VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

ÚSTAV TELEKOMUNIKACÍ

Ing. Vlastimil Člupek

AUTENTIZACE S VYUŽITÍM LEHKÉ KRYPTOGRAFIE

AUTHENTICATION USING LIGHTWEIGHT CRYPTOGRAPHY

ZKRÁCENÁ VERZE PH.D. THESIS

Obor: Teleinformatika

Školitel: doc. Ing. Václav Zeman, Ph.D.

Oponenti:

Datum obhajoby:

KLÍČOVÁ SLOVA

Lehká kryptografie, autentizace, hashovací funkce, fyzicky neklonovatelné funkce, nízkonákladová zařízení, Internet věcí.

KEYWORDS

Lightweight cryptography, authentication, hash functions, physical unclonable functions, low-cost devices, Internet of Things.

MÍSTO ULOŽENÍ PRÁCE

Disertační práce je k dispozici na Vědeckém oddělení děkanátu FEKT VUT v Brně, Technická 10, Brno, 616 00.

ISBN 80-214-

ISSN 1213-4198

OBSAH

1 ÚVOD

V dnešní době se telekomunikace stává neoddělitelnou součástí lidských životů. Nejrychleji rostoucím komunikačním prvek je v současné době Internet. Tento komunikační prostředek se neustále vyvíjí. Nyní Internet směřuje do jeho další fáze, ve které bude podstatnou roli hrát Internet věcí (Internet of Things – IoT). Internet věcí obvykle používá nízkonákladová zařízení ke sběru a výměně dat ze senzorů a dalších zařízení. Nízkonákladová zařízení, podle RFC 7228 označována jako „constrained devices“ („omezená zařízení“) zastupují zařízení s omezeným výpočetním výkonem, paměťovým prostorem, napájecím napětím či jinak omezená zařízení. Tato zařízení používají ke komunikaci bezdrátové senzorové sítě (Wireless Sensor Networks – WSN), technologii RFID, NFC, Bluetooth, ZigBee, Z-wave, 3G a 4G/LTE mobilní komunikační spojení, technologii Wi-Fi, WiMAX, Sigfox a podobně. Zařízení vytvářející Internet věcí jsou určena k implementaci v chytrých domácnostech, městech, nemocnicích, v průmyslu atd. Aby získaná data z těchto zařízení byla důvěryhodná, musí být tato zařízení a data z těchto zařízení vhodným způsobem zabezpečena. Elektronickou komunikaci mezi zařízeními po nezabezpečeném kanále je možné zabezpečit pomocí kryptografických protokolů. Tyto protokoly bývají navrhovány podle potřeb a hardwarového vybavení zařízení, jenž mají být použity k zajištění požadovaného zabezpečení. Pomocí primitiv ze symetrické a asymetrické kryptografie je možné zajistit integritu, autentičnost, důvěrnost či nepopiratelnost. Integrita zajišťuje celistvost a neměnnost dat. Autentičnost zajišťuje ověření identity osob/zařízení či zdroje dat. Důvěrnost zajišťuje, že utajovaná informace nebude dostupná neautorizovanému subjektu. Nepopiratelnost zajišťuje, že subjekt zúčastněný dané komunikace nebude moci popřít událost, kterou v minulosti vykonal. Symetrická kryptografie používá sdílený tajný klíč a je obecně méně náročná než asymetrická kryptografie využívající soukromý a veřejný klíč. Nevýhodou symetrické kryptografie je obtížná distribuce tajného klíče. Asymetrická kryptografie řeší problém distribuce tajného klíče u symetrické kryptografie. Z tohoto důvodu dochází v některých případech ke kombinování symetrické a asymetrické kryptografie. Integritu dat je možné zajistit pomocí hashovacích funkcí. Pro účely autentizace mohou dostatečně hardwarově vybavená zařízení použít k autentizaci technologie využívané v Infrastruktuře veřejných klíčů (Public Key Infrastructure – PKI), jenž je založena na asymetrické kryptografii. Při tomto způsobu autentizace musí být autentizovaná zařízení dostatečně výpočetně a zdrojově vybavená, aby byla schopná provádět matematické operace jako je modulární mocnění s 1024 (2048) bitovými čísly v případě RSA algoritmu. Takové to operace ve většině případů nedokáží nízkonákladová zařízení vykonat. Autentizace na nízkonákladových zařízeních se tak často provádí pomocí protokolů na základě symetrické kryptografie využívající sdílené tajemství.

Toto tajemství představuje tajný klíč o velikosti minimálně 80 bitů, aby byl považován za dostatečně bezpečný. Při využití sdíleného tajemství jsou tedy využívány podstatně menší velikosti klíčů při zachování obdobné kryptografické bezpečnosti v porovnání s RSA. Autentizace na nízkonákladových zařízeních je prováděna pomocí algoritmů lehké kryptografie. Lehká kryptografie (Lightweight Cryptography) je nové odvětví kryptografie, jenž se zabývá návrhem nebo optimalizací kryptografických algoritmů pro implementaci na nízkonákladových zařízeních. Tyto algoritmy jsou nenáročné na výpočetní výkon či paměťový prostor. Lehká kryptografie může být využita také k zajištění důvěrnosti na nízkonákladových zařízeních pro informace, které jsou omezené svojí cenou nebo časem utajení. Zajištění nepopiratelnosti provedených událostí je doménou především asymetrické kryptografie, avšak s využitím důvěryhodné třetí strany (DTS) je možné zajistit nepopiratelnost i pomocí symetrické kryptografie, kdy DTS zajistí vyřešení případných sporů mezi komunikujícími stranami, kdy jedna strana bude tvrdit že nastala určitá událost, zatímco druhá strana bude tvrdit, že tato událost nenastala. Autentizační protokoly využívající lehkou kryptografii jsou ve většině případů postaveny na symetrické kryptografii, kdy je mezi komunikujícími stranami zabezpečeným způsobem přenášen tajný symetrický autentizační klíč. V těchto případech zabezpečená autentizační zpráva musí být náhodná, neopakovatelná, musí být zachována její integrita a autentizační klíč musí zůstat důvěrný. V určitých případech může být u autentizačních protokolů vyžadováno zajištění nepopiratelnosti provedených událostí. Náhodnost přenášených dat je důležitá z hlediska možné kryptoanalýzy. Čím větší je náhodnost přenášených dat, tím těžší je pro útočníka odhalení tajného autentizačního klíče. Přenášená data by měla být neopakovatelná, aby útočník nemohl provést útok zopakováním již jednou použitých platných autentizačních dat. Za tímto účelem bývají v přenášených datech zahrnuta jedinečná čísla (nonce) nebo sekvenční čísla. Pokud útočník odhalí autentizační klíč, znamená to okamžité zneplatnění klíče pro budoucí autentizační relaci. Zajištění nepoporatelnosti provedených událostí je důležité pro vyřešení případných sporů mezi komunikujícími stranami. Alternativu ke klasickému způsobu autentizování využívající tajný symetrický klíč představují fyzicky neklonovatelné funkce (Physical Unclonable Functions – PUFs). Tyto funkce lze využít k autentizaci či generování šifrovacího klíče. Fyzicky neklonovatelné funkce (FNF) existují v řadě provedení a mnohé z nich umožňují implementaci na nízkonákladových zařízeních.

Předmětem práce je návrh tří autentizačních protokolů, jednosměrného autentizačního protokolu se zabezpečeným přenosem dat, obousměrného autentizačního protokolu se zabezpečeným přenosem dat a obousměrného autentizačního protokolu se zajištěním nepopiratelnosti, jenž jsou vhodné pro implementaci na nízkonákladových zařízeních. Kapitola 3 se zabývá návrhem jednosměrného autentizačního

protokolu se zabezpečeným přenosem dat, využívající hašovací funkce, fyzicky neklonovatelnou funkci, korekční kód a operaci exkluzivní disjunkce. Kapitola 4 se zabývá návrhem obousměrného autentizačního protokolu se zabezpečeným přenosem dat, využívající hašovací funkce, fyzicky neklonovatelné funkce, korekční kódy a operace exkluzivní disjunkce. V kapitole 5 je popsán návrh obousměrného autentizačního protokolu se zajištěním nepopiratelnosti uskutečněných událostí využívající hashovací funkce, sekvenční čísla a důvěryhodnou třetí stranu. Závěr k této zkrácené verzi disertační práci je sepsán v kapitole 6.

2 CÍLE PRÁCE

Zabezpečení na nízkonákladových zařízeních je aktuální výzvou pro kryptografy. Nízkonákladová zařízení neumožňují implementaci standardních kryptografických primitiv, a tak dochází k jejich úpravám a optimalizacím, anebo k vývoji nových kryptografických primitiv speciálně určených pro implementaci na nízkonákladových zařízeních. Zabezpečení na nízkonákladových zařízeních je doménou především symetrické lehké kryptografie, pro kterou byly navrženy proudové a blokové šifrovací algoritmy a hashovací funkce. Asymetrická kryptografie je vhodná pro situace, kdy zařízení poskytuje dostatečné výpočetní a zdrojové prostředky pro implementaci asymetrického algoritmu. Asymetrická kryptografie může být v určitých případech implementována i na nízkonákladových zařízeních. V těchto případech se využívá méně náročných asymetrických schémat využívající např. eliptické křivky.

Disertační práce se zaměřuje na výzkum v oblasti autentizace na nízkonákladových zařízeních a na návrh nových autentizačních protokolů zajišťující jednosměrnou a obousměrnou autentizaci komunikujících stran pomocí nových kryptografických přístupů, integritu přenesených dat, důvěrnost citlivých informací a nepopiratelnost uskutečněných událostí. Navržené protokoly používají pouze hashovací funkce, fyzicky neklonovatelné funkce, korekční kódy a operace XOR, umožnující implementaci na zařízeních, jenž mají omezené výpočetní, paměťové či napájecí prostředky.

Hlavní cíle disertační práce jsou:

- Analýza současných autentizačních algoritmů vhodných pro implementaci na nízkonákladových zařízeních (provedeno v plné verzi disertační práce).
- Návrh nového jednosměrného autentizačního protokolu se zabezpečeným přenosem dat.
- Návrh nového obousměrného autentizačního protokolu se zabezpečeným přenosem dat.
- Návrh nového obousměrného autentizačního protokolu zajišťující nepopiratelnost uskutečněných událostí.
- Provedení bezpečnostní analýzy u navržených protokolů (provedeno v plné verzi disertační práce).

3 NÁVRH JEDNOSMĚRNÉHO AUTENTIZAČNÍHO PROTOKOLU SE ZABEZPEČENÝM PŘENOSEM DAT

Tato kapitola se zabývá popisem jednosměrného autentizačního protokolu a protokolu zabezpečeného přenosu dat bez potvrzení příjmu dat, jenž jsou vhodné pro implementaci na nízkonákladových zařízeních. Princip navrženého jednosměrného autentizačního protokolu se zabezpečeným přenosem dat byl publikován v [1].

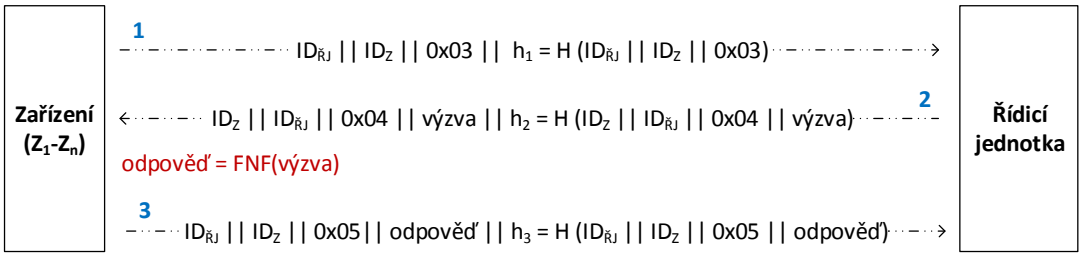
3.1 Jednosměrný autentizační protokol

Před aplikací tohoto protokolu je nutné vykonat protokol pro vytvoření databáze PVO a PD (definovaný v plné verzi disertační práce) pro vytvoření párů *výzva-odpověď* pro jednotlivé fyzicky neklonovatelné funkce a pomocných dat pro korekční kódy, jenž jsou implementované v nízkonákladových zařízeních $Z_1 - Z_n$. Po vytvoření databáze párů *výzva-odpověď* je možné vykonání algoritmu jednosměrné autentizace. Na Obr. 3.1 je vidět princip protokolu jednosměrné autentizace využívající tři zprávy, jenž jsou vyměňovány mezi zařízením $Z_1 - Z_n$ a řídicí jednotkou. Komunikaci vždy zahajuje zařízení $Z_1 - Z_n$. Zpráva 1 slouží k zaslání požadavku na autentizaci od zařízení $Z_1 - Z_n$ k řídicí jednotce a k ochraně proti útoku vytvoření databáze PVO a PD. Zpráva 2 slouží k zaslání autentizační *výzvy* od řídicí jednotky k zařízení $Z_1 - Z_n$. Zpráva 3 slouží k zaslání autentizační *odpovědi* od zařízení $Z_1 - Z_n$ k řídicí jednotce. Struktura zpráv 1, 2 a 3 je následující:

- **Zpráva 1**: $ID_{\check{R}J}||ID_Z||0x03||h_1 = H(ID_{\check{R}J}||ID_Z||0x03)$
- **Zpráva 2**: $ID_Z||ID_{\check{R}J}||0x04||výzva||h_2 = H(ID_Z||ID_{\check{R}J}||0x04||výzva)$
- **Zpráva 3**: $ID_{\check{R}J}||ID_Z||0x05||odpověď||h_3 = H(ID_{\check{R}J}||ID_Z||0x05||odpověď)$

Kde $ID_{\check{R}J}$ reprezentuje identitu řídicí jednotky a ID_Z reprezentuje identitu zařízení $Z_1 - Z_n$. Numerická hodnota 0x03 značí, že zařízení $Z_1 - Z_n$ se chce autentizovat k řídicí jednotce. Zařízení je rozlišeno pomocí jeho identifikátoru (ID_Z). Numerická hodnota 0x04 značí, že za ní bude následovat *výzva* pro fyzicky neklonovatelnou funkci implementovanou v daném zařízením. Numerická hodnota 0x05 značí, že za ní bude následovat *odpoveď* od konkrétní fyzicky neklonovatelné funkce implementované v daném zařízení. Hashe h_1, h_2 a h_3 slouží k ověření integrity přenášených dat ve zprávách 1, 2 a 3.

Princip protokolu jednosměrné autentizace je následující. Nízkonákladové zařízení $Z_1 - Z_n$ začne komunikaci tím, že odešle zprávu 1 do řídicí jednotky. Po přijetí



Obr. 3.1: Princip jednosměrné autentizace.

zprávy řídicí jednotka vypočítá hash z přijatých dat $ID_{\check{R}J}||ID_Z||0x03$ a porovná ho s přijatým hashem h_1. Pokud si budou rovny, integrita přenesených dat bude zaručena. Řídicí jednotka poté zkontroluje podle identifikátoru zařízení, jestli má ve své databázi uloženy páry *výzva-odpověď* pro fyzicky neklonovatelnou funkci implementovanou v daném zařízení. Pokud ano, odešle zprávu 2 do daného zařízení obsahující *výzvu* pro fyzicky neklonovatelnou funkci implementovanou v daném zařízení. Po přijetí zprávy, zařízení vypočítá hash z přijatých dat $ID_Z||ID_{\check{R}J}||0x04||výzva$ a porovná ho s přijatým hashem h_2. Pokud si budou rovny, integrita přenesených dat bude zaručena. Zařízení poté pomocí své fyzicky neklonovatelné funkce vypočítá z přijaté *výzvy* korektní *odpověď*. Tato operace je v protokolu značena jako *odpověď* $= FNF(výzva)$. Poté zařízení odešle řídicí jednotce zprávu 3, obsahující vypočítanou *odpověď*. Následně si zařízení uloží *výzvu* použitou pro vygenerování odeslané *odpovědi* do seznamu použitých *výzev*. Po přijetí zprávy 3, řídicí jednotka vypočítá hash z přijatých dat $ID_{\check{R}J}||ID_Z||0x05||odpověď$ a porovná ho s přijatým hashem h_3. Pokud si budou rovny, integrita přenesených dat bude zaručena. Řídicí jednotka poté porovná přijatou *odpověď* s *odpovědí*, jenž má uloženou ve své databázi a jenž tvoří pár s *výzvou*, kterou řídicí jednotka v předchozím kroku zaslala do daného zařízení. Pokud si budou rovny nebo Hammingova vzdálenost mezi přijatou *odpovědí* a uloženo *odpovědí* bude dostatečně malá, bude dané zařízení autentizováno k řídicí jednotce.

Důležitým požadavkem pro jednoznačnou autentizaci zařízení $Z_1 - Z_n$ je, aby řídicí jednotka nepoužila k autentizaci vícenásobně jednu stejnou *výzvu*. Důvodem, je že *výzvy* a *odpovědi* jsou odesílány v otevřené podobě a útočník by mohl provést útok zopakováním, kdy by se vydával za dané zařízení.

Pokud bude v zařízení implementován i protokol zabezpečeného přenosu dat bez potvrzení příjmu dat, zařízení $Z_1 - Z_n$ si za tímto účelem musí ukládat do paměti seznam použitých *výzev*. Tento krok zajistí, že zařízení $Z_1 - Z_n$ v protokolu zabez-

pečeného přenosu dat bez potvrzení příjmu dat nepoužije k šifrování dat *odpověď*, kterou již jednou zařízení použilo k autentizaci nebo k šifrování tajných dat.

3.2 Protokol zabezpečeného přenosu dat bez potvrzení příjmu dat

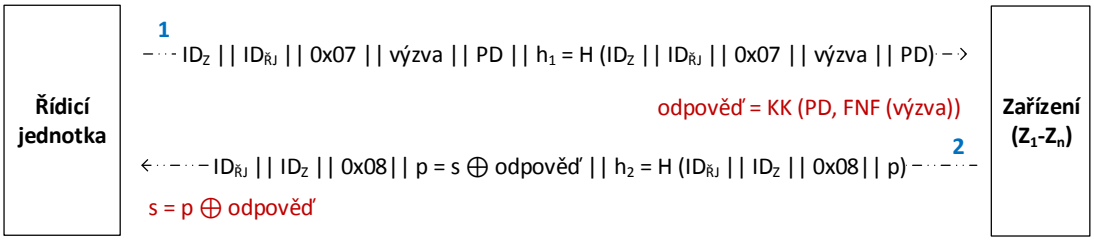
Před aplikací tohoto protokolu, musí být vykonán protokol pro vytvoření databáze PVO a PD (definovaný v plné verzi disertační práce) a jednosměrný autentizační protokol (definovaný v kapitele 3.1) pro autentizaci zařízení $Z_1 - Z_n$ k řídicí jednotce. Po autentizaci zařízení $Z_1 - Z_n$ k řídicí jednotce je možné vykonání algoritmu protokolu zabezpečeného přenosu dat bez potvrzení příjmu dat. Přenos dat se uskutečňuje ze zařízení $Z_1 - Z_n$ do řídicí jednotky. Tento protokol využívá dvě zprávy, jenž jsou vyměňovány mezi řídicí jednotkou a zařízením $Z_1 - Z_n$. Komunikaci zahajuje řídicí jednotka. Na Obr. 3.2 je vidět princip protokolu zabezpečeného přenosu dat bez potvrzení příjmu dat. Zpráva 1 slouží k zaslání *výzvy* a pomocných dat řídicí jednotkou do zařízení $Z_1 - Z_n$. Zpráva 2 slouží k odeslání dat zabezpečeným způsobem zařízením $Z_1 - Z_n$ do řídicí jednotky. Struktura zpráv 1 a 2 je následující:

- **Zpráva 1**: $ID_Z||ID_{\check{\mathrm{R}}J}||0x07||výzva||PD||h_1 = H(ID_Z||ID_{\check{\mathrm{R}}J}||0x07||výzva||PD)$
- **Zpráva 2**: $ID_{\check{\mathrm{R}}J}||ID_Z||0x08||p = s \oplus odpověď||h_2 = H(ID_{\check{\mathrm{R}}J}||ID_Z||0x08||p)$

Kde ID_Z reprezentuje identitu konkrétního zařízení a $ID_{\check{\mathrm{R}}J}$ reprezentuje identitu řídicí jednotky. Numerická hodnota 0x07 značí, že za ní bude následovat *výzva* pro fyzicky neklonovatelnou funkci implementovanou v daném zařízením a za ní pomocná data (PD) pro korekční kód. Numerická hodnota 0x08 značí, že za ní bude následovat veřejná hodnota p, jenž slouží k zabezpečenému přenosu tajných dat s do řídicí jednotky ze zařízení $Z_1 - Z_n$. Hashe h_1 a h_2 slouží k ověření integrity přenášených dat ve zprávách 1 a 2.

Princip protokolu zabezpečeného přenosu dat bez potvrzení příjmu dat je následující. Řídicí jednotka začne komunikaci tím, že odešle zprávu 1 do zařízení $Z_1 - Z_n$ obsahující *výzvu* pro fyzicky neklonovatelnou funkci a PD pro korekční kód, jenž se nachází v daném zařízení. Po přijetí zprávy, dané zařízení vypočítá hash z přijatých dat $ID_Z||ID_{\check{\mathrm{R}}J}||0x07||$ $výzva||PD$ a porovná ho s přijatým hashem h_1. Pokud si budou rovny, integrita přenesených dat bude zaručena. Zařízení poté porovná přijatou *výzvu* s *výzvami* uloženými na seznamu použitých výzev, pokud zde nenalezne shodu, zařízení pomocí své fyzicky neklonovatelné funkce vypočítá z přijaté *výzvy*

korektní *odpověď* a následně tuto vypočítanou *odpověď* upraví pomocí svého korekčního kódu s využitím přijatých PD do výsledného požadovaného tvaru. Tato operace je v protokolu značena jako $odpověď = KK(PD, FNF(výzva))$. Následně dané zařízení odešle řídicí jednotce zprávu 2, obsahující veřejnou hodnotu $p = s \oplus odpověď$, sloužící k zabezpečenému přenosu dat ze zařízení do řídicí jednotky. Následně si zařízení uloží *výzvu* použitou pro vygenerování *odpovědi* s níž zařízení šifrovalo tajná data s do seznamu použitých výzev. Po přijetí zprávy 2, řídicí jednotka vypočítá hash z přijatých dat $IP_{\check{R}J}||IP_Z||0x08||p$ a porovná ho s přijatým hashem h_2. Pokud si budou rovny, integrita přenesených dat bude zaručena. Řídicí jednotka poté vypočítá tajná data $s = p \oplus odpověď$ pomocí přijaté veřejné hodnoty p a ve své databázi uložené *odpovědi*, jenž tvoří pár s *výzvou* a pomocnými daty, jenž řídicí jednotka v předchozím kroku zaslala do daného zařízení.



Obr. 3.2: Princip protokolu zabezpečeného přenosu dat bez potvrzení příjmu dat.

Pokud část tajných dat s bude nabývat hodnot v definovaném rozsahu, může být zpráva s použita k částečné autentizaci původu dat.

V tomto protokolu je důležité, aby *odpověď* jenž byla zařízením využita při tvorbě veřejné hodnoty p byla stejná jako *odpověď* uložená v databázi řídicí jednotky, aby dešifrování tajných dat s proběhlo korektně. Za tímto účelem je nutné na výstup fyzicky neklonovatelné funkce implementovat vhodný korekční (protichybový) kód, aby daná fyzicky neklonovatelná funkce generovala na základě konkrétní *výzvy* a konkrétních pomocných dat vždy stejnou *odpověď*. Důležitým požadavkem pro bezpečný přenos dat ze zařízení $Z_1 - Z_n$ do řídicí jednotky je, aby zařízení nepoužilo k šifrování tajných dat vícenásobně stejnou *odpověď*. Této podmínky je v protokolu dosaženo tím, že zařízení $Z_1 - Z_n$ si do své paměti ukládá použité *výzvy* a na opakující se *výzvy* nereaguje. Další podmínkou pro bezpečnost přenášených dat je, aby přenášená tajná data s měla stejnou velikost jako *odpověď* s níž je vykonána operace exkluzivní disjunkce.

4 NÁVRH OBOUSMĚRNÉHO AUTENTIZAČNÍHO PROTOKOLU SE ZABEZPEČENÝM PŘENOSEM DAT

Tato kapitola se zabývá popisem obousměrného autentizačního protokolu a protokolu pro zabezpečený přenos dat s potvrzením příjmu dat, jenž jsou vhodné pro implementaci na nízkonákladových zařízeních. Obousměrný autentizační protokol musí být vykonán před aplikací protokolu zabezpečeného přenosu dat s potvrzením příjmu dat. Princip navrženého obousměrného autentizačního protokolu se zabezpečeným přenosem dat byl publikován v [2].

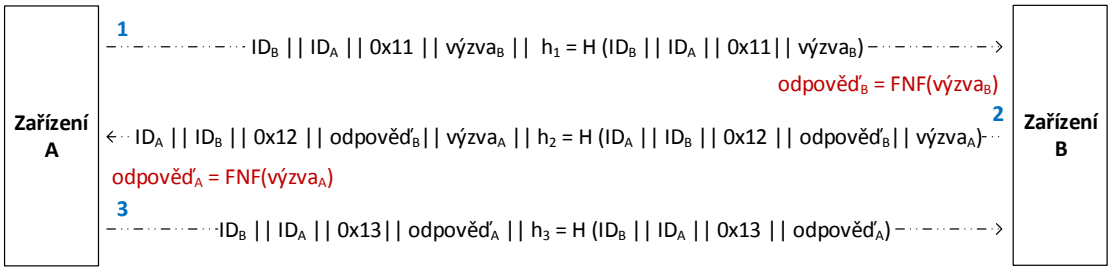
4.1 Obousměrný autentizační protokol

Před aplikací obousměrného autentizačního protokolu je nutné, aby zařízení A a B vykonalo protokol pro výměnu PVO, PV a PD (definovaný v plné verzi disertační práce) pro zaslání příslušných PVO, PV a PD do zařízení A a B. Po vykonání tohoto protokolu, kdy zařízení A vlastní PVO_B a PV_{AB} a zařízení B vlastní PVO_A a PV_{BA}, je možné vykonání algoritmu obousměrného autentizačního protokolu. Komunikaci může zahájit jak zařízení A, tak zařízení B. Na Obr. 4.1 je vidět princip protokolu obousměrné autentizace, kdy komunikaci zahajuje zařízení A. Pokud by komunikaci zahajovalo zařízení B, postup by byl zrcadlově opačný. V protokolu jsou využívány tři zprávy, jenž jsou vyměňovány mezi zařízeními A a B. V případě, kdy komunikaci zahajuje zařízení A, zpráva 1 slouží k zaslání autentizační $výzvy_B$ od zařízení A do zařízení B. Zpráva 2 slouží k zaslání autentizační $odpověď_B$ a k zaslání autentizační $výzvy_A$ od zařízení B do zařízení A. Zpráva 3 slouží k zaslání autentizační $odpověď_A$ od zařízení A do zařízení B. Struktura zpráv 1, 2 a 3 je následující:

- **Zpráva 1**: $ID_B||ID_A||0x11||výzva_B||h_1 = H(ID_B||ID_A||0x11||výzva_B)$
- **Zpráva 2**: $ID_A||ID_B||0x12||odpověď_B||výzva_A||h_2$
  $h_2 = H(ID_A||ID_B||0x12||odpověď_B||výzva_A)$
- **Zpráva 3**: $ID_B||ID_A||0x13||odpověď_A||h_3 = H(ID_{ŘJ}||ID_Z||0x13||odpověď_A)$

Kde ID_A reprezentuje identitu zařízení A a ID_B reprezentuje identitu zařízení B. Numerická hodnota 0x11 značí, že za ní bude následovat $výzva_B$ pro fyzicky neklonovatelnou funkci implementovanou v zařízení B. Numerická hodnota 0x12 značí, že za ní bude následovat $odpověď_B$ od fyzicky neklonovatelné funkce implementované v zařízení B a za ní bude následovat $výzva_A$ pro fyzicky neklonovatelnou funkci implementovanou v zařízení A. Numerická hodnota 0x13 značí, že za ní bude ná-

sledovat *odpověď*$_A$ od fyzicky neklonovatelné funkce implementované v zařízení A. Hashe h_1, h_2 a h_3 slouží k ověření integrity přenášených dat ve zprávách 1, 2 a 3.



Obr. 4.1: Princip obousměrné autentizace.

Princip protokolu obousměrné autentizace v případě, kdy komunikaci zahajuje zařízení A bude následující.

Zařízení A odešle zprávu 1 do zařízení B. Po přijetí zprávy zařízení B vypočítá hash z přijatých dat $ID_B||ID_A||0x11||výzva_B$ a porovná ho s přijatým hashem h_1. Pokud si budou rovny, integrita přenesených dat bude zaručena. Poté zařízení B porovná přijatou *výzvu*$_B$ s *výzvami* uloženými v seznamu PV_{BA}. Pokud zde nalezne shodu, zkontroluje, jestli má ve své databázi uloženy PVO_A pro fyzicky neklonovatelnou funkci implementovanou v zařízení A. Pokud ano, zařízení B pomocí implementované fyzicky neklonovatelné funkce vypočítá z přijaté *výzvy*$_B$ korektní *odpověď*$_B$. Tato operace je v protokolu značena jako *odpověď*$_B$ = $FNF(výzva_B)$. Následně zařízení B odešle zařízení A zprávu 2, obsahující vypočítanou *odpověď*$_B$ a *výzvu*$_A$. Po přijetí zprávy zařízení A vypočítá hash z přijatých dat $ID_A||ID_B||0x12||$*odpověď*$_B||výzva_A$ a porovná ho s přijatým hashem h_2. Pokud si budou rovny, integrita přenesených dat bude zaručena. Zařízení A poté porovná přijatou *odpověď*$_B$ s *odpovědí*$_{B'}$, jenž má uloženou ve své databázi a jenž tvoří pár s *výzvou*$_B$, kterou zařízení A v předchozím kroku zaslalo do zařízení B. Pokud si budou rovny nebo Hammingova vzdálenost mezi přijatou *odpovědí*$_B$ a uloženo *odpovědí*$_{B'}$ bude dostatečně malá, bude zařízení B autentizováno k zařízení A. Následně zařízení A porovná přijatou *výzvu*$_A$ s *výzvami* uloženými v seznamu PV_{AB}. Pokud zde nalezne shodu, tak zařízení A pomocí implementované fyzicky neklonovatelné funkce vypočítá z přijaté *výzvy*$_A$ korektní *odpověď*$_A$. Tato operace je v protokolu značena jako *odpověď*$_A$ = $FNF(výzva_A)$. V dalším kroku zařízení A odešle zařízení B zprávu 3, obsahující vypočítanou *odpověď*$_A$, jenž slouží k autentizaci zařízení A. Po přijetí zprávy zařízení B vypočítá hash z přijatých dat $ID_B||ID_A||0x13||$*odpověď*$_A$ a porovná ho s přijatým hashem h_3. Pokud si budou

rovny, integrita přenesených dat bude zaručena. Zařízení B poté porovná přijatou *odpověď*$_A$ s *odpovědí*$_{A'}$, jenž má uloženou ve své databázi a jenž tvoří pár s *výzvou*$_A$, kterou zařízení B v předchozím kroku zaslalo do zařízení A. Pokud si budou rovny nebo Hammingova vzdálenost mezi přijatou *odpovědí*$_A$ a uloženo *odpovědí*$_{A'}$ bude dostatečně malá, bude zařízení A autentizováno k zařízení B.

Důležitým požadavkem pro jednoznačnou autentizaci zařízení A a B je, aby zařízení A nepoužilo vícenásobně jednu *výzvu*$_B$ pro autentizaci zařízení B a aby zařízení B nepoužilo vícenásobně jednu *výzvu*$_A$ pro autentizaci zařízení A. Tato podmínka je v protokolu zajištěna tím, že zařízení A a B po využití *výzvy* a k ní odpovídající *odpovědi* odstraní tento pár *výzva-odpověď* ze seznamu autentizačních PVO.

Ochrana proti neoprávněné autentizaci je zajištěna pomocí seznamu povolených *výzev*, na které může zařízení od daného zařízení reagovat. Příchozí *výzvy* pak zařízení porovnává s povolenými *výzvami*. Pokud nalezne shodu, tak vygeneruje *odpověď* pomocí FNF na základě přijaté *výzvy* a tuto *výzvu* odstraní ze seznamu povolených výzev.

4.2 Protokol zabezpečeného přenosu dat s potvrzením příjmu dat

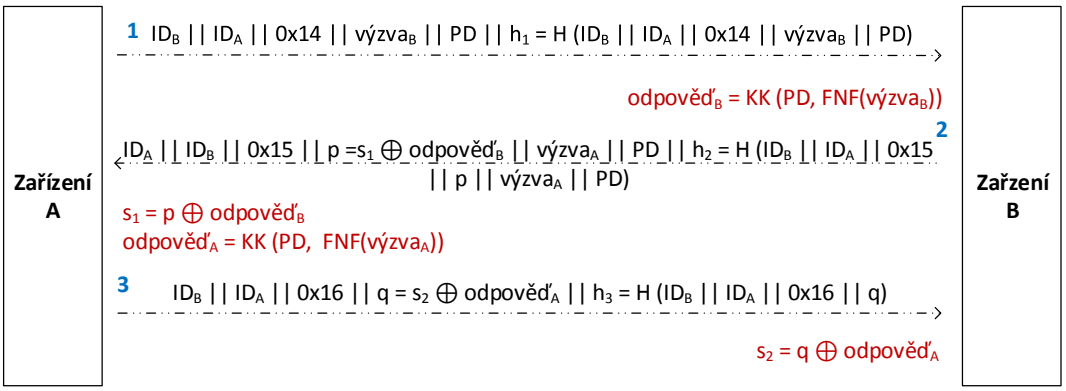
Před aplikací tohoto protokolu, musí být vykonán protokol pro vytvoření databáze PVO, PV a PD (definovaný v plné verzi disertační práce) a obousměrný autentizační protokol (definovaný v kapitole 4.1). Po vykonání těchto protokolů, kdy zařízení A a B vlastní příslušné databáze PVO, PV a PD a zařízení A a B se navzájem autentizovali, je možné vykonání algoritmu protokolu zabezpečeného přenosu dat s potvrzením příjmu dat. Komunikaci může zahájit jak zařízení A, tak zařízení B. Na Obr. 4.2 je vidět princip protokolu zabezpečeného přenosu dat s potvrzením příjmu dat, kdy komunikaci zahajuje zařízení A. Pokud by komunikaci zahajovalo zařízení B, postup by byl zrcadlově opačný. V protokolu jsou využívány tři zprávy, jenž jsou vyměňovány mezi zařízeními A a B. V případě, kdy komunikaci zahajuje zařízení A, zpráva 1 slouží k zaslání autentizační *výzvy*$_B$ a PD od zařízení A do zařízení B. Zpráva 2 slouží k zaslání veřejné hodnoty $p = s_1 \oplus$ *odpověď*$_B$ (obsahující tajná data s_1 a *odpověď*$_B$) a k zaslání autentizační *výzvy*$_A$ a PD od zařízení B do zařízení A. Zpráva 3 slouží k zaslání veřejné hodnoty $q = s_2 \oplus$ *odpověď*$_A$ (obsahující tajná data s_2 a *odpověď*$_A$) od zařízení A do zařízení B. Struktura zpráv 1, 2 a 3 je následující:

- **Zpráva 1**: $ID_B||ID_A||0x14||výzva_B||PD||h_1$
  $h_1 = H(ID_B||ID_A||0x14||výzva_B||PD)$

- **Zpráva 2**: $ID_A||ID_B||0x15||p = s_1 \oplus odpověď_B||výzva_A||PD||h_2$
  $h_2 = H(ID_A||ID_B||0x15||p||výzva_A||PD)$
- **Zpráva 3**: $ID_B||ID_A||0x16||q = s_2 \oplus odpověď_A||h_3$
  $h_3 = H(ID_B||ID_A||0x16||q)$

Kde ID_A reprezentuje identitu zařízení A a ID_B reprezentuje identitu zařízení B. Numerická hodnota 0x14 značí, že za touto hodnotou bude následovat $výzva_B$ pro fyzicky neklonovatelnou funkci a pomocná data pro korekční kód, jenž jsou implementované v zařízení B. Numerická hodnota 0x15 značí, že za ní bude následovat veřejná hodnota p, $výzva_A$ pro fyzicky neklonovatelnou funkci a pomocná data pro korekční kód, jenž jsou implementované v zařízení A. Hodnota $p = s_1 \oplus odpověď_B$ slouží k zabezpečenému přenosu tajných dat s_1 a $odpovědi_B$. Numerická hodnota 0x16 značí, že za ní bude následovat veřejná hodnota q. Hodnota $q = s_2 \oplus odpověď_A$ slouží k zabezpečenému přenosu tajných dat s_2 a $odpovědi_A$. Hashe h_1, h_2 a h_3 slouží k ověření integrity přenášených dat ve zprávách 1, 2 a 3.

Pokud část tajných dat s_1 bude nabývat hodnot v definovaném rozsahu, mohou být tajná data s_1 použita k částečné autentizaci odesílatele dat. Tajná data s_2 slouží k potvrzení příjmu dat s_1. V tajných datech s_2 je přenášen hash tajných dat s_1, jenž slouží k potvrzení příjmu tajných dat s_1 a k autentizaci odesílatele tajných dat s_2.



Obr. 4.2: Princip protokolu zabezpečeného přenosu dat s potvrzením příjmu dat.

Princip protokolu zabezpečeného přenosu dat s potvrzením příjmu dat v případě, kdy komunikaci zahajuje zařízení A bude následující. Zařízení A odešle zprávu 1, obsahující $výzvu_B$ a PD do zařízení B. Po přijetí zprávy 1 zařízení B vypočítá hash z přijatých dat $IP_B||IP_A||0x14||výzva_B||PD$ a porovná ho s přijatým hashem h_1. Pokud si budou rovny, integrita přenesených dat bude zaručena. Poté

zařízení B porovná přijatou $výzvu_B$ s *výzvami* uloženými v seznamu PV_{BA}. Pokud zde nalezne shodu, zkontroluje, jestli má ve své databázi uloženy PVO_A pro fyzicky neklonovatelnou funkci a PD pro korekční kód, jenž jsou implementované v zařízení A. Pokud ano, zařízení B pomocí implementované fyzicky neklonovatelné funkce z přijaté $výzvy_B$ vypočítá $odpověď_B$ a tu následně s využitím PD a korekčního kódu upraví do správného tvaru. Tato operace je v protokolu značena jako $odpověď_B = KK(PD, FNF(výzva_B))$. Poté zařízení B odešle zařízení A zprávu 2, obsahující veřejnou hodnotu $p = s_1 \oplus odpověď_B$, jenž slouží k zabezpečenému přenosu tajných dat s_1 do zařízení A a dále obsahuje $výzvu_A$ a PD pro zařízení A.

Po přijetí zprávy 2 zařízení A vypočítá hash z přijatých dat $ID_A||ID_B||0x15||p||výzva_A||PD$ a porovná ho s přijatým hashem h_2. Pokud si budou rovny, integrita přenesených dat bude zaručena. Zařízení A poté vypočítá tajnou hodnotu $s_1 = p \oplus odpověď_B$ pomocí přijaté veřejné hodnoty p a ve své databázi uložené $odpovědi_B$, jenž tvoří pár s $výzvou_B$ a PD, jenž zařízení A v předchozím kroku zaslalo do zařízení B. Následně zařízení A porovná přijatou $výzvu_A$ s *výzvami* uloženými v seznamu PV_{AB}. Pokud zde nalezne shodu, tak zařízení A pomocí implementované fyzicky neklonovatelné funkce z přijaté $výzvy_A$ vypočítá $odpověď_A$ a tu následně s využitím přijatých PD a korekčního kódu upraví do správné podoby. Tato operace je v protokolu značena jako $odpověď_A = KK(PD, FNF(výzva_A))$.

Následně zařízení A odešle zařízení B zprávu 3, obsahující veřejnou hodnotu $q = s_2 \oplus odpověď_A$, sloužící k zabezpečenému přenosu tajných dat s_2 do zařízení B. Po přijetí zprávy 3, zařízení B vypočítá hash z přijatých dat $IP_B||IP_A||0x16||q$ a porovná ho s přijatým hashem h_3. Pokud si budou rovny, integrita přenesených dat bude zaručena. Zařízení B poté vypočítá tajnou hodnotu $s_2 = q \oplus odpověď_A$ pomocí přijaté veřejné hodnoty q a ve své databázi uložené $odpovědi_A$, jenž tvoří pár s $výzvou_A$ a PD, jenž zařízení B v předchozím kroku zaslalo do zařízení A. Pokud výsledek operace vytvoří tajnou hodnotu s_2, která bude rovna hashi tajných dat s_1, jenž zařízení B zaslalo v předchozím kroku zařízení A, tak zařízení A přijalo tajná data s_1 korektně.

V tomto protokolu je důležité, aby $odpověď_B$, jenž byla zařízením B využita při tvorbě veřejné hodnoty p a uloženou $odpovědí_B$ v databázi zařízení A byla totožná, aby dešifrování tajné hodnoty s_1 proběhlo korektně. Taktéž je nutné aby $odpověď_A$, jenž byla zařízením A využita při tvorbě veřejné hodnoty q byla totožná s $odpovědí_A$ jenž má zařízení B uloženou ve své databázi, aby dešifrování tajné hodnoty s_2 proběhlo korektně. Za tímto účelem je nutné na výstup fyzicky neklonovatelné funkce implementovat vhodný korekční (protichybový) kód, aby daná fyzicky neklonovatelná funkce generovala na základě konkrétní *výzvy* a PD vždy stejnou *odpověď*.

Důležitým požadavkem pro bezpečný přenos dat mezi zařízeními A a B je, aby dané zařízení použilo k zabezpečenému přenosu dat vždy jinou *odpověď* od své fyzicky neklonovatelné funkce. Tato podmínka je v protokolu zajištěna tím, že zařízení A a B má uloženo seznam povolených *výzev* na které může reagovat. Příchozí *výzvy* pak porovnává s povolenými *výzvami*. Po využití povolené *výzvy* dojde k jejímu odstranění ze seznamu PV. Zařízení A a B nereaguje na *výzvy*, jenž nemá na svém seznamu PV. Zařízení A a B po využití páru *výzva-odpověď* a pomocných dat, vymaže daný pár *výzva-odpověď* a pomocná dat z databáze PVO a PD.

Další podmínkou je, aby přenášená tajná data s_1 měla stejnou velikost jako *odpověď*$_B$ s níž je vykonána operace exkluzivní disjunkce. Taktéž přenášená tajná data s_2 musí mít stejnou velikost jako *odpověď*$_A$ s níž je vykonána operace XOR.

5 NÁVRH OBOUSMĚRNÉHO AUTENTIZAČNÍHO PROTOKOLU SE ZAJIŠTĚNÍM NEPOPIRATELNOSTI

Tato kapitola se věnuje popisu obousměrného autentizačního protokolu se zajištěním nepopiratelnosti. Navržený obousměrný autentizační protokol pro zajištění nepopiratelnosti uskutečněných událostí využívá důvěryhodnou třetí stranu. Důvěryhodná třetí strana může být podle standardu ISO/IEC 13888-2:2010 (ČSN ISO/IEC 13888-2 (369787)) využita pro zajištění nepopiratelnosti pomocí symetrické kryptografie. Tento standard poskytuje popis obecných struktur, jenž mohou být použity pro zajištění nepopiratelnosti služeb, nepopiratelnosti původu a nepopiratelnosti doručení pomocí symetrické kryptografie. Princip navrženého obousměrného autentizačního protokolu zajišťující nepopiratelnost uskutečněných událostí nebyl doposud nikde prezentován.

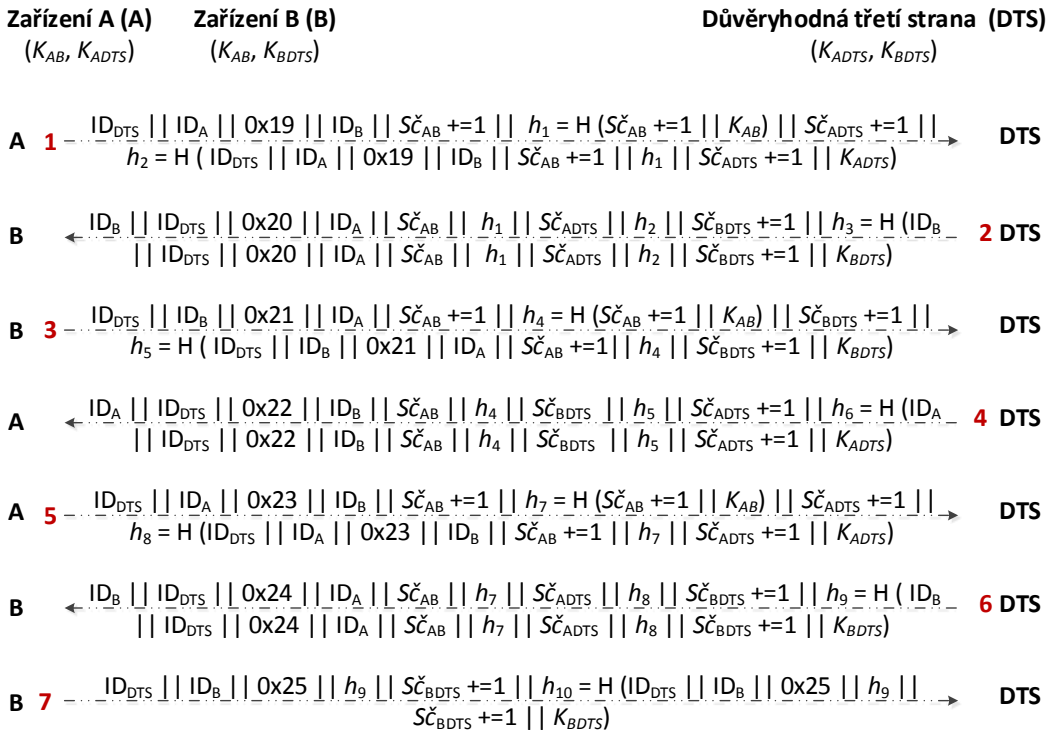
Před aplikací obousměrného autentizačního protokolu se zajištěním nepopiratelnosti je nutné, aby DTS a zařízení A a B vykonali protokol pro výměnu autentizačního klíče (definovaný v plné verzi disertační práce). Po vykonání tohoto protokolu, kdy zařízení A a DTS vlastní autentizační klíč K_{ADTS}, zařízení B a DTS vlastní autentizační klíč K_{BDTS} a zařízení A a B vlastní autentizační klíč K_{AB}, je možné vykonání algoritmu obousměrné autentizace se zajištěním nepopiratelnosti uskutečněných událostí.

Na Obr. 5.1 je vidět princip protokolu obousměrné autentizace se zajištěním nepopiratelnosti uskutečněných událostí, kdy komunikaci zahajuje zařízení A. Pokud by komunikaci zahajovalo zařízení B, postup by byl zrcadlově opačný. V protokolu je využíváno 7 zpráv, jenž jsou vyměňovány mezi DTS a zařízeními A a B. V případě, kdy komunikaci zahajuje zařízení A, zpráva 1 slouží k zaslání požadavku na autentizaci zařízení A k zařízení B do DTS od zařízení A. Zpráva 2 slouží k přeposlání požadavku na autentizaci a důkazního materiálu o zaslání požadavku na autentizaci do zařízení B od DTS. Zpráva 3 slouží k zaslání požadavku na autentizaci zařízení B k zařízení A (slouží i jako potvrzení o autentizaci zařízení A k zařízení B) do DTS od zařízení B. Zpráva 4 slouží k přeposlání požadavku na autentizaci a důkazního materiálu o zaslání požadavku na autentizaci do zařízení A od DTS. Zpráva 5 slouží k zaslání potvrzení o autentizaci zařízení B k zařízení A do DTS od zařízení A. Zpráva 6 slouží k přeposlání potvrzení o autentizaci a důkazního materiálu o zaslání potvrzení o autentizaci do zařízení B od DTS. Zpráva 7 slouží k zaslání potvrzení korektního příjmu zprávy 6 zařízením B. Struktura zpráv 1 – 7 je následující:

- **Zpráva 1**: $ID_{DTS}||ID_A||0x19||ID_B||S\check{c}_{AB}+=1||h_1 = H(S\check{c}_{AB}+=1||K_{AB})||$ $S\check{c}_{ADTS}+=1||h_2 = H(ID_{DTS}||ID_A||0x19||ID_B||S\check{c}_{AB}+=1||h_1||S\check{c}_{ADTS}+=1||K_{ADTS})$
- **Zpráva 2**: $ID_B||ID_{DTS}||0x20||ID_A||S\check{c}_{AB}||h_1||\ S\check{c}_{ADTS}||h_2||S\check{c}_{BDTS}+=1||h_3 = H(ID_B||ID_{DTS}||0x20||ID_A||S\check{c}_{AB}||h_1||\ S\check{c}_{ADTS}||h_2||S\check{c}_{BDTS}+=1||K_{BDTS})$
- **Zpráva 3**: $ID_{DTS}||ID_B||0x21||ID_A||S\check{c}_{AB}+=1||h_4 = H(S\check{c}_{AB}+=1||K_{AB})||$ $S\check{c}_{BDTS}+=1||h_5 = H(ID_{DTS}||ID_B||0x21||ID_A||S\check{c}_{AB}+=1||h_4||S\check{c}_{BDTS}+=1||K_{BDTS})$
- **Zpráva 4**: $ID_A||ID_{DTS}||0x22||ID_B||S\check{c}_{AB}||h_4||S\check{c}_{BDTS}||h_5||\ S\check{c}_{ADTS}+=1||h_6 = H(ID_A||ID_{DTS}||0x22||ID_B||S\check{c}_{AB}||h_4||S\check{c}_{BDTS}||h_5||S\check{c}_{ADTS}+=1||K_{ADTS})$
- **Zpráva 5**: $ID_{DTS}||ID_A||0x23||ID_B||S\check{c}_{AB}+=1||h_7 = H(S\check{c}_{AB}+=1||K_{AB})||$ $S\check{c}_{ADTS}+=1||h_8 = H(ID_{DTS}||ID_A||0x23||ID_B||S\check{c}_{AB}+=1||h_7||S\check{c}_{ADTS}+=1||K_{ADTS})$
- **Zpráva 6**: $ID_B||ID_{DTS}||0x24||ID_A||S\check{c}_{AB}||h_7||\ S\check{c}_{ADTS}||h_8||S\check{c}_{BDTS}+=1||h_9 = H(ID_B||ID_{DTS}||0x24||ID_A||S\check{c}_{AB}||h_7||\ S\check{c}_{ADTS}||h_8||S\check{c}_{BDTS}+=1||K_{BDTS})$
- **Zpráva 7**: $ID_{DTS}||ID_B||0x25||h_9||S\check{c}_{BDTS}+=1||h_{10} = H(ID_{DTS}||ID_B$ $||0x25||h_9||S\check{c}_{BDTS}+=1||K_{BDTS})$

Kde ID_{DTS} reprezentuje identitu DTS, ID_A reprezentuje identitu zařízení A a ID_B reprezentuje identitu zařízení B. Numerické hodnoty 0x19 – 0x25 slouží k rozeznání zpráv 1 – 7 a definují složení dat za nimi následujícími. Numerická hodnota 0x19 značí, že za ní bude následovat identifikátor zařízení, kterému má DTS přeposlat data nacházející se tímto identifikátorem. Numerická hodnota 0x20 značí, že za ní bude identifikátor zařízení od kterého DTS přeposílá čtveřici dat nacházející se za tímto identifikátorem. Sekvenční čísla $S\check{c}_{ADTS}$, $S\check{c}_{BDTS}$ a $S\check{c}_{AB}$ slouží k ochraně proti útoku zopakováním. +=1 u sekvenčních čísel značí zvětšení aktuální hodnoty sekvenčního čísla o číslo jedna. Numerická hodnota 0x21 značí, že za ní bude následovat identifikátor zařízení, které má DTS přeposlat data nacházející se za tímto identifikátorem. Numerická hodnota 0x22 značí, že za ní bude následovat identifikátor zařízení od kterého DTS přeposílá čtveřici dat nacházející se za tímto identifikátorem. Numerická hodnota 0x23 značí, že za ní bude následovat identifikátor zařízení, kterému má DTS přeposlat data nacházející se za tímto identifikátorem. Numerická hodnota 0x24 značí, že za ní bude následovat identifikátor zařízení od kterého DTS přeposílá čtveřici dat nacházející se za tímto identifikátorem. Numerická hodnota 0x25 značí, že ní bude následovat hash potvrzující příjem zprávy 6 zařízením s identifikátorem uvedeným před numerickou hodnotou 0x25. Hash h_1 slouží jako žádost o autentizaci, hash h_2 slouží jako důkaz o zaslání žádosti o autentizaci, hash h_4 jako potvrzení o autentizaci a jako žádost o autentizaci, hash h_5 slouží jako důkaz o zaslání potvrzení o autentizaci a žádosti o autentizaci, hash h_7 slouží jako potvrzení

o autentizaci, hash h_8 slouží jako důkaz o zaslání potvrzení o autentizaci a hash h_9 slouží k potvrzení příjmu zprávy 6. Hashe $h_2, h_3, h_5, h_6, h_8, h_9$ a h_{10} slouží k ověření integrity dat přenášených ve zprávách 1, 2, 3, 4, 5, 6 a 7.



Obr. 5.1: Princip obousměrné autentizace se zajištěním nepopiratelnosti.

Princip protokolu obousměrné autentizace se zajištěním nepopiratelnosti uskutečněných událostí v případě, kdy komunikaci zahajuje zařízení A bude následující (pokud by komunikaci zahajovalo zařízení B, byl by postup zrcadlově opačný).

Zařízení A odešle zprávu 1 do DTS obsahující žádost o autentizaci zařízení A k zařízení B ($h_1 = H(Sč_{AB} += 1||K_{AB})$). Po přijetí zprávy DTS vypočítá hash z přijatých dat $ID_{DTS}||ID_A||0x19||ID_B||Sč_{AB} += 1||h_1||Sč_{ADTS} += 1$ a svého tajného klíče K_{ADTS}, jenž DTS sdílí se zařízením A a porovná ho s přijatým hashem h_2. Pokud si budou rovny, integrita a autentičnost přenesených dat bude zaručena. Poté DTS porovná přijaté sekvenční číslo $Sč_{ADTS} += 1$ zprávy 1 s naposledy využitým sekvenčním číslem $Sč_{ADTS}$ mezi zařízením A a DTS. Pokud přijaté sekvenční číslo $Sč_{ADTS} += 1$ bude větší než naposledy použité sekvenční číslo $Sč_{ADTS}$ mezi zařízením A a DTS, DTS zašle zprávu 2 do zařízení B obsahující přijatou žádost

o autentizaci zařízení A k zařízení B (h_1) a důkaz o zaslání žádosti o autentizaci zařízení A k zařízení B (h_2) a k nim příslušná sekvenční čísla $S\check{c}_{AB}$ a $S\check{c}_{ADTS}$.

Zařízení B po přijetí zprávy 2 vypočítá hash z přijatých dat $ID_B||ID_{DTS}||0x20||ID_A||S\check{c}_{AB}||h_1||S\check{c}_{ADTS}||h_2||S\check{c}_{BDTS}+=1$ a svého tajného klíče K_{BDTS}, jenž zařízení B sdílí s DTS a porovná ho s přijatým hashem h_3. Pokud si budou rovny, integrita a autentičnost přenesených dat bude zaručena. Poté DTS porovná přijaté sekvenční číslo $S\check{c}_{BDTS}+=1$ zprávy 2 s naposledy využitým sekvenčním číslem $S\check{c}_{BDTS}$ mezi zařízením B a DTS. Pokud přijaté sekvenční číslo $S\check{c}_{BDTS}+=1$ bude větší než naposledy použité sekvenční číslo $S\check{c}_{BDTS}$ mezi zařízením B a DTS, zařízení B vypočítá hash z přijatého sekvenčního čísla $S\check{c}_{AB}$ a svého tajného klíče K_{AB}, jenž zařízení B sdílí se zařízením A a porovná ho s přijatým hashem h_1. Pokud si budou rovny a přijaté $S\check{c}_{AB}$ bude větší než naposledy použité sekvenční číslo $S\check{c}_{AB}$ mezi zařízením A a B, zařízení B autentizuje zařízení A. Zařízení B si uloží do své databáze hashe h_1 a h_2 a k nim příslušná sekvenční čísla $S\check{c}_{AB}$ a $S\check{c}_{ADTS}$ pro případ sporu, kdy zařízení A bude tvrdit, že nezaslalo požadavek k autentizaci na zařízení B přes DTS. Zařízení B následně zašle zprávu 3 do DTS obsahující žádost o autentizaci zařízení B k zařízení A ($h_4 = H(S\check{c}_{AB}+=1||K_{AB})$ – slouží i jako potvrzení o autentizaci zařízení A k zařízení B) a důkaz o zaslání žádosti o autentizaci zařízení B k zařízení A (h_5) a k nim příslušná sekvenční čísla $S\check{c}_{AB}+=1$ a $S\check{c}_{BDTS}+=1$.

DTS po přijetí zprávy 3 vypočítá hash z přijatých dat $ID_{DTS}||ID_B||0x21||ID_A||S\check{c}_{AB}+=1||h_4||S\check{c}_{BDTS}+=1$ a svého tajného klíče K_{BDTS}, jenž DTS sdílí se zařízením B a porovná ho s přijatým hashem h_5. Pokud si budou rovny, integrita a autentičnost přenesených dat bude zaručena. Poté DTS porovná přijaté sekvenční číslo $S\check{c}_{BDTS}+=1$ zprávy 3 s naposledy využitým sekvenčním číslem $S\check{c}_{BDTS}$ mezi zařízením B a DTS. Pokud přijaté sekvenční číslo $S\check{c}_{BDTS}+=1$ bude větší než naposledy použité sekvenční číslo $S\check{c}_{BDTS}$ mezi zařízením B a DTS, DTS zašle zprávu 4 do zařízení A obsahující přijatou žádost o autentizaci zařízení B k zařízení A (h_4 – sloužící i jako potvrzení o autentizaci zařízení A k zařízení B) a důkaz o zaslání žádosti o autentizaci zařízení B k zařízení A (h_5) a k nim příslušná sekvenční čísla $S\check{c}_{AB}$ a $S\check{c}_{BDTS}$.

Zařízení A po přijetí zprávy 4 vypočítá hash z přijatých dat $ID_A||ID_{DTS}||0x22||ID_B||S\check{c}_{AB}||h_4||S\check{c}_{BDTS}||h_5||S\check{c}_{ADTS}+=1$ a svého tajného klíče K_{ADTS}, jenž zařízení A sdílí s DTS a porovná ho s přijatým hashem h_6. Pokud si budou rovny, integrita a autentičnost přenesených dat bude zaručena. Poté zařízení A porovná přijaté sekvenční číslo $S\check{c}_{ADTS}+=1$ zprávy 4 s naposledy využitým sekvenčním číslem $S\check{c}_{ADTS}$ mezi zařízením A a DTS. Pokud přijaté sekvenční číslo $S\check{c}_{ADTS}+=1$ bude větší než naposledy použité sekvenční číslo $S\check{c}_{ADTS}$ mezi zařízením A a DTS, zařízení A vypočítá hash z přijatého sekvenčního čísla $S\check{c}_{AB}$ a ze svého tajného klíče K_{AB}, jenž zařízení A sdílí se zařízením B a porovná ho s přijatým hashem h_4. Pokud

si budou rovny a přijaté $S\check{c}_{AB}$ bude větší než naposledy použité sekvenční číslo $S\check{c}_{AB}$ mezi zařízením zařízením A a B, zařízení B potvrzuje, že autentizovalo zařízení A a zařízení B žádá o autentizaci k zařízení A. Zařízení A si uloží do své databáze hashe h_4 a h_5 a k nim příslušná sekvenční čísla $S\check{c}_{AB}$ a $S\check{c}_{BDTS}$ pro případ sporu, kdy zařízení B bude tvrdit, že neautentizovalo zařízení A a nezaslalo požadavek k autentizaci na zařízení A přes DTS. Zařízení A následně zašle zprávu 5 do DTS obsahující potvrzení o autentizaci zařízení B k zařízení A ($h_7 = H(S\check{c}_{AB}+ = 1||K_{AB})$) a důkaz o zaslání potvrzení o autentizaci zařízení B k zařízení A (h_8) a k nim příslušná sekvenční čísla $S\check{c}_{AB}+ = 1$ a $S\check{c}_{ADTS}+ = 1$.

DTS po přijetí zprávy 5 vypočítá hash z přijatých dat $ID_{DTS}||ID_A||0x23||ID_B||S\check{c}_{AB}+ = 1||h_7||S\check{c}_{ADTS}+ = 1$ a svého tajného klíče K_{ADTS}, jenž DTS sdílí se zařízením A a porovná ho s přijatým hashem h_8. Pokud si budou rovny, integrita a autentičnost přenesených dat bude zaručena. Poté DTS porovná přijaté sekvenční číslo $S\check{c}_{ADTS}+ = 1$ zprávy 5 s naposledy využitým sekvenčním číslem $S\check{c}_{ADTS}$ mezi zařízením A. Pokud přijaté sekvenční číslo $S\check{c}_{ADTS}+ = 1$ bude větší než naposledy použité sekvenční číslo $S\check{c}_{ADTS}$ mezi zařízením A a DTS, DTS zašle zprávu 6 do zařízení B obsahující přijaté potvrzení o autentizaci zařízení B k zařízení A (h_7) a důkaz o zaslání potvrzení o autentizaci zařízení B k zařízení A (h_8) a k nim příslušná sekvenční čísla $S\check{c}_{AB}$ a $S\check{c}_{ADTS}$.

Zařízení B po přijetí zprávy 6 vypočítá hash z přijatých dat $ID_B||ID_{DTS}||0x24||ID_A||S\check{c}_{AB}||h_7||S\check{c}_{ADTS}||h_8||S\check{c}_{BDTS}+ = 1$ a svého tajného klíče K_{BDTS}, jenž zařízení B sdílí s DTS a porovná ho s přijatým hashem h_9. Pokud si budou rovny, integrita a autentičnost přenesených dat bude zaručena. Poté zařízení B porovná přijaté sekvenční číslo $S\check{c}_{BDTS}+ = 1$ zprávy 6 s naposledy využitým sekvenčním číslem $S\check{c}_{BDTS}$ mezi zařízením B a DTS. Pokud přijaté sekvenční číslo $S\check{c}_{BDTS}+ = 1$ bude větší než naposledy použité sekvenční číslo $S\check{c}_{BDTS}$ mezi zařízením B a DTS, zařízení B vypočítá hash z přijatého sekvenčního čísla $S\check{c}_{AB}$ a ze svého tajného klíče K_{AB}, jenž zařízení B sdílí se zařízením A a porovná ho s přijatým hashem h_7. Pokud si budou rovny a přijaté $S\check{c}_{AB}$ bude větší než naposledy použité sekvenční číslo $S\check{c}_{AB}$ mezi zařízením zařízením A a B, zařízení A potvrzuje, že autentizovalo zařízení B. Zařízení B si uloží do své databáze hashe h_7 a h_8 a k nim příslušná sekvenční čísla $S\check{c}_{AB}$ a $S\check{c}_{ADTS}$ pro případ sporu, kdy zařízení A bude tvrdit, že neautentizovalo zařízení B. Zařízení B následně zašle zprávu 7 do DTS obsahující hash zprávy 6 (h_9), jenž slouží k potvrzení korektního příjmu zprávy 6 zařízením B.

DTS po přijetí zprávy 7 vypočítá hash z přijatých dat $ID_{DTS}||ID_B||0x25||h_9||S\check{c}_{BDTS}+ = 1$ a svého tajného klíče K_{BDTS}, jenž DTS sdílí se zařízením B a porovná ho s přijatým hashem h_{10}. Pokud si budou rovny a přijaté $S\check{c}_{BDTS}$ bude větší než naposledy použité sekvenční číslo $S\check{c}_{BDTS}$ mezi zařízením B a DTS, zařízení B korektně přijalo zprávu 6. V protokolu obousměrné autentizace se zajištěním nepo-

piratelnosti uskutečněných událostí v případě, kdy komunikaci zahajuje zařízení A, mohou nastat následující tři spory:

1. Zařízení B bude tvrdit, že přijalo požadavek na autentizaci od zařízení A přes DTS, zatímco zařízení A bude tvrdit, že neodeslalo požadavek na autentizaci k zařízení B přes DTS. Pro vyřešení tohoto sporu musí zařízení B zaslat do DTS žádost o autentizaci zařízení A k zařízení B (h_1) a důkaz o zaslání žádosti o autentizaci zařízení A k zařízení B (h_2) a k nim příslušná sekvenční čísla $S\check{c}_{AB}$ a $S\check{c}_{ADTS}$. DTS poté vypočítá hash h'_2 pomocí konstant $ID_{DTS}, ID_A, 0x19$ a ID_B a dále pomocí přijatých hodnot od zařízení B: $S\check{c}_{AB}, h_1, S\check{c}_{ADTS}$ a pomocí svého tajného klíče K_{ADTS}, jenž DTS sdílí se zařízením A. Pokud hash h'_2 bude roven přijatému hashi h_2 od zařízení B, DTS dá zapravdu zařízení B. Pokud by se vypočítaný hash h'_2 nerovnal přijatému hashi h_2, DTS by dalo zapravdu zařízení A.
2. Zařízení A bude tvrdit, že bylo autentizováno zařízením B a že přijalo požadavek na autentizaci od zařízení B přes DTS, zatímco zařízení B bude tvrdit, že neautentizovalo zařízení A a že neodeslalo požadavek na autentizaci k zařízení A přes DTS. Pro vyřešení tohoto sporu musí zařízení A zaslat do DTS žádost o autentizaci zařízení B k zařízení A (h_4 – slouží i jako potvrzení o autentizaci zařízení A zařízením B) a důkaz o zaslání žádosti o autentizaci zařízení B k zařízení A (h_5) a k nim příslušná sekvenční čísla $S\check{c}_{AB}$ a $S\check{c}_{BDTS}$. DTS poté vypočítá hash h'_5 pomocí konstant $ID_{DTS}, ID_B, 0x21$ a ID_A a dále pomocí přijatých hodnot od zařízení A: $S\check{c}_{AB}, h_4, S\check{c}_{BDTS}$ a pomocí svého tajného klíče K_{BDTS}, jenž DTS sdílí se zařízením B. Pokud hash h'_5 bude roven přijatému hashi h_5 od zařízení A, DTS dá zapravdu zařízení A. Pokud by se vypočítaný hash h'_5 nerovnal přijatému hashi h_5, DTS by dalo zapravdu zařízení B.
3. Zařízení B bude tvrdit, že bylo autentizováno zařízením A, zatímco zařízení A bude tvrdit, že neautentizovalo zařízení B. Pro vyřešení tohoto sporu musí zařízení B zaslat do DTS potvrzení o autentizaci zařízení B k zařízení A (h_7) a důkaz o zaslání potvrzení o autentizaci zařízení B k zařízení A (h_8) a k nim příslušná sekvenční čísla $S\check{c}_{AB}$ a $S\check{c}_{ADTS}$. DTS poté vypočítá hash h'_8 pomocí konstant $ID_{DTS}, ID_A, 0x23$ a ID_B a dále pomocí přijatých hodnot od zařízení B: $S\check{c}_{AB}, h_7, S\check{c}_{ADTS}$ a pomocí svého tajného klíče K_{ADTS}, jenž DTS sdílí se zařízením A. Pokud hash h'_8 bude roven přijatému hashi h_8 od zařízení B, DTS dá zapravdu zařízení B. Pokud by se vypočítaný hash h'_8 nerovnal přijatému hashi h_8, DTS by dalo zapravdu zařízení A.

6 ZÁVĚR

Předmětem disertační práce byla autentizace na nízkonákladových zařízeních. Nízkonákladová zařízení většinou představují zařízení, jenž jsou omezená výpočetním výkonem a paměťovým prostorem nebo také napájecím napětím. Na takto omezená zařízení není ve většině případů možné implementovat běžné kryptografické algoritmy z asymetrické kryptografie, jako je např. algoritmus RSA s modulem o velikosti 2048 bitů, ale i ze symetrické kryptografie, jako je např. algoritmus AES s délkou klíče 256 bitů. Z potřeby implementace kryptografie na nízkonákladových zařízeních vzniklo nové odvětví kryptografie, jenž nejčastěji bývá překládáno jako lehká kryptografie (lightweight cryptography). Lehká kryptografie se zaměřuje na implementaci nenáročných kryptografických algoritmů z běžné kryptografie, na optimalizaci kryptografických protokolů z běžné kryptografie tak, aby mohly být implementovány na nízkonákladových zařízeních a na vývoj nových kryptografických algoritmů určených pro implementaci na nízkonákladových zařízeních.

Kapitola 2 se zabývá definicí cílů práce, jenž spočívají v analýze dostupných autentizačních protokolů vhodných pro implementaci na nízkonákladových zařízeních, v návrhu nových autentizačních protokolů vhodných pro implementaci na nízkonákladových zařízeních a v provedení jejich bezpečnostní analýzy.

Kapitola 3 se zabývá popisem jednosměrného autentizačního protokolu se zabezpečeným přenosem dat. Jednosměrný autentizační protokol (popsaný v kapitole 3.1) je unikátní z hlediska jeho nároků a poskytujících kryptografických vlastností. Tento protokol vyžaduje pouze implementaci hashovací funkce a fyzicky neklonovatelné funkce. Protokol kromě robustní autentizace pomocí FNF zajišťuje integritu a neopakovatelnost autentizačních zpráv. Protokol zabezpečeného přenosu dat bez potvrzení příjmu dat (popsaný v kapitole 3.2) je unikátní z hlediska jeho nároků a poskytujících kryptografických vlastností. Tento protokol vyžaduje pouze implementaci hashovacích funkcí, fyzicky neklonovatelné funkce, korekčního kódu a operací exkluzivní disjunkce. Protokol kromě důvěrnosti tajných dat, jenž jsou šifrována pomocí principu dokonalá šifry, zajišťuje integritu a neopakovatelnost šifrovaných zpráv. V kapitole 4 byl popsán obousměrný autentizační protokol se zabezpečeným přenosem dat. Obousměrný autentizační protokol (popsaný v kapitole 4.1) je unikátní z hlediska jeho nároků a poskytujících kryptografických vlastností. Tento protokol vyžaduje pouze implementaci hashovacích funkcí a fyzicky neklonovatelných funkcí. Protokol kromě robustní autentizace pomocí FNF zajišťuje integritu a neopakovatelnost autentizačních zpráv. Protokol zabezpečeného přenosu dat s potvrzením příjmu dat (popsaný v kapitole 4.2) je unikátní z hlediska jeho nároků a poskytujících kryptografických vlastností. Tento protokol vyžaduje pouze implementaci hashovací funkcí, fyzicky neklonovatelné funkcí, korekčních kódů a operací

exkluzivní disjunkce. Protokol kromě šifrovaného přenosu tajných dat zajišťuje integritu a neopakovatelnost šifrovaných zpráv. Tajná informace je šifrována pomocí principu dokonalé šifry. Navržené autentizační protokoly využívající fyzicky neklonovatelné funkce jsou unikátní v jejich nízkých hardwarových nárocích zajišťující silnou neklonovatelnost a jiné žádoucí kryptografické vlastnosti. Nevýhodou je, že před aplikováním protokolů využívající FNF musí být vytvořena databáze párů *výzva-odpověď* a k nim příslušných pomocných dat.

Kapitola 5 se zabývá popisem obousměrného autentizačního protokolu se zajištěním nepopiratelnosti využívající pouze hashovací funkce, sekvenční čísla a důvěryhodnou třetí stranu. Obousměrný autentizační protokol se zajištěním nepopiratelnosti je unikátní z hlediska jeho nároků a poskytujících kryptografických vlastností. Tento protokol vyžaduje pouze implementaci hashovacích funkcí, sekvenčních čísel a začlenění důvěryhodné třetí strany do autentizační komunikace. Protokol kromě obousměrné autentizace zajišťuje integritu a neopakovatelnost autentizačních zpráv, nepopiratelnost odeslání autentizačního požadavku a nepopiratelnost provedení autentizace mezi komunikujícími stranami.

Navržené protokoly je možné využít v Internetu věcí k autentizaci zařízení a dat z nich přicházejících. Navržené protokoly využívající fyzicky neklonovatelné funkce jsou vhodné pro implementace v situacích s omezeným počtem možných autentizací či přenosu tajných dat. Navržený obousměrný autentizační protokol se zajištěním nepopiratelnosti stojí na důvěrnosti tajných autentizačních klíčích a na důvěře komunikujících stran k důvěryhodné třetí straně. Tento protokol je vhodný pro situace, kdy je vyžadováno objektivní vyřešení případných sporů vzniklých při obousměrné autentizaci komunikujících stran.

Navazující práce bude spočívat v implementaci navržených autentizačních protokolů na vhodných nízkonákladových zařízeních a v provedení bezpečnostní analýzy proti útokům pomocí postranních kanálů.

LITERATURA

[1] ČLUPEK, Vlastimil. Strong Unilateral Authentication of Low- cost Devices Involved in Internet of Things in Smart Homes. In *Proceedings of the 22nd Conference STUDENT EEICT 2016*. 2016. s. 589–593. ISBN: 978-80-214-5350-0.

[2] ČLUPEK, Vlastimil a ZEMAN, Václav. Robust Mutual Authentication and Secure Transmission of Information on Low- cost Devices Using Physical Unclonable Functions and Hash Functions. In *TSP 2016. International Conference on Telecommunications and Signal Processing (TSP)*. 2016. s. 100–103. ISBN: 978-1-5090-1287- 9. ISSN: 1805-5435.

A VYBRANÉ PUBLIKACE AUTORA

ČLUPEK, V.; ZEMAN, V. Robust Mutual Authentication and Secure Transmission of Information on Low- cost Devices Using Physical Unclonable Functions and Hash Functions. In *TSP 2016. International Conference on Telecommunications and Signal Processing (TSP)*. 2016. s. 100-103. ISBN: 978-1-5090-1287- 9. ISSN: 1805-5435.

ČLUPEK, V. Strong Unilateral Authentication of Low- cost Devices Involved in Internet of Things in Smart Homes. In *Proceedings of the 22nd Conference STUDENT EEICT 2016*. 2016. s. 589-593. ISBN: 978-80-214-5350- 0.

ČLUPEK, V.; ZEMAN, V. Unilateral Authentication on Low- cost Devices. In *TSP 2015*. 2015. s. 88-92. ISBN: 978-1-4799-8497- 8.

ČLUPEK, V.; FROLKA, J. Autentizace na hardwarově omezených zařízeních. *Elektrorevue - Internetový časopis (http://www.elektrorevue.cz)*, 2015, roč. 17, č. 6, s. 185-192. ISSN: 1213- 1539.

MALINA, L.; ČLUPEK, V.; MARTINÁSEK, Z.; HAJNÝ, J.; OGUCHI, K.; ZEMAN, V. Evaluation of Software- Oriented Block Ciphers on Smartphones. In *Foundations and Practice of Security. Lecture Notes in Computer Science*. Springer International Publishing, 2014. s. 353-368. ISBN: 978-3-319-05301- 1. ISSN: 0302- 9743.

ČLUPEK, V.; MALINA, L.; ZEMAN, V. Secure Digital Archiving in Post- Quantum Era. In *Proceedings of the 38th International Conference on Telecommunication and Signal Processing*. 2014. s. 622-626. ISBN: 978-1-4799-8497- 8.

Curriculum Vitae

Ing. Vlastimil Člupek

Fakulta elektrotechniky a komunikačních technologií
Vysoké učení technické v Brně
Technická 12
616 00 Brno
clupek@phd.feec.vutbr.cz
+420 54114 6944

Profesní zkušenosti

2012 – dosud	Technický pracovník na Ústavu telekomunikací, FEKT, VUT v Brně. Pracující na vývoji bezpečných kryptografických metod pro autentizaci na hardwarově omezených zařízeních. Vedoucí v laboratořích předmětu Vyšší techniky datových přenosů.

Kvalifikace

2012 – dosud	Student doktorského studia na Ústavu telekomunikací, FEKT, VUT v Brně.
2012	Ing. pro obor Telekomunikační a informační technika, VUT v Brně.
2010	Bc. pro obor Teleinformatika, VUT v Brně.

Odborné zaměření

Kryptografická bezpečnost ICT, problematika autentizace na hardwarově omezených zařízeních, bezpečné dlouhodobé archivování elektronických dokumentů.

Vybrané výzkumné projekty

2013 – 2015	TA03010818, TAČR, Využití moderních kryptografických metod pro zabezpečení komunikace v telematických systémech, (spoluřešitel).
2013 – 2015	CZ.1.05/2.1.00/03.0072, Centrum senzorických, informačních a komunikačních systémů (SIX), (student).
2015 – dosud	VI20152018002, Zátěžový tester ICT, (spoluřešitel).

ABSTRAKT

Disertační práce se zabývá kryptografickými protokoly zajišťující zabezpečenou autentizaci komunikujících stran, jenž jsou určeny primárně pro implementaci na nízkonákladových zařízeních využívaných v Internetu věcí. Nízkonákladová zařízení představují výpočetně, paměťově a napěťově omezená zařízení. Práce se zaměřuje především na možnosti využití matematicky nenáročných kryptografických prostředků pro zajištění integrity, bezpečné autentizace a důvěrnosti přenášených dat na nízkonákladových zařízeních. Hlavní cíle práce se zaměřují na návrh nových pokročilých kryptografických protokolů zajišťující integritu přenášených dat, autentizaci, zabezpečený přenos dat mezi dvěma nízkonákladovými zařízeními a autentizaci s nepopiratelností uskutečněných událostí. Práce popisuje návrhy tří autentizačních protokolů, jednoho jednosměrného autentizačního protokolu a dvou obousměrných autentizačních protokolů. Práce také popisuje návrhy dvou protokolů pro zabezpečený přenos dat mezi dvěma zařízeními, jednoho bez potvrzení příjmu dat a jednoho s potvrzením příjmu dat. V práci je dále provedena bezpečnostní analýza a diskuze k navrženým protokolům.

ABSTRACT

The dissertation thesis deals with cryptographic protocols for secure authentication of communicating parties, which are intended primarily for low-cost devices used in Internet of Things. Low-cost devices represent computationally, memory and power constrained devices. The thesis focuses mainly on the possibilities of using mathematically undemanding cryptographic resorces for ensuring integrity of transmitted dat, authenticity of and secured transmission of data on low-cost devices. The main goals of the thesis focus on the design of new advanced cryptographic protocols for ensuring integrity of transmitted data, authenticity, confidentiality of transmitted data between low-cost devices and authenticity with non-repudiation of done events. The thesis describes proposal of three authentication protocols, one unilateral authentication protocol and two mutual authentication protocols. The thesis also describes proposals of two protocols for secured transmission of data between two devices, one protocol without a proof of receipt data and one protocol with proof of receipt data. In this thesis is also performed a security analysis and a discussion to proposed protocols.