STU
SLOVENSKÁ TECHNICKÁ UNIVERZITA V BRATISLAVE

Oponentský posudok na dizertačnú prácu

Názov práce:	**Analýza a optimalizace datové komunikace pro telemetrické systémy v energetice**
Autor:	**Ing. Radek Fujdiak**
Oponent:	**doc. Ing. Miloš Orgoň, PhD.**
	Slovenská technická univerzita v Bratislave, Fakulta elektrotechniky a informatiky,
	Ústav multimediálnych informačných a komunikačných technológií

Aktuálnosť a náročnosť dizertačnej práce

Predložená práca Ing. Radka Fujdiaka je zameraná na výskum v oblasti analýzy a optimalizácie dátovej komunikácie telemetrických systémov z pohľadu informačnej bezpečnosti pre oblasť energetiky. Cieľom práce bolo zvýšenie informačnej bezpečnosti v limitovaných zariadeniach (z hľadiska napájania) a poskytnutie všetkých potrebných služieb informačnej bezpečnosti. Téma práce je veľmi aktuálna a zodpovedá študijnému odboru Teleinformatika aj súčasným trendom technického vývoja - hlavne z pohľadu novo prichádzajúcich inteligentných sietí, tzv. smart meteringu a ďalších progresívnych odvetví v tejto oblasti, kde je bezpečnosť jedným z kľúčových faktorov.

Čo sa týka náročnosti práce možno hodnotiť predloženú dizertačnú prácu za veľmi náročnú. Dizertant uskutočnil veľmi podrobnú analýzu dnešných možností zabezpečenia, ktorej výsledkom bol ucelený celkový prehľad nedostatkov dnešných progresívnych technologií v danej oblasti. Ďalej uskutočnil kritickú rešerš literatúry, ktorá prináša aj vlastné poznatky, dôležité pre návrh bezpečnostných systémov a prepojil ju s vlastnými experimentálnymi meraniami s využitím technológií a algoritmov, ktoré priniesli ďalšie dôležité znalosti potrebné na vytvorenie bezpečného, komplexného a efektívneho kryptosystému. Na základe získaných poznatkov dizertant navrhol model komunikácie v inteligentných sieťach, ktorý bol publikovaný v renomovaných časopisoch a konferenciách a následne vytvoril vlastný model hybridného kryptosystému, ktorý umožňuje komplexne riešiť problematiku informačnej bezpečnosti v inteligentných sieťach v energetike. Tento model bol taktiež prezentovaný v dvoch impaktovaných časopisoch a v rade zborníkov mezinárodných konferencií. Dizertant tiež vytvoril dva generátory náhodných čísel, jeden z nich bol založený na známom jave dvoch oscilátorov a druhý celkom nový – vlastný, založený na kvantizačnom šume. Ďalej vytvoril modul pre autentizáciu a šifrovanie a modul pre dohodu symetrického tajného kľúča. Za veľmi hodnotnú časť možno považovať aj výskum a testovanie rôznych eliptických kriviek, kde v rámci tejto časti sa dizertant zameral na parametrizáciu eliptických kriviek a efektivny výpočet bodov. Vývoj ukončil úspešnou implementáciou vyše 60-tich eliptických kriviek rôznych štandardov, ktoré možno považovať za jedinečné. Výsledky boli taktiež publikované na viacerých konferenciách a v dvoch impaktovaných časopisoch.

Orientácia dizertanta v problematike, štúdium literatúry

Dizertant v dizertačnej práci uskutočnil komplexnú analýzu možností zabezpečenia, ktorej výsledkom bol ucelený celkový prehľad nedostatkov dnešných progresívnych technologií v danej oblasti. Dizertant využil pri vypracovávaní práce celkom 344 citačných prameňov, prevažne z uznávaných vedeckých časopisov. Tento počet je nadpriemerne veľký a je dokladom toho, že dizertant počas doktorantúry nadobudol hlboké vedomosti z danej problematiky. Vlastná práca má 159 strán vrátane piatich príloh, zoznamu použitých symbolov a skratiek, literatúry a pod. Ing. Radek Fujdiak počas štúdia publikoval 41 článkov, z toho 7 v impaktovaných časopisoch a 22 na konferenciách indexovaných vo WoS či Scopus. Tieto práce sú úzko spojené s tématikou práce. Na základe toho je možné konštatovať, že publikačná aktivita dizertanta bola viac ako dostatočne splnená a zároveň poukazuje aj na hlboké znalosti v riešenej problematike.

Metodický prístup k riešeniu problematiky

Dizertant pri riešení úloh stanovených v cieľoch dizertačnej práce postupoval metodicky správne, po uskutočnení komplexnej analýzy možností zabezpečenia sietí využil syntézu získaných poznatkov na vytvorenie bezpečného, komplexného a efektívneho kryptosystému určeného na použitie v elektroenergetike.

Formulácia cieľov práce a splnenie cieľov práce

Po dôkladnom prečítaní dizertačnej práce môžem konštatovať, že ciele, ktoré boli v práci stanovené (2. kapitola), boli splnené a výsledky zodpovedajú charakteru dizertačnej práce. Dizertant najprv uskutočnil rozsiahlu technologickú aj legislatívnu analýzu, na ktorú nadväzuje so svojím kritickým pohľadom na dnešný stav riešenia problematiky. Ďalej pokračoval vlastným návrhom riešenia bezpečnosti sietí, ktorý vychádzal z experimentálnych meraní, validácie a ďalších vedeckých metód overovania a optimalizácie. Ciele boli stanovené zrozumiteľne, reálne a mali vedecký potenciál zodpovedajúci úrovni práce PhD. Dovolím si podotknúť, že aj keď uskutočnená analýza sa v tomto type prác nepovažuje za prínos, predsa len dizertantom uskutočnená analýza je veľmi cenná, pretože je komplexná, veľmi fundovaná a prispela značnou mierou k veľmi kvalitným výsledkom dizertačnej práce. Stanovené cíle práce považujem za splnené a výsledky za dostatočne overené.

Rozsah a úroveň dosiahnutých výsledkov

Za vedecké a originálne prínosy dizertanta je možné považovať dosiahnuté výsledky prezentované v kapitole 4 (návrh vlastného riešenia hybridného kryptosystému) a v kapitole 5 (vývoj a realizácia kryptosystému so zreteľom na minimalizáciu energie, potrebnej na napájanie a optimalizácia jeho dielčich častí). Za prínos je možné považovať aj vytvorenie dvoch vlastných softvérových produktov – knižnice potrebnej na generovanie náhodných čísiel a knižnice potrebnej na prácu s rôznymi eliptickými krivkami aj s veľkými číslami). Za významné výsledky možno považovať aj výsledky, ktoré dosiahol dizertant navrhnutím metody výberu eliptických kriviek, čím dosiahol omnoho jednoduchší spôsob a rýchlejší výpočet. Táto metóda sa javí ako veľmi komplexná metóda upravujúca štruktúry kryptografických algoritmov, ktorá umožňuje poskytnúť dostatočne veľké krivky (krivky s veľkosťou 256 b) na využitie spoločne so symetrickými algoritmami.

Použiteľnosť výsledkov v praxi

Výsledky dosiahnuté v predmetnej dizertačnej práci považujem veľmi cenné pre prax, hlavne pri nasadzovaní eliptických kriviek za účelom zvýšenia stupňa bezpečnosti nielen v energetike, ale aj v iných oblastiach ich nasadenia.

Prehľadnosť a štruktúra dizertačnej práce

Dizertačná práca má prehľadnú logickú štruktúru členenia textu na jednotlivé kapitoly a podkapitoly, tak ako sa to vyžaduje v tomto type prác. Text dizertačnej práce je členený do siedmych logicky nadväzujúcich kapitol: Úvod; Oblast zájmu a motivace práce; Cíle dizertace a metodiky; Analýza současného stavu problematiky; Návrh vlastního hybridního kryptosystému; Vývoj, verifikace a optimalizace navrženého kryptosystému; a Závěr.

Formálna a štylistická úroveň práce

Formálnu a štylistickú úroveň práce považujem za veľmi dobrú. Grafická úroveň je tiež na veľmi dobrej úrovni, text obsahuje zaužívané skratky a aj odkazy na literatúru. Práca je písaná zrozumiteľne a prehľadne bez významných typografických či štylistických chýb.

Celkové hodnotenie dizertačnej práce

Dizertačnú prácu, ktorú predložil Ing. Radek Fujdiak, považujem za výborne spracovanú vedeckú prácu so splnenými cieľmi, ktoré boli pre túto prácu stanovené. Posudzovaná práca spĺňa kritériá uvedené v Zákone o vysokých školách a zodpovedá obecne uznávaným požiadavkám na udelenie akademického titulu PhD. Dizertačná práca prináša nové vedecké poznatky, ktoré prispievajú k rozvoju vedy a sú využiteľné aj v praxi. Z týchto dôvodov **odporúčam dizertačnú prácu k obhajobe a po úspešnej obhajobe odporúčam udelenie titulu PhD.**

Otázky a pripomienky pre dizertanta

Pripomienky:

Na str. 3 je prvý obrázok označený Obr. 1 a ďalší na str. 5 už Obr. 1.1 **Prečo?**

Na str. 33 je nedokončená veta: „V kryptografických hašovacích funkcí musí být deterministická“. **Čo musí byť deterministické?**

Na str. 39 je uvedený nesprávny vzťah vo vete: „Asymetrické algoritmy potřebují v rámci systému pouze $2n$ klíčů, oproti symetrickým algoritmům, které potřebují $n(n-1)/20$ klíčů“. Správny vzťah je autorom napísaný na str. 34. [$n(n-1)/2$]

Na str. 59 je nezrozumiteľná veta: „ 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).“ **Ako má znieť správne?**

Na str. 67 nie je z obrázka 4.11 jasné, že inicializácia CTR je hnedá a a inicializácia ECB je zelená.

Vysvetlite tvrdenie pod obr. 5.16 na str. 92: „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“.

Na str. 94 za označením krivky $\mathbb{F}_2^{233}$ **niečo tam chýba?**

Na str. 142 v Prílohe C je tabuľka, ktorá má netradične pomenovanie stĺpcov v poslednom riadku - nedá sa zistiť, pokiaľ sú to minuty, resp. odkiaľ sú to sekundy. Mimochodom, minúty majú jednotku [min].

Otázky:

1. V rámci práce sú overené jednotlivé dielčie časti kryptosystému, bol taktiež overený kryptosystém ako celok?
2. Prečo nebola ešte využitá v súčasnosti často popisovaná krivka Curve25519, resp. iné ďalšie neštandardné riešenia ECC?

V Bratislave dňa 7.8.2017

.....
doc. Ing. Miloš Orgoň, PhD.