallings. *Network and internetwork security: principles and practice*, volume 1. Prentice Hall Englewood Cliffs, 1995.

[86] Mihir Bellare, Ran Canetti, and Hugo Krawczyk. Keying hash functions for message authentication. In *Crypto*, volume 96, pages 1–15. Springer, 1996.

[87] Charles E Perkins. Authentication, authorization, and accounting (aaa) registration keys for mobile ipv4. 2005.

[88] Adrian Perrig, Robert Szewczyk, Justin Douglas Tygar, Victor Wen, and David E Culler. Spins: Security protocols for sensor networks. *Wireless networks*, 8(5):521–534, 2002.

[89] Sigrid Gürgens, Carsten Rudolph, and Holger Vogt. On the security of fair non-repudiation protocols. *International Journal of Information Security*, 4(4):253–262, 2005.

[90] Haowen Chan and Adrian Perrig. Security and privacy in sensor networks. *computer*, 36(10):103–105, 2003.

[91] Patrick McDaniel and Stephen McLaughlin. Security and privacy challenges in the smart grid. *IEEE Security & Privacy*, 7(3), 2009.

[92] Himanshu Khurana, Mark Hadley, Ning Lu, and Deborah A Frincke. Smart-grid security issues. *IEEE Security & Privacy*, 8(1), 2010.

[93] Soma Shekara Sreenadh Reddy Depuru, Lingfeng Wang, and Vijay Devabhaktuni. Smart meters for power grid: Challenges, issues, advantages and status. *Renewable and sustainable energy reviews*, 15(6):2736–2742, 2011.

[94] Ye Yan, Yi Qian, Hamid Sharif, and David Tipper. A survey on smart grid communication infrastructures: Motivations, requirements and challenges. *IEEE communications surveys & tutorials*, 15(1):5–20, 2013.

[95] Wenye Wang and Zhuo Lu. Cyber security in the smart grid: Survey and challenges. *Computer Networks*, 57(5):1344–1371, 2013.

[96] Nikos Komninos, Eleni Philippou, and Andreas Pitsillides. Survey in smart grid and smart home security: Issues, challenges and countermeasures. *IEEE Communications Surveys & Tutorials*, 16(4):1933–1954, 2014.

[97] Anzar Mahmood, Nadeem Javaid, and Sohail Razzaq. A review of wireless communications for smart grid. *Renewable and sustainable energy reviews*, 41:248–260, 2015.

[98] Damminda Alahakoon and Xinghuo Yu. Smart electricity meter data intelligence for future energy systems: A survey. *IEEE Transactions on Industrial Informatics*, 12(1):425–436, 2016.

[99] Yasin Kabalci. A survey on smart metering and smart grid communication. *Renewable and Sustainable Energy Reviews*, 57:302–318, 2016.

[100] Ilhami Colak, Seref Sagiroglu, Gianluca Fulli, Mehmet Yesilbudak, and Catalin-Felix Covrig. A survey on the critical issues in smart grid technologies. *Renewable and Sustainable Energy Reviews*, 54:396–405, 2016.

[101] E Union. Directive 2009/72/ec of the european parliament and of the council of 13 july 2009 concerning common rules for the internal market in electricity and repealing directive 2003/54/ec. *Off. J. Eur. Union L*, 211:55–93, 2009.

[102] Jiri KUDRNAC. Investice do distribučních sítí nové technologie amm/sg, 2011. Odborná Přednáška.

[103] Alex Sinclair. Vision of smart home the role of mobile in the home of the future. *GSMA, London*, 2011.

[104] Timothy Schoechle. Getting smarter about the smart grid. *National Institute for Science, Law & Public Policy, Tech. Rep*, 2012.

[105] CEZ. Umíme měřit - umíte šetřit, 2011. Účelová publikace pro obyvatele města Vrchlabí.

[106] E.ON. Výroční zpráva, 2011. E.ON ČESKÁ REPUBLIKA, s.r.o.

[107] Landys+Gyr. Účinná řešení pro inteligentní řízení v energetice, 2012. LM Brochure CZ (D000045576_a_cz.

[108] General Data Protection Regulation. Regulation (eu) 2016/679 of the european parliament and of the council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46. *Official Journal of the European Union (OJ)*, 59:1–88, 2016.

[109] Vláda ČR. *Zákon o kybernetické bezpečnosti (č. 181/2014)-Komentář*. 2015.

[110] *Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti)*. 2015. Vyhláška č. 316/2014 Sb.

[111] *Vyhláška o významných informačních systémech a jejich určujících kritériích*. 2015. Vyhláška č. 317/2014 Sb.

[112] *ODVĚTVOVÁ KRITÉRIA PRO URČENÍ PRVKU KRITICKÉ INFRASTRUKTURY*. 2014. Nařízení vlady č. 315/2014 Sb.

[113] *Změna zákona o kyberneticke bezpečnosti č. ... /2017 Sb.* 2017.

[114] Ludmila Georgieva. The first eu-wide legislation on cybersecurity the directive on security of network and information systems as a game-changer for a stronger european cybersecurity. *European Energy Journal*, 6(3):62–76, 2016.

[115] Eric D Knapp and Joel Thomas Langill. *Industrial Network Security: Securing critical infrastructure networks for smart grid, SCADA, and other Industrial Control Systems*. Syngress, 2014.

[116] Smart grid security. Technical report, ENISA, 2013. Anex II. Security aspects of the Smart Grid.

[117] List of cybersecurity for smart grid standards and guidelines collected by frances cleveland, xanthus consulting international. Technical report, XANTUS, 2013. Convenor IEC TC57 WG15.

[118] Řízení energetických soustav a přidružená výměna informací - bezpečnost dat a komunikací - Část 3: Komunikační síť a systémová bezpečnost - profily zahrnující tcp/ip. Technical report, 2015. ČSN 62351-3.

[119] Kryptographische verfahren: Empfehlungen und schlüssellängen. Technical report, 2017. Version: 2017-01, BSI TR-02102-1.

[120] Référentiel général de sécurité. Technical report, 2014. Version: 2, Annexe B1.

[121] Smart grid security certification in europe. Technical report, ENISA, 2014. Challenges and recommendation.

[122] National electric grid security and resilience action plan. Technical report, NSA, 2016.

[123] Guildelines for smart grid cybersecurity. Technical report, NIST, 2014. Volume 1 - Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements.

[124] William Stallings. *Cryptography and network security: principles and practices*. Pearson Education India, 2006.

[125] Fred Piper. *Cryptography*. Wiley Online Library, 2002.

[126] Phillip Rogaway and Thomas Shrimpton. Cryptographic hash-function basics: Definitions, implications, and separations for preimage resistance, second-preimage resistance, and collision resistance. In *International Workshop on Fast Software Encryption*, pages 371–388. Springer, 2004.

[127] Alfred J Menezes, Paul C Van Oorschot, and Scott A Vanstone. *Handbook of applied cryptography*. CRC press, 1996.

[128] Rudolf Lidl and Harald Niederreiter. *Finite fields*, volume 20. Cambridge university press, 1997.

[129] Mehdi Ayat, Reza Ebrahimi Atani, and Sattar Mirzakuchaki. On design of puf-based random number generators. *Int. J. Netw. Secur. Appl*, 3(3):30–40, 2011.

[130] Smart true random number generator. Technical report, 2013. Product Brief (CLP-800).

[131] Lisa J Carnahan and Miles E Smid. Security requirements for cryptographic modules. *Federal Inf. Process. Stds.(NIST FIPS)-140-2*, 2002.

[132] Mehdi Ayat, Reza Ebrahimi Atani, and Sattar Mirzakuchaki. On design of puf-based random number generators. *Int. J. Netw. Secur. Appl*, 3(3):30–40, 2011.

[133] Umar Mujahid, Adnan Sharif, Tauqeer Khan, Adnan Qavi, et al. A novel lightweight pseudorandom number generator for passive rfid systems. In *Multi-Topic Conference (INMIC), 2014 IEEE 17th International*, pages 149–154. IEEE, 2014.

[134] A Rukhin. A statistical test suite for random and pseudorandom number generators for cryptographic applications [electronic resource], 2016.

[135] George MARSAGLIA. Diehard statistical test suite, 2016.

[136] Kalikinkar Mandal, Xinxin Fan, and Guang Gong. Warbler: A lightweight pseudorandom number generator for epc c1 gen2 passive rfid tags. *Int. J. RFID Secur. Cryptogr*, 2:82–91, 2013.

[137] Jiageng Chen, Atsuko Miyaj, Hiroyuki Sato, and Chunhua Su. Improved lightweight pseudo-random number generators for the low-cost rfid tags. In *Trustcom/BigDataSE/ISPA, 2015 IEEE*, volume 1, pages 17–24. IEEE, 2015.

[138] Jiageng Chen, Atsuko Miyaj, Hiroyuki Sato, and Chunhua Su. Improved lightweight pseudo-random number generators for the low-cost rfid tags. In *Trustcom/BigDataSE/ISPA, 2015 IEEE*, volume 1, pages 17–24. IEEE, 2015.

[139] Yi-Pin Liao and Chih-Ming Hsiao. A secure ecc-based rfid authentication scheme integrated with id-verifier transfer protocol. *Ad Hoc Networks*, 18:133–146, 2014.

[140] Vikram B Suresh, Daniele Antonioli, and Wayne P Burleson. On-chip lightweight implementation of reduced nist randomness test suite. In *Hardware-Oriented Security and Trust (HOST), 2013 IEEE International Symposium on*, pages 93–98. IEEE, 2013.

[141] Alberto Peinado, Jorge Munilla, and Amparo Fúster-Sabater. Epcgen2 pseudorandom number generators: Analysis of j3gen. *Sensors*, 14(4):6500–6515, 2014.

[142] Kaiyuan Yang, Dennis Michael Sylvester, David Theodore Blaauw, David Alan Fick, Michael B Henry, and Yoonmyung Lee. True random number generator, May 10 2016. US Patent 9,335,972.

[143] Anthony Van Herrewege. Lightweight puf-based key and random number generation. 2015.

[144] Liu Feng and Gao Xiaoxing. A new construction of pseudorandom number generator. *journal of Networks*, 9(8):2176–2182, 2014.

[145] Anthony Van Herrewege. Lightweight puf-based key and random number generation. 2015.

[146] Akif Akgul, Chunbiao Li, and Ihsan Pehlivan. Amplitude control analysis of a four-wing chaotic attractor, its electronic circuit designs and microcontroller-based random number generator. *Journal of Circuits, Systems and Computers*, page 1750190, 2017.

[147] Minseo Kim, Unsoo Ha, Kyuho Jason Lee, Yongsu Lee, and Hoi-Jun Yoo. A 82-nw chaotic map true random number generator based on a sub-ranging sar adc. *IEEE Journal of Solid-State Circuits*, 2017.

[148] Random number generation using the msp430 (msp430 applications). Technical report, 2006. Aplication Report (SLAA338).

[149] Charalampos Manifavas, George Hatzivasilis, Konstantinos Fysarakis, and Yannis Papaefstathiou. A survey of lightweight stream ciphers for embedded systems. *Security and Communication Networks*, 9(10):1226–1246, 2016.

[150] Steve Babbage, C Canniere, Anne Canteaut, Carlos Cid, Henri Gilbert, Thomas Johansson, Matthew Parker, Bart Preneel, Vincent Rijmen, and Matthew Robshaw. The estream portfolio. *eSTREAM, ECRYPT Stream Cipher Project*, 2008.

[151] Steve Babbage, Christophe De Canniere, Anne Canteaut, Carlos Cid, Henri Gilbert, Thomas Johansson, Matthew Parker, Bart Preneel, Vincent Rijmen, and Matthew Robshaw. The estream portfolio (rev. 1). *ECRYPT Network of Excellence*, 2008.

[152] Carlos Cid, Matthew Robshaw, and EIIDD SymLab. The estream portfolio 2009 annual update. *eSTREAM, ECRYPT Stream Cipher Project, Tech. Rep*, 2009.

[153] C Cid and M Robshaw. S. babbage, j. borghoff and v. velichkov (contributors) the estream portfolio in 2012,(january 16, 2012), version 1.0.

[154] Tim Good, William Chelton, and Mohammed Benaissa. Review of stream cipher candidates from a low resource hardware perspective. *SASC 2006 Stream Ciphers Revisited*, 125, 2006.

[155] Hendrik W Lenstra Jr. Factoring integers with elliptic curves. *Annals of mathematics*, pages 649–673, 1987.

[156] Neal Koblitz. Elliptic curve cryptosystems. *Mathematics of computation*, 48(177):203–209, 1987.

[157] Victor S Miller. Use of elliptic curves in cryptography. In *Conference on the Theory and Application of Cryptographic Techniques*, pages 417–426. Springer, 1985.

[158] Lawrence C Washington. *Elliptic curves: number theory and cryptography*. CRC press, 2008.

[159] Darrel Hankerson, Alfred J Menezes, and Scott Vanstone. *Guide to elliptic curve cryptography*. Springer Science & Business Media, 2006.

[160] Arjen Lenstra. Handbook of information security, chapter key lengths, 2004.

[161] Bora A Akyol, Harold Kirkham, Samuel L Clements, and Mark D Hadley. A survey of wireless communications for the electric power system. Technical report, Pacific Northwest National Laboratory (PNNL), Richland, WA (US), 2010.

[162] Vehbi C Gungor, Dilan Sahin, Taskin Kocak, Salih Ergut, Concettina Buccella, Carlo Cecati, and Gerhard P Hancke. Smart grid technologies: Communication technologies and standards. *IEEE transactions on Industrial informatics*, 7(4):529–539, 2011.

[163] Ahmad Usman and Sajjad Haider Shami. Evolution of communication technologies for smart grid applications. *Renewable and Sustainable Energy Reviews*, 19:191–199, 2013.

[164] Islam Safak Bayram and Ioannis Papapanagiotou. A survey on communication technologies and requirements for internet of electric vehicles. *EURASIP Journal on Wireless Communications and Networking*, 2014(1):223, 2014.

[165] Ramyar Rashed Mohassel, Alan Fung, Farah Mohammadi, and Kaamran Raahemifar. A survey on advanced metering infrastructure. *International Journal of Electrical Power & Energy Systems*, 63:473–484, 2014.

[166] Aziz Naamane and NK Msirdi. Towards a smart grid communication. *Energy Procedia*, 83:428–433, 2015.

[167] D Baimel, S Tapuchi, and N Baimel. Smart grid communication technologies-overview, research challenges and opportunities. In *Power Electronics, Electrical Drives, Automation and Motion (SPEEDAM), 2016 International Symposium on*, pages 116–120. IEEE, 2016.

[168] Michael Emmanuel and Ramesh Rayudu. Communication technologies for smart grid applications: A survey. *Journal of Network and Computer Applications*, 74:133–148, 2016.

[169] Fahad Khan, Atiq ur Rehman, Muhammad Arif, Muhammad Aftab, and Baber Khan Jadoon. A survey of communication technologies for smart grid connectivity. In *Computing, Electronic and Electrical Engineering (ICE Cube), 2016 International Conference on*, pages 256–261. IEEE, 2016.

[170] Nikoleta Andreadou, Miguel Olariaga Guardiola, and Gianluca Fulli. Telecommunication technologies for smart grid projects with focus on smart metering applications. *Energies*, 9(5):375, 2016.

[171] Petr Mlynek, Fujdiak Radek, Ondřej Krajsa, K. Zeman, Pospichal L., P. Kubicek, and J. Babka. Nové progresivní komunikační technologie a kybernetická bezpečnost chytrých sítí v energetice. In *ČK CIRED*, pages 1–11, 2016. ISBN: 978-80-87373-37- 8.

[172] Petr Mlynek, Fujdiak Radek, Pavel Mašek, Jiři Hošek, Jiři Pařizek, and Juan Zamphiropolos. Komunikační technologie pro konkrétní oblasti smart grid a provoz mřížové sítě. In *ČK CIRED*, pages 1–11, 2016. ISBN: 978-80-87373-37-8.

[173] Petr Mlynek, Fujdiak Radek, Pavel Šilhavý, Jiři Mišurec, Jiři Franěk, Juan Zamphiropolos, and Jiři Pařizek. Role plc v smart metering rollouts – porovnání a metodika hodnocení pilotních plc realizací. In *ČK CIRED*, pages 1–19, 2015. ISBN: 978-80-905014-4- 7.

[174] Lutz Lampe. *Power Line Communications: Principles, Standards and Applications from Multimedia to Smart Grid*. John Wiley & Sons, 2016.

[175] Xavier Carcelle. *Power line communications in practice*. Artech House, 2009.

[176] Petr Mlynek, Jiri Misurec, Martin Koutny, and Radek Fujdiak. Transfer function of power line channel—influence of topology parameters and power line topology estimation. In *Innovative Smart Grid Technologies Conference Europe (ISGT-Europe), 2014 IEEE PES*, pages 1–5. IEEE, 2014.

[177] Petr Mlynek, Martin Koutny, Jiri Misurec, and Radek Fujdiak. Evaluation of load impedances, discontinuity and impedance mismatch in plc networks by experimental measurements with coupling circuits. In *Telecommunications and Signal Processing (TSP), 2015 38th International Conference on*, pages 657–661. IEEE, 2015.

[178] P Mlynek, J Misurec, Z Kolka, J Slacik, and R Fujdiak. Narrowband power line communication for smart metering and street lighting control. *IFAC-PapersOnLine*, 48(4):215–219, 2015.

[179] Jan Slacik, Petr Mlynek, Fujdiak Radek, and Katerina Dobesova. Experimental measurements of multi- carrier power line communication systems. In *Proc. 40th Int. Conf. Telecommunications and Signal Processing*, pages 91–96, 2017. ISBN: 978-1-5090-3981- 4.

[180] Petr Mlynek, Radek Fujdiak, Jiri Misurec, and Jan Slacik. Experimental measurements of noise influence on narrowband power line communication. In *Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2016 8th International Congress on*, pages 94–100. IEEE, 2016.

[181] Petr Mlynek, Radek Fujdiak, and Jiri Misurec. Power line topology prediction using time domain reflectometry. In *Telecommunications and Signal Processing (TSP), 2016 39th International Conference on*, pages 199–202. IEEE, 2016.

[182] P Mlynek, J Misurec, M Koutny, R Fujdiak, and T Jedlicka. Analysis and experimental evaluation of power line transmission parameters for power line communication. *Measurement Science Review*, 15(2):64–71, 2015.

[183] Petr Mlynek, Jiri Misurec, Radek Fujdiak, Zdenek Kolka, and Ladislav Pospichal. Heterogeneous networks for smart metering–power line and radio communication. *Elektronika ir Elektrotechnika*, 21(2):85–92, 2015.

[184] Petr Mlynek, Zeynep Hasirci, Jiri Misurec, and Radek Fujdiak. Analysis of channel transfer functions in power line communication system for smart metering and home area network. *Advances in Electrical and Computer Engineering*, 16(4):51–56, 2016.

[185] Patrick Marsch, Michał Maternia, Michal Panek, Ali Yaver, Ryszard Dokuczał, and Rybakowski Marcin. 3gpp mobile communications: Wcdma and hspa. *The Telecommunications Handbook: Engineering Guidelines for Fixed, Mobile and Satellite Systems*, pages 371–416, 2015.

[186] Zia Ur Rahman, Ejaz Ali, Suliman Shah, Kamran Ali Shah, et al. Overview of smart communication in light of lte. *IJACTA*, 4(2):247–251, 2017.

[187] Ahmad Usman and Sajjad Haider Shami. Evolution of communication technologies for smart grid applications. *Renewable and Sustainable Energy Reviews*, 19:191–199, 2013.

[188] DP Upadhyay, Priyanka Sharma, and Sharada Valiveti. Randomness analysis of a5/1 stream cipher for secure mobile communication. *International Journal Of Computer Science & Communication*, 3:95–100, 2014.

[189] Shahzad Khan, Shahzad Shahid Peracha, and Zain Ul Abideen Tariq. Evaluation of cryptanalytic algorithm for a5/2 stream cipher. *International Journal of Computer Science and Information Security*, 12(4):8, 2014.

[190] Orr Dunkelman, Nathan Keller, and Adi Shamir. A practical-time related-key attack on the kasumi cryptosystem used in gsm and 3g telephony. *Journal of cryptology*, 27(4):824–849, 2014.

[191] Adrian Dabrowski, Nicola Pianta, Thomas Klepp, Martin Mulazzani, and Edgar Weippl. Imsi-catch me if you can: Imsi-catcher-catchers. In *Proceedings of the 30th annual computer security applications Conference*, pages 246–255. ACM, 2014.

[192] Ammar Muthanna, Pavel Masek, Jiri Hosek, Radek Fujdiak, Oshdi Hussein, Alexander Paramonov, and Andrey Koucheryavy. Analytical evaluation of d2d connectivity potential in 5g wireless systems. In *International Conference on Next Generation Wired/Wireless Networking*, pages 395–403. Springer, 2016.

[193] Pavel Masek, Krystof Zeman, Zenon Kuder, Jiri Hosek, Sergey Andreev, Radek Fujdiak, and Franz Kropfl. Wireless m-bus: an attractive m2m technology for 5g-grade home automation. In *Internet of Things. IoT Infrastructures: Second International Summit, IoT 360° 2015, Rome, Italy, October 27-29, 2015. Revised Selected Papers, Part I*, pages 144–156. Springer, 2016.

[194] Pavel Masek, Radek Fujdiak, Krystof Zeman, Jiri Hosek, and Ammar Muthanna. Remote networking technology for iot: Cloud-based access for alljoyn-enabled devices. In *FRUCT*, pages 200–205, 2016.

[195] Pavel Masek, Jan Masek, Petr Frantik, Radek Fujdiak, Aleksandr Ometov, Jiri Hosek, Sergey Andreev, Petr Mlynek, and Jiri Misurec. A harmonized perspective on transportation management in smart cities: the novel iot-driven environment for road traffic modeling. *Sensors*, 16(11):1872, 2016.

[196] Radek Fujdiak and Pavel Mašek. In- depth analysis of smart city in modern age. In *Proceedings of the 22th Conference Student EEICT*, volume 2014, 2014.

[197] CTU. Všeobecné oprávnění č. vo-r/10/05.2014-3.

[198] LoRaWAN Specification. the lora alliance, 2016.

[199] LoRa Alliance. A technical overview of lora and lorawan. *White paper, Nov*, 2015.

[200] T-Mobile. Sigfox: NovÁ bezdrÁtovÁ sÍŤ pro „internet vĚcÍ“ v ČeskÉ republice.

[201] Low-Power Wide-Area Network and Low-Power Network LPN. Platforms and technologies. 2016.

[202] DM Hernandez, G Peralta, L Manero, R Gomez, J Bilbao, and C Zubia. Energy and coverage study of lpwan schemes for industry 4.0. In *Electronics, Control, Measurement, Signals and their Application to Mechatronics (ECMSM), 2017 IEEE International Workshop of*, pages 1–6. IEEE, 2017.

[203] Low-Power Wide-Area Network and Low-Power Network LPN. Low power wide area network. *Network*, 6:1, 2016.

[204] LoRa Alliance. Lorawan™ specification. *LoRa Alliance*, 2015.

[205] Juan Carlos Zuniga and Benoit Ponsard. Sigfox system description. *LPWAN@ IETF97, Nov. 14th*, 2016.

[206] GSM ETSI. 03.20:"digital cellular telecommunications system (phase 2+). *Security related network functions*, 1992.

[207] TS GPP. 23.401: General packet radio service (gprs) enhancements for evolved universal terrestrial radio access network (e-utran) access. *V12*, 5, 2014.

[208] Radek Fujdiak, Pavel Masek, Petr Mlynek, Jiri Misurec, and Ekaterina Olshannikova. Using genetic algorithm for advanced municipal waste collection in smart city. In *Communication Systems, Networks and Digital Signal Processing (CSNDSP), 2016 10th International Symposium on*, pages 1–6. IEEE, 2016.

[209] Petra Seflova, Vladimir Sulc, Jiri Pos, and Rostislav Spinar. Iqrf wireless technology utilizing iqmesh protocol. In *Telecommunications and Signal Processing (TSP), 2012 35th International Conference on*, pages 101–104. IEEE, 2012.

[210] Prerna Mahajan and Abhishek Sachdeva. A study of encryption algorithms aes, des and rsa for security. *Global Journal of Computer Science and Technology*, 2013.

[211] B Padmavathi and S Ranjitha Kumari. A survey on performance analysis of des, aes and rsa algorithm along with lsb substitution. *International Journal of Science and Research (IJSR), India.*

[212] Gurpreet Singh. A study of encryption algorithms (rsa, des, 3des and aes) for information security. *International Journal of Computer Applications*, 67(19), 2013.

[213] Rounak Sinha, Hemant Kumar Srivastava, and Sumita Gupta. Performance based comparison study of rsa and elliptic curve cryptography. *International Journal of Scientific & Engineering Research*, 4(5):720–725, 2013.

[214] Vivek Kapoor, Vivek Sonny Abraham, and Ramesh Singh. Elliptic curve cryptography. *Ubiquity*, 2008(May):7, 2008.

[215] Zhifeng Xiao, Yang Xiao, and DH-C Du. Non-repudiation in neighborhood area networks for smart grid. *IEEE Communications Magazine*, 51(1):18–26, 2013.

[216] Stephen McLaughlin, Dmitry Podkuiko, and Patrick McDaniel. Energy theft in the advanced metering infrastructure. pages 176–187, 2009.

[217] M Madrazo. Today's energy theft detection models help protect revenues while enhancing neighborhood safety. *Pipeline & Gas Journal*, 237(7):16–18, 2010.

[218] Mansoor Ebrahim, Shujaat Khan, and Umer Bin Khalid. Symmetric algorithm survey: a comparative analysis. 2014.

[219] Nachiketh R Potlapally, Srivaths Ravi, Anand Raghunathan, and Niraj K Jha. Analyzing the energy consumption of security protocols. pages 30–35, 2003.

[220] NIST-FIPS Standard. Announcing the advanced encryption standard (aes). *Federal Information Processing Standards Publication*, 197:1–51, 2001.

[221] Damien Giry and Philippe Bulens. Cryptographic key length recommendation, 2009.

[222] MEgA. Přenosný pq monitor meg31.

[223] EN ČSN. 50160. *Charakteristiky napětí elektrické energie dodávané z veřejné distribuční sítě*, 2000.

[224] Bernhard Esslinger. Cryptool 2. 2008.

[225] Selva Kumar Podila Sushma. An efficient vlsi implementation of low power aes – ctr. *IOSR Journal of VLSI and Signal Processing (IOSR-JVSP)*, 2014.

[226] Lane Westlund. Random number generation using the msp430. *App. Report. SLAA338*, 2006.

[227] Pritamkumar N Khose and Vrushali G Raut. Hardware implementation of aes encryption and decryption for low area & power consumption. *IJRET: International Journal of Research in Engineering and Technology eISSN*, pages 2319–1163, 2014.

[228] J Hall. C implementation of cryptographic algorithms. *Texas Instruments*, 2013.

[229] Razvi Doomun, Jayramsingh Doma, and Sundeep Tengur. Aes-cbc software execution optimization. In *Information Technology, 2008. ITSim 2008. International Symposium on*, volume 1, pages 1–8. IEEE, 2008.

[230] Daniel J Bernstein and Peter Schwabe. New aes software speed records. In *International Conference on Cryptology in India*, pages 322–336. Springer, 2008.

[231] Texas Instruments. Enabling secure portable medical devices with ti's msp430™ mcu and wireless technologies, 2013.

[232] Bruce Schneier. *Applied cryptography: protocols, algorithms, and source code in C*. john wiley & sons, 2007.

[233] Dobre Blazhevski, Adrijan Bozhinovski, Biljana Stojchevska, and Veno Pachovski. Modes of operation of the aes algorithm. 2013.

[234] Phillip Rogaway. Evaluation of some blockcipher modes of operation. *Cryptography Research and Evaluation Committees (CRYPTREC) for the Government of Japan*, 2011.

[235] Chi-Wu Huang, TU Ying-Hao, Shih-Hao Liu, and Hsing-Chang Yeh. The platform built based on the mode operations of aes and the image applications. *International Journal of Modern Education and Computer Science (IJMECS)*, 3(4):1, 2011.

[236] William Stallings. *Cryptography and network security: principles and practices*. Pearson Education India, 2006.

[237] Helger Lipmaa. Idea: A cipher for multimedia architectures? In *Selected areas in cryptography*, volume 98, pages 248–263. Springer, 1998.

[238] Abdelrahman Altigani, Muawia Abdelmagid, and Bazara Barry. Evaluating aes performance using nist recommended block cipher modes of operation. 2015.

[239] Wei Dai. Crypto++: benchmarks.

[240] Petr Švenda. Basic comparison of modes for authenticated-encryption (iapm, xcbc, ocb, ccm, eax, cwc, gcm, pcfb, cs), 2016.

[241] Gernot R Bauer, Philipp Potisk, and Stefan Tillich. Comparing block cipher modes of operation on micaz sensor nodes. In *Parallel, Distributed and Network-based Processing, 2009 17th Euromicro International Conference on*, pages 371–378. IEEE, 2009.

[242] Phillip Rogaway, Mihir Bellare, and John Black. Ocb: A block-cipher mode of operation for efficient authenticated encryption. *ACM Transactions on Information and System Security (TISSEC)*, 6(3):365–403, 2003.

[243] Mark N Wegman and J Lawrence Carter. New hash functions and their use in authentication and set equality. *Journal of computer and system sciences*, 22(3):265–279, 1981.

[244] Mihir Bellare and Chanathip Namprempre. Authenticated encryption: Relations among notions and analysis of the generic composition paradigm. *Journal of Cryptology*, 21(4):469–491, 2008.

[245] Hugo Krawczyk. The order of encryption and authentication for protecting communications (or: How secure is ssl?). In *Advances in Cryptology—CRYPTO 2001*, pages 310–331. Springer, 2001.

[246] Mihir Bellare, Joe Kilian, and Phillip Rogaway. The security of the cipher block chaining message authentication code. *Journal of Computer and System Sciences*, 61(3):362–399, 2000.

[247] Matthew Green and Johns Hopkins. A few thoughts on cryptographic engineering, 2015.

[248] Elaine Baker. Suite b cryptography, 2006.

[249] Hassan M Elkamchouchi and Eman F Abu Elkair. An efficient protocol for authenticated key agreement. In *Radio Science Conference (NRSC), 2011 28th National*, pages 1–7. IEEE, 2011.

[250] Elaine Barker, Don Johnson, and Miles Smid. Nist special publication 800-56a: Recommendation for pair-wise key establishment schemes using discrete logarithm cryptography (revised). *Comput. Secur. Natl. Inst. Stand. Technol.(NIST), Publ. by NIST*, 2007.

[251] D Brown. Standards for efficient cryptography, sec 1: elliptic curve cryptography. *Released Standard Version*, 1, 2009.

[252] Daniel J Bernstein. Curve25519: new diffie-hellman speed records. In *International Workshop on Public Key Cryptography*, pages 207–228. Springer, 2006.

[253] Mike Hamburg. Fast and compact elliptic-curve cryptography. *IACR Cryptology ePrint Archive*, 2012:309, 2012.

[254] Hamish Ivey-Law and Robert Rolland. Constructing a database of cryptographically strong elliptic curves. *Proceeding of SAR-SSI*, 2010, 2010.

[255] Joppe W Bos, Craig Costello, Patrick Longa, and Michael Naehrig. Selecting elliptic curves for cryptography: an efficiency and security analysis. *Journal of Cryptographic Engineering*, 6(4):259–286, 2016.

[256] Elaine Barker, Lily Chen, Allen Roginsky, and Miles Smid. Recommendation for pair-wise key establishment schemes using discrete logarithm cryptography. *NIST special publication*, pages 800–56A, 2007.

[257] D Brown. Standards for efficient cryptography, sec 1: elliptic curve cryptography. *Released Standard Version*, 1, 2009.

[258] Gesine Hinterwälder, Amir Moradi, Michael Hutter, Peter Schwabe, and Christof Paar. Full-size high-security ecc implementation on msp430 microcontrollers. In *International Conference on Cryptology and Information Security in Latin America*, pages 31–47. Springer, 2014.

[259] Pascal Sasdrich and Tim Güneysu. Efficient elliptic-curve cryptography using curve25519 on reconfigurable devices. *ARC*, 8405:25–36, 2014.

[260] Nils Gura, Arun Patel, Arvinderpal Wander, Hans Eberle, and Sheueling Chang Shantz. Comparing elliptic curve cryptography and rsa on 8-bit cpus. In *CHES*, volume 4, pages 119–132. Springer, 2004.

[261] Erich Wenger and Mario Werner. Evaluating 16-bit processors for elliptic curve cryptography. In *International Conference on Smart Card Research and Advanced Applications*, pages 166–181. Springer, 2011.

[262] Erich Wenger, Thomas Unterluggauer, and Mario Werner. 8/16/32 shades of elliptic curve cryptography on embedded processors. In *International Conference on Cryptology in India*, pages 244–261. Springer, 2013.

[263] Xiaoyun Wang, Yiqun Lisa Yin, and Hongbo Yu. Finding collisions in the full sha-1. In *Crypto*, volume 3621, pages 17–36. Springer, 2005.

[264] Xiaoyun Wang, Andrew C Yao, and Frances Yao. Cryptanalysis on sha-1. In *Cryptographic Hash Workshop hosted by NIST*, 2005.

[265] Marc Stevens. On collisions for md5, 2007.

[266] Marc Stevens, Arjen K Lenstra, and Benne De Weger. Chosen-prefix collisions for md5 and applications. *International Journal of Applied Cryptography*, 2(4):322–359, 2012.

[267] David Molnar, Marc Stevens, Arjen Lenstra, Benne de Weger, Alexander Sotirov, Jacob Appelbaum, Dag Arne Osvik, Day Day, and Room Saal. Md5 considered harmful today. In *Proceedings of 25th Chaos Computer Congress, January, Berlin, Germany. http://dewy. fem. tu-imenau. de/CCC/25C3/video_-h264_720x756/25c3-3023-en-making_ the_theoretical_possible. mp4. torrent (accessed August 2009)*, 2009.

[268] Florian Mendel, Tomislav Nad, and Martin Schläffer. Improving local collisions: new attacks on reduced sha-256. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 262–278. Springer, 2013.

[269] Maria Eichlseder, Florian Mendel, and Martin Schläffer. Branching heuristics in differential collision search with applications to sha-512. In *International Workshop on Fast Software Encryption*, pages 473–488. Springer, 2014.

[270] Christoph Dobraunig, Maria Eichlseder, and Florian Mendel. Analysis of sha-512/224 and sha-512/256. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 612–630. Springer, 2014.

[271] Hung-Yu Chien. Sasi: A new ultralightweight rfid authentication protocol providing strong authentication and strong integrity. *IEEE Transactions on Dependable and Secure Computing*, 4(4):337–340, 2007.

[272] Pedro Peris-Lopez, Julio Cesar Hernandez-Castro, Juan M Estévez-Tapiador, and Arturo Ribagorda. Lmap: A real lightweight mutual authentication protocol for low-cost rfid tags. In *Proc. of 2nd Workshop on RFID Security*, page 06, 2006.

[273] Pedro Peris-Lopez, Julio Cesar Hernandez-Castro, Juan M Estevez-Tapiador, and Arturo Ribagorda. Emap: An efficient mutual-authentication protocol for low-cost rfid tags. In *OTM Confederated International Conferences: On the Move to Meaningful Internet Systems*, pages 352–361. Springer, 2006.

[274] Pedro Peris-Lopez, Julio Cesar Hernandez-Castro, Juan M Estevez-Tapiador, and Arturo Ribagorda. Mˆ 2ap: A minimalist mutual-authentication protocol for low-cost rfid tags. *UIC*, 6:912–923, 2006.

[275] Hung-Yu Chien and Chen-Wei Huang. Security of ultra-lightweight rfid authentication protocols and its improvements. *ACM SIGOPS Operating Systems Review*, 41(4):83–86, 2007.

[276] Hung-Yu Chien and Chen-Wei Huang. Security of ultra-lightweight rfid authentication protocols and its improvements. *ACM SIGOPS Operating Systems Review*, 41(4):83–86, 2007.

[277] Donald Welch and Scott Lathrop. Wireless security threat taxonomy. In *Information Assurance Workshop, 2003. IEEE Systems, Man and Cybernetics Society*, pages 76–83. IEEE, 2003.

[278] Donald Welch and Scott Lathrop. Wireless security threat taxonomy. In *Information Assurance Workshop, 2003. IEEE Systems, Man and Cybernetics Society*, pages 76–83. IEEE, 2003.

[279] Nikita Borisov. (in) security of the wep algorithm. *http://www. isaac. cs. berkeley. edu/isaac/wepfaq. html*, 2001.

[280] Donald Welch and Scott Lathrop. Wireless security threat taxonomy. In *Information Assurance Workshop, 2003. IEEE Systems, Man and Cybernetics Society*, pages 76–83. IEEE, 2003.

[281] David McGrew. An interface and algorithms for authenticated encryption. Technical report, 2008.

[282] Russell Housley. Using advanced encryption standard (aes) counter mode with ipsec encapsulating security payload (esp). Technical report, 2004.

[283] Nicholas Jansma and Brandon Arrendondo. Performance comparison of elliptic curve and rsa digital signatures. *nicj. net/files*, 2004.

[284] Petr Mlynek, Martin Koutny, and Jiri Misurec. The communication unit for remote data acquisition via the internet. In *WSEAS International Conference. Proceedings. Mathematics and Computers in Science and Engineering*, number 7. World Scientific and Engineering Academy and Society, 2008.

[285] Lili Qiu, Yin Zhang, Feng Wang, Mi Kyung, and Han Ratul Mahajan. Trusted computer system evaluation criteria. In *National Computer Security Center*. Citeseer, 1985.

[286] Aydan R Yumerefendi and Jeffrey S Chase. The role of accountability in dependable distributed systems. In *Proceedings of HotDep*, volume 5, pages 3–3, 2005.

[287] Gwan-Hwan Hwang, Kuh-Yih Huang, and Yu-Cheng Hsiao. A framework for cryptography based accountability and service invocation control for service composition in a multicloud architecture. In *Trustcom/BigDataSE/ISPA, 2015 IEEE*, volume 1, pages 1116–1121. IEEE, 2015.

[288] Ralf Küsters, Tomasz Truderung, and Andreas Vogt. Accountability: definition and relationship to verifiability. In *Proceedings of the 17th ACM conference on Computer and communications security*, pages 526–535. ACM, 2010.

[289] Hiren Kumar Deva Sarma and Avijit Kar. Security threats in wireless sensor networks. In *Carnahan Conferences Security Technology, Proceedings 2006 40th Annual IEEE International*, pages 243–251. IEEE, 2006.

[290] David R Raymond and Scott F Midkiff. Denial-of-service in wireless sensor networks: Attacks and defenses. *IEEE Pervasive Computing*, 7(1), 2008.

[291] Necla Bandirmali and İsmail Ertürk. Increasing the reliability of security protocols for wsns. In *Application of Information and Communication Technologies, 2009. AICT 2009. International Conference on*, pages 1–5. IEEE, 2009.

[292] Jun Zheng and Abbas Jamalipour. *Wireless sensor networks: a networking perspective*. John Wiley & Sons, 2009.

[293] Shahnaz Saleem, Sana Ullah, and Kyung Sup Kwak. A study of ieee 802.15. 4 security framework for wireless body area networks. *Sensors*, 11(2):1383–1395, 2011.

[294] Paul Syverson. A taxonomy of replay attacks [cryptographic protocols]. In *Computer Security Foundations Workshop VII, 1994. CSFW 7. Proceedings*, pages 187–191. IEEE, 1994.

[295] Li Gong and Xiaolei Qian. *Fail-stop protocols: An approach to designing secure protocols*. SRI International, Computer Science Laboratory, 1994.

[296] Tuomas Aura. Strategies against replay attacks. In *Computer Security Foundations Workshop, 1997. Proceedings., 10th*, pages 59–68. IEEE, 1997.

[297] Catherine A Meadows. Analyzing the needham-schroeder public key protocol: A comparison of two approaches. In *European Symposium on Research in Computer Security*, pages 351–364. Springer, 1996.

[298] Murat Dener. Security analysis in wireless sensor networks. *International Journal of Distributed Sensor Networks*, 10(10):303501, 2014.

[299] Vidya Bharrgavi Balasubramanyn, Geethapriya Thamilarasu, and Ramalingam Sridhar. Security solution for data integrity inwireless biosensor networks. In *Distributed Computing Systems Workshops, 2007. ICDCSW'07. 27th International Conference on*, pages 79–79. IEEE, 2007.

[300] Dorothy E Denning and Giovanni Maria Sacco. Timestamps in key distribution protocols. *Communications of the ACM*, 24(8):533–536, 1981.

[301] Sreekanth Malladi, Jim Alves-Foss, and Robert B Heckendorn. On preventing replay attacks on security protocols. Technical report, IDAHO UNIV MOSCOW DEPT OF COMPUTER SCIENCE, 2002.

[302] Obada Al-Khatib, Wibowo Hardjawana, and Branka Vucetic. Queuing analysis for smart grid communications in wireless access networks. In *Smart Grid Communications (SmartGridComm), 2014 IEEE International Conference on*, pages 374–379. IEEE, 2014.

[303] Soumyadip Sengupta, Swagatam Das, Md Nasir, Athanasios V Vasilakos, and Witold Pedrycz. An evolutionary multiobjective sleep-scheduling scheme for differentiated coverage in wireless sensor networks. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, 42(6):1093–1102, 2012.

[304] Michael Roche. Time synchronization in wireless networks. *CSE574S: Advanced Topics in Networking: Wireless and Mobile Networking (Spring 2006), Washington University in St. Louis*, 23, 2006.

[305] Tie Qiu, Xize Liu, Min Han, Huansheng Ning, and Dapeng Wu. A secure time synchronization protocol against fake timestamps for large scale internet of things. *IEEE Internet of Things Journal*, 2017.

[306] Sreekanth Malladi, Jim Alves-Foss, and Robert B Heckendorn. On preventing replay attacks on security protocols. Technical report, IDAHO UNIV MOSCOW DEPT OF COMPUTER SCIENCE, 2002.

[307] Fujdiak Radek, Pavel Masek, Jiri Hosek, Petr Mlynek, and Jiri Misurec. Efficiency evaluation of different types of cryptography curves on low-power devices. In *Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2015 7th International Congress on*, pages 269–274. IEEE, 2015.

[308] Ondrej Raso, Petr Mlynek, Radek Fujdiak, Ladislav Pospichal, and Pavel Kubicek. Implementation of elliptic curve diffie hellman in ultra-low power

microcontroller. In *Telecommunications and Signal Processing (TSP), 2015 38th International Conference on*, pages 662–666. IEEE, 2015.

[309] Radek Fujdiak, Petr Mlynek, Jiri Misurec, and Janko Slacik. Software optimization of advanced encryption standard for ultra-low-power msp430. In *Computer Science On-line Conference*, pages 469–478. Springer, 2017.

[310] RADEK Fujdiak, JIRI Misurec, PETR Mlynek, and JG Leonard. Cryptograph key distribution with elliptic curve diffie-hellman algorithm in low-power devices for power grids. *Rev. Roum. Sci. Tech. Serie Électrotechn. et Énerg*, 61(1):84–88, 2016.

[311] RADEK Fujdiak, Petr Dzurenda, Petr Mlynek, Jiri Misurec, Orgon Milost, and Sergey Bezzeteev. Anomalous behaviour of cryptographic elliptic curves over finite field. *Elektronika IR Elektrotechnika*, XX(X):XX–XX, 2017. (v tisku).

[312] Texas, Instruments. Advanced encryption standard. *Software*, 2009.

[313] Petr Mlynek, Martin Koutny, Jiri Misurec, and Ondrej Raso. Autentizační a šifrovací dll knihovna. `http://www.utko.feec.vutbr.cz/~mlynek/dll.html`, 2013. Software.

[314] Radek Fujdiak, Jiři Mišurec, Petr Mlynek, and Rášo Ondřej. Knihovna pro využití eliptických křivek v nízkovýkonovém zařízení. `http://www.utko.feec.vutbr.cz/~fujdiak/EC/cz.html`, 2015. Software.

[315] OpenSSL. Open source project that provides a robust, commercial-grade, and full-featured toolkit for the transport layer security (tls) and secure sockets layer (ssl). *2013-05)[2013-12-15] http://www. OpenSSL. com*, 2017. Cryptography and SSL/TLS Toolkit.

[316] Texas Instruments. Msp430 datasheet. *2013-05)[2013-12-15] http://www. ti. com*, 2001.

[317] Radek Fujdiak, P Mlynek, J Misurec, and O Raso. Random number generator in msp430 x5xx families. *Elektrorevue*, 4(1):70–74, 2013.

[318] Radek Fujdiak, J Misurec, P Mlynek, and O Raso. Cryptography in ultra-low power microcontroller msp430. *IJETT*, 6(8):398–404, 2013.

[319] Radek Fujdiak, Jiři Mišurec, Petr Mlynek, and Rášo Ondřej. Knihovna pro generování náhodných čísel na msp430. `http://www.utko.feec.vutbr.cz/~fujdiak/RNG/cz.html`, 2014. Software.

[320] Robert G Brown, Dirk Eddelbuettel, and David Bauer. Dieharder: A random number test suite. *Open Source software library, under development*, 2013.

[321] Rourab Paul, Hemanta DEy, Amlan Chakrabrti, and Ranjan Ghosh. Nist statistical test suite. *arXiv preprint arXiv:1609.01389*, 2016.

[322] Radek Fujdiak, Jiri Misurec, Petr Mlynek, and Ondrej Raso. Analysis of random number generator from texas instrument in msp430 x5xx families. In *Telecommunications and Signal Processing (TSP), 2015 38th International Conference on*, pages 653–656. IEEE, 2015.

[323] Stewart Robson, Bosco Leung, and Guang Gong. Truly random number generator based on a ring oscillator utilizing last passage time. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 61(12):937–941, 2014.

[324] Taiki Yamazaki and Atsushi Uchida. Performance of random number generators using noise-based superluminescent diode and chaos-based semiconductor lasers. *IEEE Journal of Selected Topics in Quantum Electronics*, 19(4):0600309–0600309, 2013.

[325] Kaiyuan Yang, David Blaauw, and Dennis Sylvester. An all-digital edge racing true random number generator robust against pvt variations. *IEEE Journal of Solid-State Circuits*, 51(4):1022–1031, 2016.

[326] John G Webster and Halit Eren. *Measurement, instrumentation, and sensors handbook: spatial, mechanical, thermal, and radiation measurement*, volume 1. CRC press, 2014.

[327] Robert H Walden. Analog-to-digital converter survey and analysis. *IEEE Journal on selected areas in communications*, 17(4):539–550, 1999.

[328] Pieter Harpe, Eugenio Cantatore, and Arthur van Roermund. A 2.2/2.7 fj/conversion-step 10/12b 40ks/s sar adc with data-driven noise reduction. In *Solid-State Circuits Conference Digest of Technical Papers (ISSCC), 2013 IEEE International*, pages 270–271. IEEE, 2013.

[329] Pieter Harpe, Eugenio Cantatore, and Arthur van Roermund. A 10b/12b 40 ks/s sar adc with data-driven noise reduction achieving up to 10.1 b enob at 2.2 fj/conversion-step. *IEEE Journal of Solid-State Circuits*, 48(12):3011–3018, 2013.

[330] Pieter Harpe, Eugenio Cantatore, and Arthur van Roermund. 11.1 an oversampled 12/14b sar adc with noise reduction and linearity enhancements achieving

up to 79.1 db sndr. In *Solid-State Circuits Conference Digest of Technical Papers (ISSCC), 2014 IEEE International*, pages 194–195. IEEE, 2014.

[331] Radek Fujdiak, Petr Mlynek, Jiri Misurec, and Pavel Masek. Design of low-power random number generator using signal quantization error in smart grid. In *Telecommunications and Signal Processing (TSP), 2016 39th International Conference on*, pages 7–10. IEEE, 2016.

[332] Radek Fujdiak. Measurement of symmetric cipher on low power devices for power grids. In *Proceedings of the 21th Conference Student EEICT*, volume 2015, 2015.

[333] Radek Fujdiak and Petr Mlynek. Advanced encryption standard v nízkovýkonovych zařízeních. *Elektrorevue*, 17(2):37–44, 2015.

[334] Radek Fujdiak. Asymmetric-key algorithm in network with limited sources. In *Proceedings of the 21th Conference Student EEICT*, volume 2013, 2013.

[335] NIST. Recommended elliptic curves for federal government use, 1999.

[336] SECG. Sec 2: Recommended elliptic curve domain parameters, 2010. (Version 2.0).

[337] ANSI. Public key cryptography for the financial services industry: The elliptic curve digital signature algorithm, 2005. X9.62-2005.

[338] Radek Fujdiak, Pavel Masek, Jiri Hosek, Petr Mlynek, and Jiri Misurec. Efficiency evaluation of different types of cryptography curves on low-power devices. In *Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2017 7th International Congress on*, pages XXX–XXX. IEEE, 2017. (v recenzním řizení).

[339] Ravi Kishore Kodali, Srikrishna Karanam, Kashyapkumar Patel, and Harpreet Singh Budwal. Fast elliptic curve point multiplication for wsns. In *TENCON Spring Conference, 2013 IEEE*, pages 194–198. IEEE, 2013.

[340] Shuanggen Liu, Guanglu Qi, and Xu An Wang. Fast and secure elliptic curve scalar multiplication algorithm based on a kind of deformed fibonacci-type series. In *P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2015 10th International Conference on*, pages 398–402. IEEE, 2015.

[341] Maryam Mohammadi and Amir Sabbagh Molahosseini. Efficient design of elliptic curve point multiplication based on fast montgomery modular multiplication.

In *Computer and Knowledge Engineering (ICCKE), 2013 3th International eConference on*, pages 424–429. IEEE, 2013.

[342] Daniel J Bernstein. Curve25519: new diffie-hellman speed records. In *International Workshop on Public Key Cryptography*, pages 207–228. Springer, 2006.

[343] Zhe Liu, Johann Großschädl, Zhi Hu, Kimmo Järvinen, Husen Wang, and Ingrid Verbauwhede. Elliptic curve cryptography with efficiently computable endomorphisms and its hardware implementations for the internet of things. *IEEE Transactions on Computers*, 66(5):773–785, 2017.

[344] Kai Liao, Xiaoxin Cui, Nan Liao, Tian Wang, Xiao Zhang, Ying Huang, and Dunshan Yu. High-speed constant-time division module for elliptic curve cryptography based on gf (2 m). In *Circuits and Systems (ISCAS), 2014 IEEE International Symposium on*, pages 818–821. IEEE, 2014.

# VYBRANÉ PUBLIKACE AUTORA

## Impaktované články

[1] FUJDIAK, R.; DZURENDA, R.; DZURENDA, P.; MLYNEK, P.; MISUREC, J.; ORGON, M.; SERGEY, B. Anomalous behaviour of cryptographic elliptic curves over finite field. Elektronika IR Elektrotechnika, XX(X):XX–XX, 2017. **IF: 0.859** (`v tisku`).

[2] MALINA, L.; HAJNY, J.; FUJDIAK, R.; HOSEK, J. On Perspective of Security and Privacy- Preserving Solutions in the Internet of Things. Computer Networks, 2016, roč. 102, č. 2016, s. 83–95. ISSN: 1389-1286. **IF: 2.516**

[3] FUJDIAK, R.; MISUREC, J.; MLYNEK, P.; LEONARD, J. Cryptograph key distribution with elliptic curve Diffie-Hellman algorithm in low- power devices for power grids. Revue Roumaine des Sciences Techniques - Serie Électrotechnique et Énergétique, 2016, roč. 61, č. 1, s. 84–88. ISSN: 0035–4066. **IF: 1.036**

[4] MLYNEK, P.; MISUREC, J.; FUJDIAK, R.; HASIRCI, Z. Analysis of Channel Transfer Functions in Power Line Communication System for Smart Metering and Home Area Network. Advances in Electrical and Computer Engineering, 2016, roč. 16, č. 4, s. 51–56. ISSN: 1844–7600. **IF: 0.595**

[5] MLYNEK, P.; MISUREC, J.; KOUTNY, M.; FUJDIAK, R.; JEDLICKA, T. Analysis and Experimental Evaluation of Power Line Transmission Parameters for Power Line Communication. Measurement Science Review, 2015, roč. 15, č. 2, s. 64–71. ISSN: 1335–8871. **IF: 1.344**

[6] MLYNEK, P.; MISUREC, J.; FUJDIAK, R.; KOLKA, Z.; POSPICHAL, L. Heterogeneous Networks for Smart Metering – Power Line and Radio Communication. Elektronika Ir Elektrotechnika, 2015, roč. 21, č. 2, s. 85–92. ISSN: 1392- 1215. **IF: 0.859**

## Mezinárodní konference WoS/Scopus

[7] FUJDIAK, R.; MLYNEK, P.; MISUREC, J.; SLACIK, J. Software Optimization of Advanced Encryption Standard for Ultra-Low-Power MSP430. In: Computer Science On-line Conference. Springer, Cham, 2017. p. 469–478.

[8] FUJDIAK, R.; MASEK, P.; HOSEK, J.; MLYNEK, P.; MISUREC, J. Efficiency evaluation of different types of cryptography curves on low-power devices. In Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2017 9th International Congress on, pages XXX–XXX. IEEE, 2017. `(v recenzi)`

[9] SLACIK, J.; MLYNEK, P.; FUJDIAK, R.; DOBESOVA, K. Experimental Measurements of Multi- carrier Power Line Communication Systems. In Proc. 40th Int. Conf. Telecommunications and Signal Processing. Barcelona: 2017. s. 91–96. ISBN: 978-1-5090-3981- 4.

[10] FUJDIAK, R.; MLYNEK, P.; MISUREC, J.; MASEK, P. Design of Low- Power Random Number Generator Using Signal Quantization Error in Smart Grid. In Proceedings of the 39th International Conference on Telecommunication and Signal Processing, TSP 2016. 2016. s. 7–10. ISBN: 978-1-5090-1287- 9.

[11] MLYNEK, P.; FUJDIAK, R.; MISUREC, J.; SLACIK, J. Experimental Measurements of Noise Influence on Narrowband Power Line Communication. In 2016 8th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT). Lisabon: 2016. s. 1–7. ISBN: 978-1-4673-8817- 7.

[12] MASEK, P.; MASEK, J.; FRANTIK, P.; FUJDIAK, R.; OMETOV, A.; HOŠEK, J.; ANDREEV, S.; MLÝNEK, P.; MIŠUREC, J. A Harmonized Perspective on Transportation Management in Smart Cities: The Novel IoT- Driven Environment for Road Traffic Modeling. SENSORS, 2016, roč. 11, č. 1872, s. 1–23. ISSN: 1424-8220.

[13] MUTHANNA, A.; MASEK, P.; HOSEK, J.; FUJDIAK, R.; HUSSEIN, O.; PARAMONOV, A.; KOUCHERYAVY, A. Analytical Evaluation of D2D Connectivity Potential in 5G Wireless Systems. In Internet of Things, Smart Spaces, and Next Generation Networks and Systems. 2016. s. 395–403. ISBN: 978-3-319-46300- 1.

[14] KRIVTSOVA, I.; LEBEDEV, I.; SUKHOPAROV, M.; BAZHAYEV, N.; ZIKRATOV, I.; OMETOV, A.; ANDREEV, S.; MASEK, P.; FUJDIAK, R.; HOSEK, J. Implementing a Broadcast Storm Attack on a Mission- Critical Wireless Sensor Network. In The 14th International Conference on Wired/Wireless Internet Communications - WWIC 2016. 2016. s. 1–12. ISBN: 978-3-319-22572-2.

[15] MASEK, P.; FUJDIAK, R.; ZEMAN, K.; HOSEK, J.; MUTHANNA, A. Remote Networking Technology for IoT: Cloud-based Access for AllJoyn- enabled Devices. In Proceedings of the 18th FRUCT & ISPIT Conference, 18-22 April 2016, Technopark of ITMO University, Saint-Petersburg, Russia. FRUCT Oy, Finland. St. Petersburg: 2016. s. 1–6. ISBN: 978-952-68397-3- 8.

[16] FUJDIAK, R.; MASEK, P.; HOSEK, J.; MLYNEK, P.; MISUREC, J. Efficiency Evaluation of Different Types of Cryptography Curves on Low- Power Devices. In 2015 7th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT). Brno, Czech Republic: 2015. s. 230–235. ISBN: 978-1-4673-9282- 2.

[17] MLYNEK, P.; RASO, O.; FUJDIAK, R.; POSPICHAL, L.; KUBICEK, P. Implementation of Elliptic Curve Diffie Hellman in Ultra- Low Power Microcontroller. In Proceedings of the 38th International Conference on Telecommunication and Signal Processing. Berlin, Germany: 2014. s. 662–666. ISBN: 978-1-4799-8497- 8.

[18] FUJDIAK, R.; MISUREC, J.; MLYNEK, P. Analysis of Random Number Generator from Texas Instrument in MSP430 x5xx Families. In Proceedings of the 38th International Conference on Telecommunication and Signal Processing. 2014. s. 653–656. ISBN: 978-1-4799-8497- 8.

[19] MASEK, P.; ZEMAN, K.; KUDER, Z.; HOSEK, J.; ANDREEV, S.; FUJDIAK, R.; KROPFL, F. Wireless M-BUS: An Attractive M2M Technology for 5G-Grade Home Automation. In EAI International Conference on CYber physiCaL systems, iOt and sensors Networks (CYCLONE 2015). Řím: 2015. s. 1–12. ISBN: 978-1-4673-9282- 2. Detail

## Ostatní

[20] MLYNEK, P.; FUJDIAK, R.; MASEK, P.; HOŠEK, J.; PAŘÍZEK, J.; ZAMPHIROPOLOS, J. Komunikační technologie pro konkrétní oblasti Smart grid a provoz mřížové sítě. In Sborník příspěvků konference ČK CIRED. 2016. s. 1–11. ISBN: 978-80-87373-37- 8.

[21] MLÝNEK, P.; FUJDIAK, R.; KRAJSA, O.; ZEMAN, K.; POSPICHAL, L.; KUBICEK, P.; BABKA, J. Nové progresivní komunikační technologie a kybernetická bezpečnost chytrých sítí v energetice. In Sborník příspěvků konference ČK CIRED. 2016. s. 1–11. ISBN: 978-80-87373-37- 8.

# SEZNAM SYMBOLŮ, VELIČIN A ZKRATEK

| | |
|---|---|
| IoT | Internet věcí - Internet of Everything |
| SoC | Integrované systémy - System on Chip |
| PoC | Pilotní projekty - Proof of Concept |
| 2G | Druhá (případně jiná) generace mobilní sítě (2G+ značí vše od druhé generace výše) |
| LPWAN | Nízkoenergetické bezdrátové technologie dlouhého dosahu - Low Power Wide Area Network |
| Wi-Fi | Bezdrátová technologie |
| PLC | Přenos dat po elektrickém vedení - Power Line Communication |
| LAN | Lokální síť - Local Area Network |
| WLAN | Bezdrátová lokální síť - Wireless Local Area Network |
| HAN | Domácí síť - Home Area Network |
| MAN | Metropolitní síť - Metropolitan Area Network |
| WAN | Rozsáhlá síť - Wide Area Network |
| PAN | Síť v osobním prostoru - Personal Area Network |
| BAN | Síť uvnitř těla - Body Area Network |
| NAN | Síť v bezprostřední blízkosti - NearMe Area Network |
| NFC | Komunikace v blízkém poli - Near Field Communication |
| CAN | Kampus (Korporátní) síť - Campus (Corporate) Area Network |
| IAN | Síť v síti Internet - Internet Area Network |
| CIA | Tři principy bezpečnosti Důvěrnost-Integrita-Dostupnost - Confidentiality-Integrity-Availability |
| C&S | Impaktovaný časopis Communication & Science |
| ISACA | Auditorská a kontrolní asociace - Information System Audit and Control Association |
| ISO | Mezinárodní organizace pro normalizaci - International Organization for Standardization |
| MTBF | Střední doba mezi poruchami v síti - Mean Time Between Failures |
| MTBF | Průměrná doba výpadku - Mean Time To Repair |
| DoS | Odepření služby - Denial of Service |
| AE | Autentizované šifrování - Authentication Encryption |
| HDO | Hromadné dálkové ovládání |
| GDPR | Evropské nařízení - General Data Protection Regulation |
| ZKB | Zákon Kybernetické Bezpečnosti |
| ENISA | Evropská agentura informační bezpečnosti - European Network and Information Security Agency |
| BSI | Německý úřad pro informační bezpečnost - Bundesamt für Sicherheit in |

| | |
|---|---|
| | der Informationstechnik |
| ANSSI | Francouzská agentura informační bezpečnosti - Agence nationale de la sécurité des systèmes d'information |
| NSA | Americká národní bezpečnostní agentura - National Security Agency |
| NIST | Americký národní institut standardizace a technologií - National Institute of Standards and Technology |
| PRGN | Pseudonáhodný generátor čísel - Pseudo-Random Number Generator |
| TRGN | Skutečně náhodný generátor čísel - True Random Number Generator |
| RFID | Identifikace na rádiové frekvenci - Radio Frequency Identification |
| PUF | Fyzicky neklonovatelné funkce - Physical Unclonable function |
| ECB | Symetrický blokový mód - Electronical Code Book |
| CBC | Symetrický blokový mód - Cipher Block Chaining |
| CTR | Symetrický blokový mód - Counter mode |
| CFB | Symetrický blokový mód - Cipher Feedback |
| MAC | Autentizační kód zprávy - Message Auhentication Code |
| HMAC | Autentizační kód zprávy využívající hašovou funkci - Hash Message Auhentication Code |
| EtM | Metoda autentizačního šifrování - Encrypto-Then-Mac |
| E&M | Metoda autentizačního šifrování - Encrypto-And-Mac |
| MtE | Metoda autentizačního šifrování - Mac-Then-Encrypt |
| RSA | Asymetrický kryptografický algoritmus - Rivest Shamir Adleman |
| DSA | Asymetrický kryptografický algoritmus - Digital Signature Algorithm |
| DH | Asymetrický kryptografický algoritmus - Diffie-Hellman |
| ECDH | Asymetrický algoritmus nad eliptickými křivkami - Elliptic Curve Diffie-Hellman |
| ECDSA | Asymetrický algoritmus nad eliptickými křivkami - Elliptic Curve Digital Signature Algorithm |
| ECC | Kryptografie eliptických křivek - Elliptic Curve Cryptography |
| NB | Úzké pásmo - Narrowband |
| BP | Široké pásmo - Broadband |
| P2P | Komunikace typu bod-bod - Point-to-Point |
| E2E | Komunikace typu konec-konec - End-to-End |
| CRC | Cyklický redundantní součet - Cyclic Redundancy Check |
| AM | Aktivní mód - Active Mode |
| LPM | Nízko-energetický mód - Low Power Mode |
| SL | Takto jsou označovány nejpomalejší algoritmy, prvky či funkce |
| FA | Takto jsou označovány nejpomalejší algoritmy, prvky či funkce |
| # | Identifikátor využívaný k rozlišení jednotlivých funkcí pro lepší přehlednost grafů |

| | |
|---|---|
| LTE | Celulární technolgie - Long Term Evolution |
| MCU | Výpočetní jednotka, mikrokontroler - Microcontroller Unit |

# SEZNAM PŘÍLOH

# A KOMENTOVANÝ PŘÍKLAD UŽITÍ VYTVOŘENÝCH FUNKCÍ PRO PRÁCI S VELKÝMI ČÍSLY

```
// Statická definice a, b, m, r, rem, jedná se o statické pole typu BN_ULONG
BN_ULONG a[]={0x16a0,0x5678,0x0000,0x0000,0x000,0x0000,0x0000,0x0000};
BN_ULONG b[]={0x14cd,0x01fa,0x0000,0x0000,0x000,0x0000,0x0000,0x0000};
BN_ULONG m[]={0xffa1,0xfffa,0x00ff,0x0000,0x000,0x0000,0x0000,0x0000};
BN_ULONG r[]={0x0000,0x0000,0x0000,0x0000,0x000,0x0000,0x0000,0x0000};
BN_ULONG rem[]={0x0001,0x0000,0x0000,0x0000,0x000,0x0000,0x0000,0x0000};

BN_CTX *ctx1;           // Deklarace ukazatele na BN_CTX strukturu, který slouží pro
// dynamickou alokaci proměnných pro pomocné výpočty uvnitř volaných funkcí.
BN_MONT_CTX *mtx1;      // Deklarace ukazatele na BN_MONT_CTX strukturu, obsahuje
// pomocné parametry pro Montgomeryho násobení a redukci
int ret=0;              // návratová hodnota
BIGNUM bn_a, bn_b, bn_r, bn_m, bn_rem;
// prefix bn značí big number, tyto proměnné jsou použity pro
// demonstraci funkcí z knihovny

// následující kód obsahuje inicializaci proměnných
bn_a.d=a; bn_a.dmax=8; bn_a.top=2; bn_a.neg=0;          // inicializace bn_a
bn_b.d=b; bn_b.dmax=8; bn_b.top=2; bn_b.neg=0;          // inicializace bn_b
bn_m.d=m; bn_m.dmax=8;bn_m.top=3; bn_m.neg=0;           // inicializace bn_m
bn_r.d=r; bn_r.dmax=8;bn_r.top=0; bn_r.neg=0;           // inicializace bn_r
bn_rem.d=rem; bn_rem.dmax=8;bn_rem.top=1; bn_rem.neg=0; // inicializace bn_rem

// Porovnání dvou velkých čísel, když platí a==b pak funkce vrací 1.
ret=BN_cmp(&bn_a,&bn_a); ret=BN_cmp(&bn_a,&bn_b);

// Testování zda (a==0), pokud ano pak funkce vrací 1.
ret=BN_is_zero(&bn_r); ret=BN_is_zero(&bn_a);

// Testování zda (a==1), pokud ano pak funkce vrací 1.
ret=BN_is_one(&bn_rem); BN_zero(&bn_rem); // <--- vynuluje bn_rem

// BN_copy zkopíruje bn_a do bn_rem
ret=BN_copy(&bn_rem,&bn_a); BN_zero(&bn_rem); // <--- BN_zero opět vynuluje bn_rem

ctx1 = bn_ctx_new(); mtx1 = BN_MONT_CTX_new(); // Vytvoření struktur ctx1 a mtx1

ret=BN_mod_add(&bn_r, &bn_a, &bn_b, &bn_m, ctx1); // r = (a+b) mod m
ret=BN_mod_sub(&bn_r, &bn_a, &bn_b, &bn_m, ctx1); // r = (a-b) mod m
ret=BN_mod_mul(&bn_r, &bn_a, &bn_b, &bn_m, ctx1); // r = (a*b) mod m

ret=BN_MONT_CTX_set(mtx1, &bn_m, ctx1); // Naplněni struktury mtx1 z modulu bn_m
ret=BN_mod_mul_montgomery(&bn_r, &bn_a, &bn_b, mtx1, ctx1); // Montgomeryho násobeni
ret=BN_to_montgomery(&bn_rem, &bn_r, mtx1, ctx1); // Zpětná konverze, bn_rem je (a*b) mod m

ret=BN_mod_sqr(&bn_r, &bn_a, &bn_m, ctx1); // r= (a^2) mod m
ret=BN_mod(&bn_r, &bn_a, &bn_m, ctx1); // r = a mod m
ret=BN_div(&bn_r, &bn_rem, &bn_a, &bn_b, ctx1); // r = a / b; rem = a mod b

//uvolnění struktur ctx1 a mtx1
BN_CTX_free(ctx1); BN_MONT_CTX_free(mtx1);
```

# B KOMENTOVANÝ PŘÍKLAD UŽITÍ VLASTNÍCH FUNKCÍ PRO PRÁCI S ELIPTICKÝMI KŘIVKAMI

```
#define HASH_len 128 // Délka hashovací funkce

EC_KEY *a=NULL; EC_KEY *a=NULL; // Struktury pro strany Alice a Bob

unsigned char abuf[HASH_len], bbuf[HASH_len]; int alen,blen,ret=0,aout,bout=0;
const EC_POINT *pub_keyA=NULL, *pub_keyB=NULL;

a = EC_KEY_new_by_curve_name(nid); if (a == NULL) goto err;
// Strana A, generování základní struktury + podmínka pro chybu při generování, parametr nid je název
// křivky například NID_sect113r1 tedy konkrétně zapsáno EC_KEY_new_by_curve_name(NID_sect113r1)

b = EC_KEY_new_by_curve_name(nid); if (b == NULL) goto err;
// Strana B, generování základní struktury + podmínka pro chybu při generování, parametr nid musí být
// stejný na obou stranách

if (!EC_KEY_generate_key(a,0)) goto err;
// Generování veřejného a soukromého klíče, strana A.
// Pokud je druhý parametr 1 tak se očekává, že soukromý klíč je již nastaven.

if (!EC_KEY_generate_key(b,0)) goto err;
// Generování veřejného a soukromého klíče, strana B. Pokud je druhý parametr 1 tak se očekává,
// že soukromý klíč je již nastaven.

pub_keyA = EC_KEY_get0_public_key(a);
// Uložení veřejného klíče A do pub_keyA ze struktury a

pub_keyB = EC_KEY_get0_public_key(b);
// Uložení veřejného klíče B do pub_keyB ze struktury b
// pub_keyA a pub_keyB je třeba zveřejnit (tedy předat protistraně)

aout=ECDH_compute_key(abuf,HASH_len,pub_keyB,a,NULL);
// Výpočet soukromého klíče, strana A.
bout=ECDH_compute_key(bbuf,HASH_len,pub_keyA,b,NULL);
// Výpočet soukromého klíče, strana B.
// Výpočet soukromého klíče, ten bude mít délku HASH_len. Poslední parametr této funkce je
// ukazatel na hashovací funkci, v tomto příkladu žádná nebyla použita a proto má hodnotu NULL.

if ((bout != aout) || (memcmp(abuf,bbuf,aout) != 0)) goto err;
// tento bod je možný ověřit pouze v rámci testování na jednom zařízení, pokud se již kód rozdělí
// na strany A a B již musí  být tato podmínka zaručena a otestována, jelikož není možné zveřejnit
// soukromé klíče.

ret=1;

err:
if (b) EC_KEY_free(b);
if (a) EC_KEY_free(a);
return(ret);
```

# C VÝSLEDKY EXPERIMENTÁLNÍHO MĚŘENÍ ELIPTICKÝCH KŘIVEK NAD POLEM O ŘÁDU 2. NA MSP430

| **Křivka** | $\mathbb{F}_{2m}$ [b] | **Velikost haldy** [B] | **Čas** [m] |
|---|---|---|---|
| **Křivky řady** `NID_sect` | | | |
| `sect113r1` | 113 | 2400 | 0,6 |
| `sect113r2` | 113 | 2400 | 0,6 |
| `sect131r1` | 131 | 2400 | 1,2 |
| `sect131r2` | 131 | 2400 | 1,2 |
| `sect163k1` | 163 | 2400 | 1,5 |
| `sect163r1` | 163 | 2400 | 1,6 |
| `sect163r2` | 163 | 2800 | 1,6 |
| `sect193r1` | 193 | 2800 | 2,1 |
| `sect193r2` | 193 | 2800 | 2,1 |
| `sect233k1` | 233 | 2800 | 3,0 |
| `sect233r1` | 233 | 2800 | 3,4 |
| `sect239k1` | 239 | 2800 | 3,1 |
| `sect283k1` | 283 | 3200 | 5,9 |
| `sect283r1` | 283 | 3200 | 6,7 |
| `sect409k1` | 409 | 4000 | 14,0 |
| `sect409r1` | 409 | 4000 | 16,0 |
| `sect571k1` | 571 | 4400 | 66,0 |
| `sect571r1` | 571 | 4400 | 80,0 |
| **Křivky řady** `NID_X9_62` | | | |
| `c2pnb163v1` | 163 | 2400 | 3,3 |
| `c2pnb163v2` | 163 | 2400 | 3,3 |
| `c2pnb163v3` | 163 | 2400 | 3,3 |
| `c2pnb176v1` | 176 | 2400 | 3,3 |
| `c2tnb191v1` | 191 | 2800 | 3,5 |
| `c2tnb191v2` | 191 | 2800 | 3,5 |
| `c2tnb191v3` | 191 | 2800 | 3,5 |
| `c2pnb208w1` | 208 | 2800 | 6 |
| `c2tnb239v1` | 239 | 2800 | 6,9 |
| `c2tnb239v2` | 239 | 2800 | 6,9 |
| `c2tnb239v3` | 239 | 2800 | 6,9 |
| `c2pnb272w1` | 272 | 3200 | 11,8 |
| `2pnb304w1` | 304 | 3200 | 13,7 |
| `c2tnb359v1` | 359 | 3600 | 21,2 |
| `c2pnb368w1` | 368 | 3600 | 22,9 |
| `c2tnb431r1` | 431 | 4000 | 33,3 |
| **Křivka** | $\mathbb{F}_{2^m}$ [b] | **Velikost haldy** [b] | **Čas** [s] |

# D VÝSLEDKY EXPERIMENTÁLNÍCH MĚŘENÍ PARAMETRICKÉ ZÁVISLOSTI ELIPTICKÝCH KŘIVEK NAD POLEM ŘÁDU 2 NA RASPBERRY PI 2B.

| Křivka | Velikost [b] | No. [-] | $t_{G1}$ [µs] | $\Delta t_1$ [%] |
|---|---|---|---|---|
| wtls1 | 2114 | 2 | 3,362 | 0,00 |
| wtls4 | 2114 | 0 | 3,496 | +3,99 |
| sect113r1 | 2114 | 0 | 3,5 | +4,10 |
| sect113r2 | 2114 | 0 | 3,528 | +4,94 |
| sect113k1 | 2114 | 0 | 3,487 | +3,72 |
| sect131r1 | 2132 | 0 | 6,235 | 0,00 |
| sect131r2 | 2132 | 0 | 6,464 | +3,67 |
| ipsec3 | 2156 | 4 | 6,417 | +2,92 |
| wtls3 | 2164 | 2 | 8,174 | +2,14 |
| wtls5 | 2164 | 0 | 8,815 | +10,15 |
| sect163r1 | 2164 | 0 | 8,802 | +9,98 |
| sect163k1 | 2164 | 2 | 8,197 | +2,42 |
| c2pnb163v1 | 2164 | 0 | 8,822 | +10,23 |
| c2pnb163v2 | 2164 | 0 | 8,795 | +9,92 |
| c2pnb163v3 | 2164 | 0 | 8,795 | +9,90 |
| c2pnb176v1 | 2177 | 0 | 8,739 | +9,20 |
| ipsec4 | 2186 | 4 | 8,003 | 0,00 |
| wtls10 | 2234 | 2 | 15,865 | +0,23 |
| wtls11 | 2234 | 1 | 17,474 | +10,40 |
| sect233r1 | 2234 | 1 | 17,493 | +10,52 |
| sect233k1 | 2234 | 2 | 15,828 | 0,00 |
| sect239k1 | 2240 | 2 | 16,244 | +2,63 |
| c2tnb239v1 | 2240 | 0 | 17,89 | +13,03 |
| c2tnb239v2 | 2240 | 0 | 17,843 | +12,73 |
| c2tnb239v3 | 2240 | 0 | 17,784 | +12,36 |
| sect283r1 | 2284 | 1 | 32,072 | +11,91 |
| sect283k1 | 2284 | 2 | 28,659 | 0,00 |
| sect409r1 | 2410 | 2 | 76,16 | +14,35 |
| sect409k1 | 2410 | 1 | 66,605 | 0,00 |
| sect571r1 | 2572 | 2 | 174,749 | +14,86 |
| sect571k1 | 2572 | 1 | 152,143 | 0,00 |

# E SROVNÁNÍ VÝSLEDKŮ EXPERIMENTÁLNÍCH MĚŘENÍ PARAMETRICKÉ ZÁVISLOSTI NA RASPBERRY PI 2B A MCU MSP430.

| Křivka | Velikost [b] | Par. 0 [-] | $t_{G1}$ [µs] | $\Delta t_1$ [%] | $t_{G2}$ [µs] | $\Delta t_2$ [%] |
|---|---|---|---|---|---|---|
| wtls6 | 112 | 0 | 2,555 | 0.00 | 10,696 | +8.68 |
| wtls8 | 112 | 4 | 2,953 | +15.58 | 10,897 | +10.72 |
| secp112r1 | 112 | 0 | 2,57 | +0.59 | 9,842 | 0.00 |
| secp112r2 | 112 | 0 | 2,599 | +1.72 | 11,413 | 15,96 |
| secp128r1 | 128 | 0 | 2,825 | +10.57 | 12,092 | 22,86 |
| secp128r2 | 128 | 0 | 2,899 | +13.46 | 12,986 | 31,94 |
| wtls7 | 160 | 0 | 4,13 | 0.00 | 13,031 | 0.00 |
| wtls9 | 160 | 4 | 4,704 | +13.90 | 19,612 | +50.50 |
| secp160r1 | 160 | 0 | 4,143 | +0.31 | 13,05 | +0.15 |
| secp160r2 | 160 | 0 | 4,143 | +0.31 | 13,963 | +7.15 |
| secp160k1 | 160 | 2 | 4,557 | +10.34 | 15,08 | +15.72 |
| secp192k1 | 192 | 2 | 6,364 | +11.92 | 23,674 | 7.57 |
| prime192v1 | 192 | 0 | 5,716 | +0.53 | 25,4 | 13.04 |
| prime192v2 | 192 | 0 | 5,686 | 0.00 | 22,47 | 0.00 |
| prime192v3 | 192 | 0 | 5,701 | +0.26 | 24,171 | 5.36 |
| wtls12 | 224 | 0 | 7,483 | +0.09 | 26,631 | 0.00 |
| secp224r1 | 224 | 0 | 7,476 | 0.00 | 27,02 | 1.46 |
| secp224k1 | 224 | 2 | 8,388 | +12.20 | 30,771 | 15.55 |
| secp256k1 | 256 | 2 | 11,007 | +12.28 | - | - |
| prime256v1 | 256 | 0 | 9,803 | 0.00 | - | - |

*Curriculum Vitae*

# Ing. Radek Fujdiak

**Základní údaje:**


| | |
|---|---|
| Adresa: | Březová 622/64 Brno 63700, Česká Republika |
| E-mail: | fujdiak@feec.vutbr.cz |
| Tel.: | +420 541 146 967, +420 723 745 239 |
| WWW: | https://www.vutbr.cz/en/people/radek-fujdiak-106440 |
| | https://www.linkedin.com/in/fujdiak/ |


**Pracovní zkušenosti:**

| | |
|---|---|
| 2017–dosud | Vědecký pracovník, Peoples' Friendship University, Rusko |
| 2013–dosud | Mladý výzkumný pracovník, Vysoké učení technické v Brně |
| 2013–dosud | Šéfredaktor ve vědecko-odborném časopise, Elektrorevue |
| 2010–2012 | Pomocný technický pracovník, Bachl s.r.o. |
| 2009 | IT Pracovník, Fakultní nemocnice Královské Vinohrady |
| 2008 | Analytik, QVISION s.r.o. |
| 2007 | Projektant energetických rozvodných sítí, ES Projekt s.r.o. |
| 2006 | Pomocný IT pracovník, AR System s.r.o. |

**Vzdělání:**

| | |
|---|---|
| 2013–2017 | Vysoké učení technické v Brně, Česká Republika, Ph.D.<br>Závěrečná práce: Analýza a optimalizace datové komunikace v telemetrických systémech pro energetiku |
| 2011–2013 | Vysoké učení technické v Brně, Česká Republika, Ing.<br>Závěrečná práce: Kryptografický protokol s veřejným klíčem |
| 2007–2011 | Vysoké učení technické v Brně, Česká Republika, Bc.<br>Závěrečná práce: Demonstrační kit technologie Keeloq |

**Dlouhodobé zahraniční vědecké stáže**:

| | |
|---|---|
| 2017 | Saint Petersburg State University of Aerospace Instrumentation, Rusko (měsíční stáž)<br>Téma výzkumu: Kryptografie & Eliptické křivky |
| 2013–2015, 2017 | Escuela Superior Politécnica, Španělsko (vždy měsíční stáž)<br>Téma výzkumu: Internet věcí & Chytrá města |

**Odborné znalosti**:

| | |
|---|---|
| Specializace | Kryptografie, Informační bezpečnost, Počítačová a síťová bezpečnost, Energetika a inteligentní sítě, zařízení s limitovanými zdroji, Eliptické křivky, Bezdrátové komunikační technologie, Kybernetická bezpečnost, Chytré technologie, |
| Programování | C/C++(Expert), C# (Pokročilý), HTML/CSS (Středně Pokročilý), JAVA(Základy), Python (Základy) |
| Certifikace | Kurzy CISCO Akademie (CCNA1–4), Brno |

**Jazykové dovednosti**:

Čeština (Rodilý mluvčí), Angličtina (C1), Němčina (B2)

**Ocenění**:

| | |
|---|---|
| 2016 | EEICT 2016 - Druhé místo vědecké soutěže v rámci konference EEICT 2016 |
| 2015 | EEICT 2015 - Druhé místo vědecké soutěže v rámci konference EEICT 2015 |

**Participace na vědeckých projektech:**

| | |
|---|---|
| 2017–dosud | VI20172019057, Monitoring a analýza komunikace pro bezpečnostní dohled kritických energetických infrastruktur |
| 2017–dosud | LO1401, Interdisciplinární výzkum bezdrátových technologií (INWITE) |
| 2016–dosud | VI20162018007, Výzkum a vývoj inteligentního systému pro řízení energetických sítí a identifikaci hrozeb v energetické infrastruktuře |
| 2016–dosud | TF02000036, Nové metody pro optimalizaci energetické náročnosti a škálovatelnosti ultraširokopásmových lokalizačních systémů |
| 2016–dosud | TA04021490, Prvky pro zavedení Smart Grids v distribučních sítích |
| 2016 | HS18457030, Studie a výběr nejvhodnější komunikační technologie |

| | |
|---|---|
| | pro konkrétní use case: Smart Grid a provoz mřížové sítě v lokalitě Brno |
| 2013–2016 | CZ.1.05/2.1.00/03.0072, Centrum senzorických, informačních a komunikačních systémů |
| 2013–2015 | TA03010818, Využití moderních kryptografických metod pro zabezpečení komunikace v telematických systémech |
| 2013–2015 | TA02020856, Aplikovaný výzkum inteligentních systémů pro sledování energetických sítí |

**Odborný recenzent:**

• Mezinárodní expert pro projekty v programu "Operational Programme Research and Innovation 2014–2020" (Ministerstvo školství, vědy a výzkumu, Slovenská republika)
• Odborný recenzent projektů bezpečnostního výzkumu programu BV III/1-VS (Ministerstvo vnitra, Česká Republika)
• Odborný recenzent projektů aplikačního charakteru programů $\alpha$–$\zeta$ (Technologická agentura České republiky)
• Odborný recenzent projektů aplikačního charakteru programu MPO TRIO (Ministerstvo průmyslu, Česká republika)
• Odborný recenzent pro vědecký časopis Pervasive and Mobile Computing (IF: 1.719, ISSN: 1574–1192)
• Odborný recenzent pro vědecký časopis Transactions on Internet and Information Systems (IF: 0.365, ISSN: 1976–7277)
• Odborný recenzent pro mezinárodní konferenci Information and Software Technologies (Indexována ve WoS/Scopus)
• Odborný recenzent pro mezinárodní konferenci Advances in Computing, Communications and Informatics (Indexována ve WoS/Scopus)
• Odborný recenzent pro mezinárodní konferenci Telecommunications and Signal Processing (Indexována ve WoS/Scopus)
• Odborný recenzent pro mezinárodní konferenci Ultra Modern Telecommunications & Control Systems (Indexována ve WoS/Scopus)
• Zvaný recenzent pro mezinárodní sympozium Signal Processing for Wireless and Multimedia Communication (Indexována ve WoS/Scopus)

**Vybrané zvané přednášky:**

• 2017, Talent Education Era+ 2017, Brno, Česká Republika
• 2016, Czech IoT Summit 2016, Prague, Česká Republika
• 2015, Escuela Superior Politécnica, Mataro, Spain
• 2014, Intelligent Buildings, Brno, Česká Republika

**Publikační aktivita:**

• Články publikované v impaktovaných časopisech: **7** (*+1 v tisku*)
• Články v ostatních odborných/vědeckých časopisech: **6**
• Články ve sborníku mezinárodní konference indexované ve WoS/Scopus: **22**
• Články ve sbornících ostatních konferencí: **6**
• H-index odpovídající databázi WoS (k 7/2017): **3** (celkem 17 citací)
• H-index odpovídající databázi Scopus (k 7/2017): **3** (celkem 30 citací)
• Produkty: **5**

**Pedagogické zkušenosti:**

| | |
|---|---|
| 2016–dosud | Asistující přednášející, Vyšší techniky datových přenosů – MVDP (VUT v Brně) |
| 2014–dosud | Vedoucí laboratoří, Datové komunikace – BDAK (VUT v Brně) |
| 2017 | Vedení odborné stáže vědecké pracovnice z Norska |
| 2016 | Vedení odborné stáže třech zahraničních studentů z Ruska |

**Reference:**

*Prof. Sergey Bezzateev*
Vedoucí ústavu Informační bezpečnosti
Saint-Petersburg State University of Aerospace Instrumentation
Bolshaya Morskaya str., 190000, Saint-Petersburg, Rusko
Email: bsv@aanet.ru

*Dr. Leonard Janer Garcia*
Vedoucí transferu technologií (TTO)
Fundacio Tecnocampus Mataro-Maresme
Av.Ernest Llunch 2, 08302, Mataro, Španělsko
Email: leonard@tecnocampus.cat