SLOVENSKÁ TECHNICKÁ
UNIVERZITA V BRATISLAVE
FAKULTA ELEKTROTECHNIKY
A INFORMATIKY

Marek Repka

Autoreferát dizertačnej práce

VYLEPŠENIE CPA ÚTOKU NA (EC)DSA A ANALÝZA DOBY VÝPOČTU MCELIECE PKC

na získanie akademickej hodnosti doktor (philosophiae doctor, PhD.)

v doktorandskom študijnom programe: **Aplikovaná informatika**

v študijnom odbore 9.2.9 Aplikovaná informatika

Miesto a dátum: Bratislava, 30.09.2015

SLOVENSKÁ TECHNICKÁ UNIVERZITA
V BRATISLAVE
FAKULTA ELEKTROTECHNIKY A INFORMATIKY

Marek Repka

Autoreferát dizertačnej práce

VYLEPŠENIE CPA ÚTOKU NA (EC)DSA A ANALÝZA DOBY VÝPOČTU MCELIECE PKC

na získanie akademickej hodnosti doktor (philosophiae doctor, PhD.)

v doktorandskom študijnom programe:
Aplikovaná informatika

Miesto a dátum: Bratislava, 30.09.2015

Dizertačná práca bola vypracovaná v externej forme doktorandského štúdia

Na Ústave Informatiky a Matematiky, Fakulta Elektroniky a Informatiky,
Slovenská Technická Univerzita v Bratislave

Predkladateľ: Marek Repka

Školiteľ: prof. RNDr. Otokar Grošek, PhD.

Oponenti: prof. Ing. Viktor Fischer, PhD.,
Hubert Curien Laboratory, Jean Monnet University,
18, rue Pr. Lauras, 42000 Saint-Etienne, FR.

doc. RNDr. Ladislav Satko, PhD.,
Púpavova 11, 841 04 Bratislava, SR.

Autoreferát bol rozoslaný: 30.09.2015

Na Ústave Informatiky a Matematiky, Fakulta Elektrotechniky a Informatiky,
Ilkovičová 3, 812 19 Bratislava.

prof. Dr. Ing. Miloš Oravec,
Dekan Fakulty Elektrotechniky
a Informatiky STU

Contents

1 Úvod **1**

2 Ciele **3**

3 Metodológia **4**

3.1 Analyzované kryptosystémy 4

3.2 Vykonané analýzy 5

3.3 Merania 6

4 Výsledky **9**

4.1 Vylepšenie CPA útoku na (EC)DSA 9

4.2 Analýza doby výpočtu s vnášaním chýb McEliece PKC 12

4.3 p-ta odmocnina v rozšírených konečných poliach charakteristiky p 13

5 Zoznam príspevkov autora **15**

5.1 Zoznam príspevkov kategórie A 15

5.2 Zoznam príspevkov kategórie B 16

5.3 Zoznam prezentácií na konferenciach 17

Referencie **19**

Kapitola 1

Úvod

Postranné kanály sú tu tak dlho ako kryptografia, no formálne prvá práca zaoberajúca sa postrannými kanálmi bola publikovaná v roku 1996 [18]. Pokrok za posledné desaťročie v tejto oblasti je nesmierny. Niet divu, veď útoky postrannými kanálmi sú jedinou možnosť ako zlomiť dnešnú i budúcu kryptografiu. Táto práca sa zaoberá útokom korelačnou analýzou spotreby na DSA a ECDSA a implementáciou pôvodného originálneho McEliece kryptosystému s verejným kľúčom (McEliece PKC) obsahujúc nástroj na meranie úniku informácie postranným kanálom. V práci je CPA útok na DSA a ECDSA vylepšený a je tu tiež diskutované účinné a efektívne protiopatrenie voči tomuto útoku. V práci je ďalej prezentovaná implementácia originálneho McEliece PKC s nástrojom na meranie zvolených typov únikov. Možnosti tohto nástroja sú v práci aj demonštrované, ako aj analýza doby výpočtu v spojení s vnášaním chýb, ktorá je tiež vylepšená. Návrh efektívnej metódy pre výpočet p-tej odmocniny v konečných poliach charakteristiky p je uvedený ako posledný výsledok. Práca uvádza súčasný stav problematiky, metodológiu, ktorá mapuje analyzované kryptografické implementácie, meracie nástroje, a metódy útokov, ktoré boli použité na dosiahnutie požadovaných výsledkov.

Tabuľka 1.1: Zoznam bežne zneužívaných postranných kanálov

Postranné kanály	**Referencia**
Spotreba	[17], [3]
Elektromagnetické vyžarovanie	[22], [5]
Softvérovo definované rádio	[10]
Doba výpočtu	[18], [4]
Zvuk	[9]
Emisia fotónov	[15]
Neštandardné správanie	[1],[41]
Zbytkové dáta	[12]
Sociálne inžinierstvo	[11]

Útoky postrannými kanálmi môžeme rozdeliť vzhľadom na možnosti útočníkov manipulovať so zariadením na neinvzívne, semi-invazívne a invazívne (dochádza k úplnému poškodeniu), podľa možnosti manipulácie s výpočtom na aktívne a pasívne, a tiež podľa použitej analýzy na jednoduché, univariačné a multivariačné bez a so šablónami.

Protiopatrenia majú za úlohu učiniť dátovo a operačne závislé prejavy nezávislými. K tomuto účelu sa používajú techniky ukrývania, ako generátory šumu, náhodné vykonávanie prázdnych operácií alebo operácii spracúvajúcich náhodné dáta, či dual-rail princíp logiky, a tiež techniky maskovania, kedy sa dáta maskujú nezávislými náhodne generovanými hodnotami pred každým spracovaním, maskované dáta sa spracujú, a výsledok je na výstupe demaskovaný.

Kapitola 2

Ciele

Jedným z hlavných cieľov bolo vylepšiť CPA analýzu celočíselnej násobičky a vylepšiť tak útok na (EC)DSA. Za týmto účelom museli byť splnené čiastkové ciele ako implementácia nástroja na vykonanie analýz CPA a vykonanie niekoľkých CPA útokov na celočíselné násobenie. Simulované útoky nie sú presné, preto popri hľadaní vylepšenia CPA útoku má byť cieľom aj eliminácia chyby simulovaných CPA útokov.

Ďalším hlavným cieľom bolo vykonať analýzu doby výpočtu s vnášaním chýb vybraných krokov McEliece PKC. Za týmto účelom bolo nutné implementovať originálny McEliece PKC, ktorý by umožňoval voliť všetky relevantné parametre kryptosystému, produkoval testovacie vektory pre všetky potrebné medzivýsledky, a tiež by obsahoval nástroj na merania postrannej informácie.

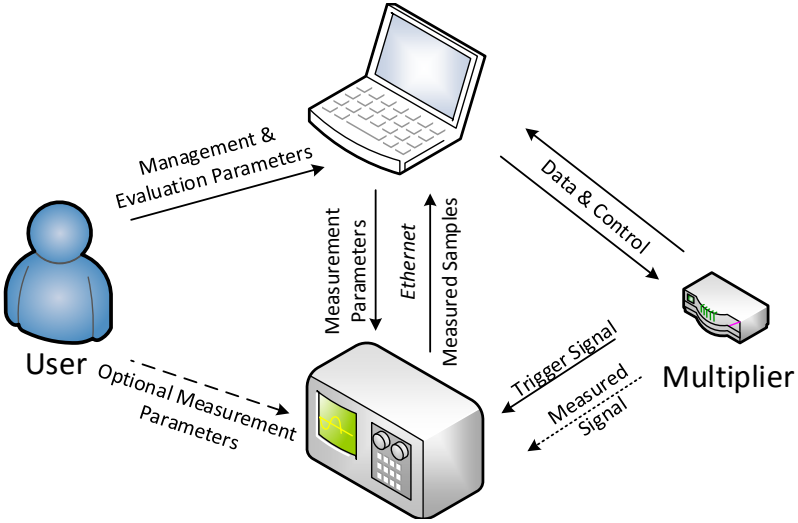
Kapitola 3

Metodológia

Počas riešenia dizertačnej práce boli analyzované symetrické ako aj asymetrické kryptosystémy a to hlavne AES, ECDSA a McEliece PKC.

3.1 Analyzované kryptosystémy

AES bol implementovaný v dvoch analyzovaných laboratórnych kryptografických zariadeniach. V μkontroleri PIC18F2520 a v FPGA ACTEL FUSION M7AFS600, ktoré sa líšili technológiou ako aj prípadmi použitia. V μkontroler PIC18F2520 bol implementovaný AES-128 so sekvenčným spracovávaním stavu AES po 8 bitoch, pretože je to 8-bitový μkontroler. Útok na tento μkontroler s AES-128 bol prezentovaný v (Repka [25]). V FPGA ACTEL FUSION M7AFS600 bol implementovaný AES-128 so 128-bitovou dátovou cestou. Celý stav AES-128 bol spracovávaný paralelne. ECDSA bol analyzovaný v FPGA ALTERA Cyclone III, presnejšie bola implementovaná len časť ECDSA, ktorá bola podrobená útokom. Bola to 16-bitová celočíselná násobička. McEliece PKC s nástrojom na meranie rôznych únikov postrannej informácie bol implementovaný (Repka [27]) softvérovo na operačnom systéme Linux a Windows v jazyku C++ za použitia knižnice NTL, pričom expe-



Obr. 3.1: Topológia meraní a útokov

rimenty boli realizované na 64-bitovej platforme. V práci (Varchola, Drutarovský, and Repka [40]) sa tiež zaoberáme skutočne náhodnými generátormi.

3.2 Vykonané analýzy

Uvedené kryptografické zariadenia implementácie AES a ECDSA boli podrobené skúmaniu útokov korelačnou analýzou spotreby a McEliece PKC bol podrobený skúmaniu útokov analýzou doby výpočtu v spojení s vnášaním chýb do výpočtu. Na vykonanie analýz boli vyvinuté aplikácie v programovacom jazyku C++ na meranie elektrickej spotreby, elektromagnetického vyžarovania a meranie doby výpočtu. Taktiež boli vyvinuté aplikácie na vykonávania samotných útokov v C++ a na vykonanie analýz boli vyvinuté aplikácie v C++, MATLAB a R. Aplikácie boli vyvinuté s podporou viac jadrových procesorov, čo zrýchlilo niekoľko násobne realizované výpočty. K záveru prace bola použitá aj CUDA a výpočty boli tak realizované na grafických kartách. Na Obr. 3.1 je uvedená topológia útokov a analýz.

3.3 Merania

Pri zrealizovaných analýzach a útokoch boli použité tri rôzne meracie zariadenia pre rôzne meracie body. Bol použitý osciloskop LeCroy WavePro 7200A s 8-bitovým A/D prevodníkom s 2GHz šírkou pásma a 20GS/s vzorkovaciu frekvenciou, ktorý bol použitý na meranie spotreby na zemi μkontrolera PIC18F2520 pomocou pasívnej napäťovej sondy. Druhým meracím zariadeným bol osciloskop LeCroy WavePro 740Zi s 8-bitovým A/D prevodníkom, 4GHz šírkou pásma a 40GS/s vzorkovaciu frekvenciou, ktorý bol použitý na meranie spotreby FPGA ACTEL FUSION M7AFS600 na rezistore umiestnenom na napájacej vetve jadra FPGA pomocou aktívnej diferenciálnej napäťovej sondy, a tiež bodovou pasívnou elektromagnetickou sondou. Tretie meracie zariadenie, osciloskop AGILENT INFINIIUM DSO9404A s 8-bit A/D prevodníkom, 4GHz šírkou pásma a 20GS/s vzorkovacou frekvenciou, bolo použité na meranie spotreby na kondenzátore na napájacej vetve jadra FPGA ALTERA Cyclone III pomocou koaxiálneho kábla. Pri meraniach bol použitý sekvenčný mód zaznamenávania vzoriek, vďaka čomu boli merania veľmi rýchle. Napríklad meranie 1M priebehov spotreby trvá 65 s, pričom jeden priebeh spotreby obsahuje 2000 vzoriek (50 ns).

Útočiť na registre v programovateľnej logike FPGA (ďalej len „registre“) je jednoduchšie (hlavne čo sa týka ACTEL), ako útok na vstavané pamäte, ktoré tvoria súčasť RAM FPGA, tzv. embedded memory (ďalej len „RAM“). Táto skutočnosť bola prezentovaná na FPGA rodiny FUSION M7AFS600 od firmy ACTEL, kde bol implementovaný AES S-box. V tomto FPGA sú pamäte RAM smart pamäťami implementovanými pri jadre FPGA. Tieto pamäte sú napevno dané, ich logika sa neprogramuje, je možné len do nich zapisovať, alebo z nich čítať. V prípade registra tomu tak nie je. Registre sú v prípade ACTEL FUSION M7AFS600 tvorené pomocou tzv. „VersaTile“ buniek, prostredníctvom ktorých je možné vytvoriť štandardné logické elementy, ako sú napríklad OR, NAND, XOR, multiplexery, registre a latche. Princíp programovania je založený na prepínačoch, ktoré sú realizované flash pamäťovými bunkami. Prostredníctvom týchto prepínačov je možné zvoliť aký ele-

ment má daný VersaTile implementovať. Technológia s prepínačmi tvorenými flash pamäťovými bunkami sa nazýva nevolatilna, pretože po odpojení napájania sa nestratí konfigurácia FPGA. Zneužiteľná spotreba teda závisí od zložitosti hardvéru, resp. dĺžky spojov a elementov umiestnených na týchto spojoch, cez ktoré sa musí vstupný signál pretransformovať, aby sa stal signálom výstupným. Zabudovaná RAM pamäť je menšia, a teda na realizáciu svojej funkcie spotrebuje menej elektrickej energie ako register v logike, ktorý je väčší, súčasťou programovateľných VersaTiles. Práve preto je vo všeobecnosti ťažšie zaútočiť na ASIC, než na FPGA, pretože ASIC je jednoúčelový a optimalizovaný na jeho jednoúčelovú funkciu.

Útok na μkontroler alebo procesor je zväčša jednoduchší, než na FPGA. Dôvodom je, že procesory majú rovnomernú zbernicu, po ktorej dáta prúdia sem a tam. Táto zbernica je symetrická a je konštante široká. Napríklad μkontroler PIC18F2520, ktorý bol podrobený útokom, má 8-bitov širokú zbernicu, a teda vie spracovávať 8-bitové slová v jednom takte. Ďalej môže byť šírka zbernice napríklad 16, 32, alebo 64 bitov. Pričom platí, že čím širšia je zbernica, tým je útok zložitejší, pretože, buď je SNR pre útok menej priaznivé, alebo je počet hypotéz po zrealizovanom útoku vyšší. Keďže sú zbernice symetrické, je možné spotrebu a vyžarovanie modelovať jednoduchšie, napr. HW modelom spotreby. Naopak pri FPGA sú zbernice nesymetrické, nie sú rovnako dlhé, a nie je na každom vodiči rovnaký počet logických elementov. Dokonca pri opätovnej konfigurácii FPGA rovnakou funkciou, je funkcia inak implementovaná, keďže syntéza a spôsob smerovania (rooting) nie sú deterministické. Toto spôsobuje, že HW model spotreby je v prípade FPGA omnoho menej efektívny než HD model spotreby. Tento fakt bol potvrdení pri porovnaní útoku na AES-128 v 8-bitovom μkontroléri v (Repka [25]), kde bol spracovávaný stav jedného kola sekvenčne S-box po S-boxe, narozdiel od FPGA v (Repka, Gaspar, and Fischer [30]), kde bolo implementované spracovávanie celého stavu paralelne a teda všetkých 16 S-boxov súčasne. V práci k dizertačnej skúške ďalej bolo ukázané, že počet hypotéz, závisí od architektúry kryptografického algoritmu. Kryptografický algoritmus môže byť implementovaný rôznym usporiadaním funkčných blokov a registrov. Práve preto je možné učiniť útok postranným

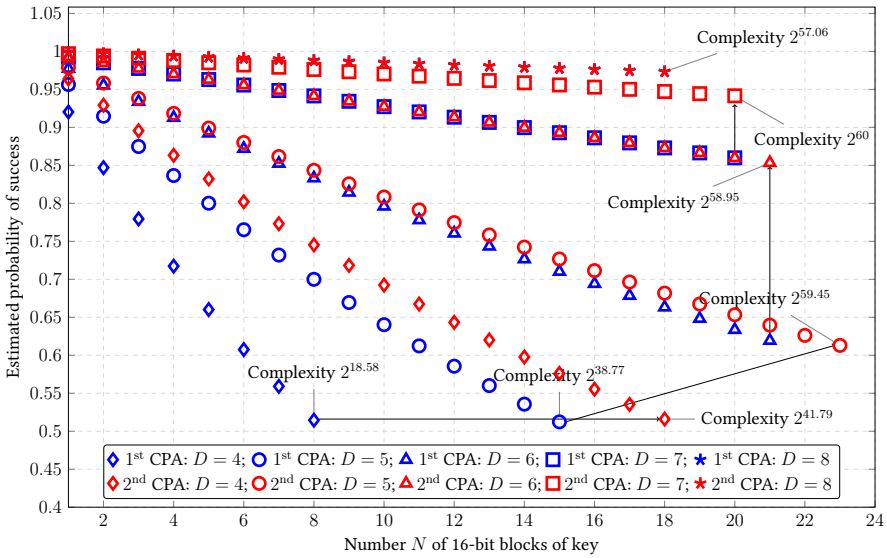
kanálom zložitejším a niekdy aj nemožným, ak sa tieto funkčné bloky a registre usporiadajú s ohľadom na možnosti zostrojovania hypotéz. Takéto protiopatrenie zväčša nevyžaduje žiadne ďalšie zdroje a tak môže byť takéto protiopatrenie klasifikované ako „cost-efficient“, dokonca niekedy aj „zero-cost“ protiopatrenie. Takéto protiopatrenie bolo prezentované na rôznych možnostiach RTL architektúry šifry AES-128 v (Repka et al. [35]) a v (Repka [23]). Na úrovni architektúry bol tento typ protiopatrení využitý aj pri návrhu kryptoprocesora v (Gaspar et al. [8]), ktorý vďaka tomuto prístupu získal prirodzenú odolnosť voči niektorým typom postranných útkov, ako FIA, CPA, CEMA, na určitej úrovni. Využilo sa usporiadanie funkčných blokov a návrh multiplexovania tak, aby niektoré útoky neboli vôbec možné, a iné zasa viac zložité. K týmto protiopatreniam môžeme zaradiť aj návrh hierarchie manažmentu šifrovacích kľúčov a nastavenie počtu použití kľúčov na rôznych úrovniach, pretože univariačné a multivariačné útoky z rodiny DPA a CPA potrebujú, aby sa rovnaký kľúč použil niekoľko krát. Chvíľka pozornosti bola venovaná aj boolovskému maskovaniu S-boxu, ktorého aplikovanie musí byť tiež zvážené na úrovni algoritmu, architektúry a implementácie, s ohľadom na možnosti zostrojovania hypotéz, pretože pri nesprávnom alebo nedostatočnom maskovaní nie je citlivý medzivýsledok zamaskovaný dostatočne, alebo je zamaskovaný na jednom mieste, avšak na iných miestach zamaskovaný nemusí byť vôbec. Pri správnom prístupe maskovania má byť maskovanie aplikované hneď na vstupe ešte pred prvou registráciou v obvode a nová nezávislá maska má byť aplikovaná pred každým ďalším spracovávaním alebo registrovaním. Výsledok má byť demaskovaný až pri výstupe z obvodu po čítaní výsledku z registra. Maska má byť nezávislá nie len naprieč časovej osi tak, ako sa dáta spracúvajú, ale aj naprieč šírky dát, napríklad ak sa dáta delia na menšie bloky, ktoré sú spracovávané samostatne inými alebo rovnakými funkciami.

Kapitola 4

Výsledky

4.1 Vylepšenie CPA útoku na (EC)DSA

Medzi hlavné výsledky dizertačnej práce patrí hlavne analýza vybraných útokov na asymetrickú kryptografiu. Skúmanie bolo upriamené na elektronický podpis ECDSA, ktorý je dnes veľmi využívaný. Doposiaľ bolo publikovaných veľa útokov postrannými kanálmi na eliptické krivky a tiež adekvátne protiopatrenia na eliminovanie publikovaných útokov. Pri útoku na ECDSA bolo ukázané, že nie len samotné operácie na eliptických krivkách môžu byť zraniteľné, a teda, že nestačí aplikovať protiopatrenia len na ne, ale že aj operácie ako celočíselné násobenie môžu poskytnúť únik o privátnom kľúči. Toto platí hlavne pri podpisoch z rodiny DSA, pretože architektúra algoritmov týchto podpisov používa privátny kľúč až pri konci algoritmu ako jeden z operandov celočíselného násobenia, kde druhý operand tohto násobenia je známy, je časťou podpisu. Vďaka tomu sú útoky typu DPA, CPA, a CEMA účinnými. Keďže tieto podpisy sú dnes zväčša implementované na smart kartách, alebo iných zariadeniach využívajúce procesory, ktoré obsahujú 8, 16, alebo 32 bitové celočíselné násobičky, tieto útoky radikálne zužujú množinu možných privátnych kľúčov. V prácach (Repka, Tomeček, and Varchola [31]), (Re-



Obr. 4.1: Odhad zložitosti a úspešnosti útoku po 1. a 2. CPA.

pka and Varchola [32]), (Repka, Varchola, and Drutarovsky [33]), bol vyšetrovaný tento aspekt. Úspešnosť útoku s reálne nameranými dátami dosahuje vyšších hodnôt, ako úspešnosť útoku so simulovanými vzorkami. Preto malo prínos uvažovať chybu odhadu zložitosti útoku (reprezentovanú počtom zostávajúcich hypotéz po útoku) a úspešnosti útoku (pravdepodobnosti, že medzi tými zostávajúcimi hypotézami je tá správna). V rámci tejto úvahy boli vysvetlené chyby prvého a druhého druhu, ako aj bola zadefinovaná relevantná chyba z pohľadu analýzy úrovne zraniteľnosti kryptosystému. Významným prínosom bolo zlepšenie úspešnosti v oboch prípadoch, v prípade nameraných vzoriek, ako aj v prípade simulovaných vzoriek. Boli aplikované v sérii dva CPA útoky s HD modelom spotreby. Prvý CPA útok zoradil všetky možné hypotézy o bloku kľúča. V danom prípade bola použitá 16-bitová násobička v ALTERA FPGA. Za účelom dosiahnutia čo najpriaznivejšieho SNR pre útok, bol použitý HD model spotreby popisujúci celú 32-bitovú šírku výsledku násobenia. Z predošlých experimentov bolo zistené, že ak sa zoberie pr-

Tabuľka 4.1: Porovnanie úspešnosti a zložitosti po 1. a 2. CPA. Maximálna zložitosť je ohraničená 2^{60}. Pre detailnejšie porovnanie úspešnosti a zložitosti po 1. a 2. CPA pozri Obr. 4.1.

Veľkosť kľúča [bity]	Po 1. CPA		Po 2. CPA	
	Pravdepodobnosť	Zložitosť	Pravdepodobnosť	Zložitosť
368	NA	NA	0.613	$2^{59.45}$
352	NA	NA	0.626	$2^{56.89}$
336	0.619	$2^{58.95}$	0.853	$2^{56.95}$
320	0.856	2^{60}	0.941	2^{60}
304	0.866	2^{57}	0.944	2^{57}
288	0.973	$2^{57.06}$	0.973	$2^{57.06}$

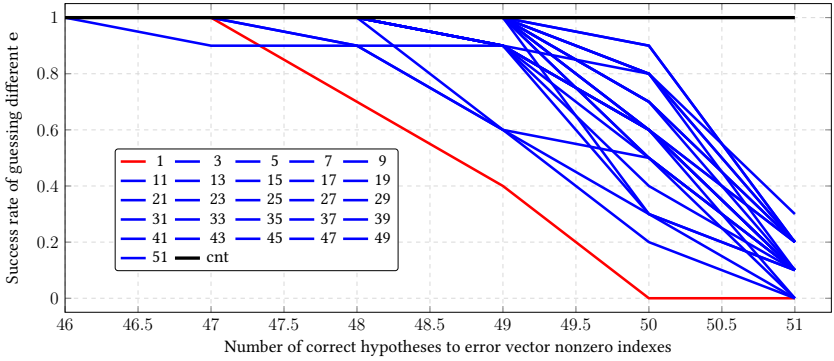
vých 10 takto zoradených hypotéz, po takto zrealizovanom CPA, tak je medzi nimi správna hypotéza o privátnom kľúči s pravdepodobnosťou veľmi blízkou 1. V sérii druhý útok bol aplikovaný na týchto prvých 10 hypotéz za účelom ich prezoradenia. V druhom útoku bol použitý HD model spotreby popisujúci len spodných 16 bitov výsledku násobenia. Tento postup priniesol značné zlepšenie pri útoku s použitím nameraných vzoriek a ešte väčšie zlepšenie úspešnosti v prípade použitia simulovaných vzoriek. Prínos sa prejavil aj v znížení zložitosti a zvýšení úspešnosti útoku. Po zrealizovaní tohto druhého útoku sa chyba simulovaného útoku stáva zanedbateľnou, čo ma veľký význam pri odhadoch zložitosti a úspešnosti útokov na základe simulácií. Porovnanie úspešnosti a zložitosti útoku po prvom a druhom CPA je možné nájsť v (Repka, Varchola, and Drutarovsky [33]; Obr. 4.1; Tab. 4.1).

Ako protiopatrenie voči tomuto útoku bolo navrhnuté efektívne protiopatrenie nevyžadujúce žiadne ďalšie zdroje, až na jedno násobenie navyše (Repka, Varchola, and Drutarovsky [33]). Na maskovanie bolo použité náhodné číslo, ktoré sa používa v rámci (EC)DSA na konci výpočtov. Toto náhodné číslo bolo použité na zamaskovanie citlivého násobenia známeho výstupného operandu s privátnym kľúčom. Viac o tomto efektívnom protiopatrení je možné nájsť v (Varchola et al. [39]).

4.2 Analýza doby výpočtu s vnášaním chýb McEliece PKC

V dizertačnej práci boli skúmané aj útoky využívajúce postranný kanál doby výpočtu algoritmu alebo jeho častí. Pri skúmaní tohto typu postranného útoku bol analýze doby výpočtu podrobený Pattersonov algebraický dekódovací algoritmus, ktorý je súčasťou dešifrovacieho procesu McEliece kryptosystému s verejným kľúčom. Ešte pred samotným podrobením tohto kryptosystému analýze doby výpočtu bolo nutné tento algoritmus implementovať. Bola vyvinutá implementácia originálneho McEliece PKC, presne podľa popisu samého McEliece (1978). Táto implementácia, ak je správne použitá (CCA2 bezpečne), je považovaná za post-kvantový kryptosystém s verejným kľúčom, teda kryptosystém odolný voči kvantovej kryptoanalýze, kryptoanalýze využívajúcej kvantový počítač. Táto implementácia bola nazvaná McEliece PKC Calculator (Repka [27]), práve preto, že všetky parametre sú voliteľné a poskytuje testovacie vektory pre každý relevantný medzivýsledok, a navyše implementuje aj nástroj na meranie doby výpočtu jednotlivých krokov Pattersonovho algebraického dekódovacieho algoritmu. Tento nástroj na meranie doby výpočtu je prezentovaný v (Repka [26]). Prehľad rôznych variant tohto kryptosystému a jeho bezpečnosti je možné nájsť v (Repka and Zajac [34]), ako aj v (Repka and Cayrel [29]), kde je poskytnutý celkový pohľad na kryptografiu založenú na lineárnych samoopravných kódoch. Analýza doby výpočtu rôznych krokov dekódovacieho algoritmu je uvedená v dizertačnej práci, pričom pozornosť bola upriamená na rozšírený Euklidov algoritmus (EEA) použitý pri riešení kľúčovej rovnice (key equation). Analýza doby výpočtu tohto EEA bola tiež vylepšená. Niekoľko poznámok o možnosti implementovať modulárnu redukciu v rozšírených konečných poliach pre McEliece PKC je možné nájsť v práci (Repka [28]).

Na grafe Obr. 4.2 je možné vidieť značné zlepšenie úspešnosti útoku z obyčajného (červená - 1) na vylepšený (čierna - cnt). Vylepšenie spočíva v zopakovaní útoku niekoľko krát s použitím informácie z predošlých útokov a nakoniec spočítania počtov výskytov hypotéz cez jednotlivé útoky, ktoré sa vyskytli na pozícii od



Obr. 4.2: Graf znázorňujúci úspešnosť hádania chybového vektoru pre McEliece PKC s $m = 11, t = 51$. Červená čiara (1) je pre klasické hádanie priamo podľa doby výpočtu. Ďalšie modré čiary (3-51) znázorňujú klasické hádanie berúc do úvahy informáciu z predošlých útokov. Čierna čiara (cnt) znázorňuje hádanie vzhľadom na počet výskytov hypotéz na prvých t pozíciach vo všetkých vykonaných útokoch.

0 do t, kde t je Hammingova váha chybového vektora.

4.3 p-ta odmocnina v rozšírených konečných poliach charakteristiky p

Výpočet p-tej odmocniny je dôležitý v mnohých aplikáciach, ako v teórii kódovania [21, 19] a v kryptografii [14, 37, 2]. Preto existujú alternatívy ako takúto p-tu odmocninu, počítať [27, 7, 36, 13, 16, 6, 38, 20]. Dizertačná práca uvádza efektívnu alternatívnu metódu pre $p \geq 2$ modulo ireducibilný polynóm bez obmedzenia. Táto metóda bola publikovaná v (Repka [24]). Okrem toho, že je metóda efektívna je aj skvele škálovateľná a paralelizovateľná, vďaka čomu je dobre implementovateľná v hardvéri. Matica pre výpočet odmocniny je rozmeru $t \times \left(t - \lceil \frac{t}{p} \rceil\right)$, čo je menej než rozmer $t \times t$ matíc používaný na výpočet odmocniny v súčasných implementáciách McEliece PKC. V súvislosti s modularnou redukciou v rozšírených konečných poliach je možné nájsť niekoľko poznámok v práci (Repka [28]).

Táto odmocnina bola implementovaná v C++ pomocou knižnice NTL, pričom implementácia bola využitá na výpočet odmocnín v náhodne generovaných rozšírených poliach $\mathbb{GF}(p^{mt})$, kde odmocnina v podpoly $\mathbb{GF}(p^m)$ bola implementovaná využitím diskrétneho logaritmu primitívneho elementu a odmocnina v rozšírenom poly $\mathbb{GF}(p^{mt})$ bola implementovaná mojou metódou. V Tab. 4.2 je príklad náhodne generovaných polí v ktorých boli odmocniny počítané.

Tabuľka 4.2: Vybraný zoznam náhodne generovaných rozšírených polí $\mathbb{GF}(p^{mt})$, v ktorých boli odmocniny počítané mojou metódou.

p	m	t	Poznámka
2	1	10.000	
2	1	100.000	Dlhý výpočet matice
2	20	51	
2	23	51	cca 5GB RAM a dlhší výpočet matice kvôli podpolu $\mathbb{GF}(p^m)$
3	3	1.000	
5	11	47	cca 15GB RAM a dlhší výpočet matice kvôli podpolu $\mathbb{GF}(p^m)$
13	6	1.000	
31	3	100	
41	2	1.000	
7919	1	1.000	
15.485.863	1	100	
32.452.843	1	100	
49.979.687	1	100	
67.867.967	1	100	
86.028.121	1	100	
104.395.301	1	100	

Chapter 5

Zoznam príspevkov autora

V nasledujúcej časti je uvedený zoznam vybraných príspevkov autora. Príspevky sú začlenené do kategórií podľa kritérií na hodnotenie úrovne výskumnej, vývojovej, umeleckej a ďalšej tvorivej činnosti v rámci komplexnej akreditácie činností vysokej školy.

5.1 Zoznam príspevkov kategórie A

5.1.1 Current Contents

[24] M. Repka. "Computing pth roots in extended finite fields of prime characteristic p >= 2". In: *Electronics Letters* 52.9 (Apr. 2016), pp. 718–719. ISSN: 0013-5194. DOI: 10.1049/el.2015.4141.

5.1.2 Science Citation Index Expanded

[27] Marek Repka. "McEliece PKC Calculator". In: *Journal of Electrical Engineering* 65.6 (2014), pp. 333–341.

[28] Marek Repka. "Note on modular reduction in extended finite fields and polynomial rings for simple hardware". In: *Journal of Electrical Engineering* 67.1 (2016), pp. 56–60.

[33] Marek Repka, Michal Varchola, and Miloš Drutarovsky. "Improving CPA against DSA and ECDSA". In: *Journal of Electrical Engineering* 66.3 (2015), pp. 159–163.

5.1.3 Pozvané články

[40] Michal Varchola, Miloš Drutarovský, and Marek Repka. "Robust FPGA based True Random Number Generator utilizing Oscillatory Metastability in Transition Effect Ring Oscillators - Invited Paper". In: *Proceedings of the 9th International Conference on Circuits, Systems, Signal and Telecommunications (CSST'15), Dubai, United Arab Emirates, February 22-24, 2015.* Ed. by Nikos E. Mastorakis and Zoran Bojkovic. WSEAS press, 2015, pp. 90–98.

5.2 Zoznam príspevkov kategórie B

[8] Lubos Gaspar et al. "Cryptoprocessor with Native Resistance against Side Channel and Fault Injection Attacks". In: *Proceedings of the 13th International Conference on Telecommunications and Informatics (TELE-INFO'14), Istanbul, Turkey, December 15-17, 2014.* Ed. by Nikos E. Mastorakis et al. WSEAS press, 2014, pp. 88–97.

[29] Marek Repka and Pierre-Louis Cayrel. In: *Multidisciplinary Perspectives in Cryptology and Information Security.* Ed. by Sattar B. Sadkhan Al Maliky and Nidaa A. Abaas. IGI Global, 2014. Chap. Cryptography Based on Error Correcting Codes: A Survey, pp. 133–156.

[32] Marek Repka and Michal Varchola. “Correlation Power Analysis using Measured and Simulated Power Traces based on Hamming Distance Power Model – Attacking 16-bit Integer Multiplier in FPGA”. In: *International Journal of Computer Network and Information Security(IJCNIS)* 7.6 (2014), pp. 10–16.

[34] Marek Repka and Pavol Zajac. “Overview of the McEliece Cyptosystem and its Security”. In: *Tatra Mt. Math. Publ* 60.3 (2014), pp. 57–83.

[39] M. Varchola et al. “Side Channel Attack on Multiprecision Multiplier Used in Protected ECDSA Implementation”. In: *2015 International Conference on ReConFigurable Computing and FPGAs, ReConFig15, Cancun, Mexico, December 7-9, 2015*. IEEE.

5.3 Zoznam prezentácií na konferenciach

[30] Marek Repka, Lubos Gaspar, and Viktor Fischer. “Correlation Power Analysis of an AES Implementation in FPGA”. In: *TatraCrypt 2012: Book of abstracts*. 2012.

[35] Marek Repka et al. “Hamming Distance Power Model Analysis of AES at Architecture Level”. In: *COSADE 2012: 3rd International Workshop on Constructive Side-Channel Analysis and Secure Design. Darmstadt, Germany, May 3-4, 2012. Darmstadt, Technische Universität Darmstadt.*

Referencie

[1] Alessandro Barenghi et al. "Exploring the Feasibility of Low Cost Fault Injection Attacks on Sub-Threshold Devices through an example of a 65nm AES implementation". In: *Workshop on RFID Security – RFIDSec'11*. Amherst, Massachusetts, USA, 2011.

[2] DanielJ. Bernstein, Tanja Lange, and Christiane Peters. "Wild McEliece Incognito". English. In: *Post-Quantum Cryptography*. Ed. by Bo-Yin Yang. Vol. 7071. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2011, pp. 244–254. ISBN: 978-3-642-25404-8. DOI: 10.1007/978-3-642-25405-5_16. URL: http://dx.doi.org/10.1007/978-3-642-25405-5_16.

[3] Eric Brier, Christophe Clavier, and Francis Olivier. "Correlation Power Analysis with a Leakage Model". In: *CHES*. 2004, pp. 16–29.

[4] David Brumley and Dan Boneh. "Remote timing attacks are practical". In: *Proceedings of the 12th conference on USENIX Security Symposium - Volume 12*. Washington, DC: USENIX Association, 2003, p. 1. URL: http://portal.acm.org/citation.cfm?id=1251354.

[5] Guo Liang Ding et al. "Correlation Electromagnetic Analysis for Cryptographic Device". In: *Proceedings of the 2009 Pacific-Asia Conference on Cir-*

cuits, Communications and Systems. Washington, DC, USA: IEEE Computer Society, 2009, pp. 388–391. ISBN: 978-0-7695-3614-9. DOI: 10.1109/PACCS.2009.144. URL: http://dl.acm.org/citation.cfm?id=1636711.1637668.

[6] Javad Doliskani and Éric Schost. "Computing in Degree 2^K 2K-extensions of Finite Fields of Odd Characteristic". In: *Des. Codes Cryptography* 74.3 (Mar. 2015), pp. 559–569. ISSN: 0925-1022. DOI: 10.1007/s10623-013-9875-7. URL: http://dx.doi.org/10.1007/s10623-013-9875-7.

[7] Martin Döring. "On the Theory and Practice of Quantum-Immune Cryptography". PhD thesis. Darmstadt: Technische Universität, 2008. URL: http://tuprints.ulb.tu-darmstadt.de/1072/.

[8] Lubos Gaspar et al. "Cryptoprocessor with Native Resistance against Side Channel and Fault Injection Attacks". In: *Proceedings of the 13th International Conference on Telecommunications and Informatics (TELE-INFO'14), Istanbul, Turkey, December 15-17, 2014.* Ed. by Nikos E. Mastorakis et al. WSEAS press, 2014, pp. 88–97.

[9] Daniel Genkin, Adi Shamir, and Eran Tromer. "RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis". In: *Advances in Cryptology - CRYPTO 2014 - 34th Annual Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2014, Proceedings, Part I.* Ed. by Juan A. Garay and Rosario Gennaro. Vol. 8616. Lecture Notes in Computer Science. Springer, 2014, pp. 444–461. ISBN: 978-3-662-44370-5. DOI: 10.1007/978-3-662-44371-2_25. URL: http://dx.doi.org/10.1007/978-3-662-44371-2_25.

[10] Daniel Genkin et al. "Stealing Keys from PCs Using a Radio: Cheap Electromagnetic Attacks on Windowed Exponentiation". In: *Cryptographic Hardware and Embedded Systems - CHES 2015 - 17th International Workshop, Saint-Malo, France, September 13-16, 2015, Proceedings.* 2015, pp. 207–228. DOI: 10.

1007/978-3-662-48324-4_11. URL: http://dx.doi.org/10.1007/978-3-662-48324-4_11.

[11] Christopher Hadnagy. *Social engineering : the art of human hacking*. Hoboken, N.J. Wiley Chichester: John Wiley, 2011. ISBN: 978-0-470-63953-5. URL: http://opac.inria.fr/record=b1133491.

[12] J. Alex Halderman et al. "Lest We Remember: Cold-boot Attacks on Encryption Keys". In: *Commun. ACM* 52.5 (May 2009), pp. 91–98. ISSN: 0001-0782. DOI: 10.1145/1506409.1506429. URL: http://doi.acm.org/10.1145/1506409.1506429.

[13] Stefan Heyse. "Low-Reiter: Niederreiter Encryption Scheme for Embedded Microcontrollers". In: *Post-Quantum Cryptography, Third International Workshop, PQCrypto 2010, Darmstadt, Germany, May 25-28, 2010. Proceedings*. Ed. by Nicolas Sendrier. Vol. 6061. Lecture Notes in Computer Science. Springer, 2010, pp. 165–181. ISBN: 978-3-642-12928-5. DOI: 10.1007/978-3-642-12929-2_13. URL: http://dx.doi.org/10.1007/978-3-642-12929-2_13.

[14] Stefan Heyse and Tim Güneysu. "Towards One Cycle per Bit Asymmetric Encryption: Code-Based Cryptography on Reconfigurable Hardware". In: *CHES*. Ed. by Emmanuel Prouff and Patrick Schaumont. Vol. 7428. LNCS. Springer, 2012, pp. 340–355. ISBN: 978-3-642-33026-1.

[15] Martin Hlaváč. "Využití postranných kanálů v symetrické a asymetrické kryptoanalýze". In: *Disertačná práce*. Universita Karlova v Praze, Matematicko-fyzikální fakulta, Katedra algebry, 2010.

[16] "IEEE Standard Specifications for Public-Key Cryptography". In: *IEEE Std 1363-2000* (2000), pp. 1–228. DOI: 10.1109/IEEESTD.2000.92292.

[17] Paul C. Kocher, Joshua Jaffe, and Benjamin Jun. "Differential Power Analysis". In: *Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology*. CRYPTO '99. London, UK: Springer-Verlag,

1999, pp. 388–397. ISBN: 3-540-66347-9. URL: http://dl.acm.org/citation.cfm?id=646764.703989.

[18] PaulC. Kocher. "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems". English. In: *Advances in Cryptology — CRYPTO '96*. Ed. by Neal Koblitz. Vol. 1109. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 1996, pp. 104–113. ISBN: 978-3-540-61512-5. DOI: 10.1007/3-540-68697-5_9. URL: http://dx.doi.org/10.1007/3-540-68697-5_9.

[19] J.S. Lemos-Neto and V.C. da Rocha. "Cyclically permutable codes specified by roots of generator polynomial". In: *Electronics Letters* 50.17 (2014), pp. 1202–1204. ISSN: 0013-5194. DOI: 10.1049/el.2014.0296.

[20] D. Panario and D. Thomson. "Efficient pth root computations in finite fields of characteristic p". English. In: *Designs, Codes and Cryptography* 50.3 (2009), pp. 351–358. ISSN: 0925-1022. DOI: 10.1007/s10623-008-9236-0. URL: http://dx.doi.org/10.1007/s10623-008-9236-0.

[21] N. J. Patterson. "The algebraic decoding of Goppa codes". In: *IEEE Transactions on Information Theory* 21 (2 1975), pp. 203–207. DOI: 10.1109/TIT.1975.1055350.

[22] Jean-Jacques Quisquater and David Samyde. "ElectroMagnetic Analysis (EMA): Measures and Counter-Measures for Smart Cards". In: *Proceedings of the International Conference on Research in Smart Cards: Smart Card Programming and Security*. E-SMART '01. London, UK, UK: Springer-Verlag, 2001, pp. 200–210. ISBN: 3-540-42610-8. URL: http://dl.acm.org/citation.cfm?id=646803.705980.

[23] Gaspar Ľuboš Repka Marek. "Hamming Distance Power Model is Architecture Dependent". In: *ELOSYS. Elektrotechnika, informatika a telekomunikácie 2012 Trenčín, 9.-12.10.2012.* Nakladateľstvo STU, 2012.

[24] M. Repka. “Computing pth roots in extended finite fields of prime characteristic p >= 2”. In: *Electronics Letters* 52.9 (Apr. 2016), pp. 718–719. ISSN: 0013-5194. DOI: 10.1049/el.2015.4141.

[25] Marek Repka. “DPA of an AES Implementation”. In: *KOZÁKOVÁ, A. ELITECH 2011: 13th Conference of Doctoral Students Faculty of Electrical Engineering and Information Technology. Bratislava, Slovak Republic, 17 May, 2011.* Nakladateľstvo STU, 2011, pp. 1–6. ISBN: 978-80-227-3500-1.

[26] Marek Repka. “Leakage Measurement Tool of McEliece PKC Calculator”. In: *Proceedings of the 13th International Conference on Telecommunications and Informatics (TELE-INFO’14), Istanbul, Turkey, December 15-17, 2014.* Ed. by Nikos E. Mastorakis et al. WSEAS press, 2014, pp. 124–132.

[27] Marek Repka. “McEliece PKC Calculator”. In: *Journal of Electrical Engineering* 65.6 (2014), pp. 333–341.

[28] Marek Repka. “Note on modular reduction in extended finite fields and polynomial rings for simple hardware”. In: *Journal of Electrical Engineering* 67.1 (2016), pp. 56–60.

[29] Marek Repka and Pierre-Louis Cayrel. In: *Multidisciplinary Perspectives in Cryptology and Information Security.* Ed. by Sattar B. Sadkhan Al Maliky and Nidaa A. Abaas. IGI Global, 2014. Chap. Cryptography Based on Error Correcting Codes: A Survey, pp. 133–156.

[30] Marek Repka, Lubos Gaspar, and Viktor Fischer. “Correlation Power Analysis of an AES Implementation in FPGA”. In: *TatraCrypt 2012: Book of abstracts.* 2012.

[31] Marek Repka, Jozef Tomeček, and Miachal Varchola. “Correlation Hamming Distance Power Analysis of 16-bit Integer Multiplier in FPGA”. In: *Proceedings of the 13th International Conference on Telecommunications and Informatics (TELE-INFO’14), Istanbul, Turkey, December 15-17, 2014.* Ed. by Nikos E. Mastorakis et al. WSEAS press, 2014, pp. 49–53.

[32] Marek Repka and Michal Varchola. "Correlation Power Analysis using Measured and Simulated Power Traces based on Hamming Distance Power Model – Attacking 16-bit Integer Multiplier in FPGA". In: *International Journal of Computer Network and Information Security(IJCNIS)* 7.6 (2014), pp. 10–16.

[33] Marek Repka, Michal Varchola, and Miloš Drutarovsky. "Improving CPA against DSA and ECDSA". In: *Journal of Electrical Engineering* 66.3 (2015), pp. 159–163.

[34] Marek Repka and Pavol Zajac. "Overview of the McEliece Cyptosystem and its Security". In: *Tatra Mt. Math. Publ* 60.3 (2014), pp. 57–83.

[35] Marek Repka et al. "Hamming Distance Power Model Analysis of AES at Architecture Level". In: *COSADE 2012: 3rd International Workshop on Constructive Side-Channel Analysis and Secure Design. Darmstadt, Germany, May 3-4, 2012. Darmstadt, Technische Universität Darmstadt.*

[36] Daniel Shanks. "Five number-theoretic algorithms". In: *Proceedings of the Second Manitoba Conference on Numerical Mathematics (Univ. Manitoba, Winnipeg, Man., 1972).* Winnipeg, Man.: Utilitas Math., 1973.

[37] Abdulhadi Shoufan et al. "A Novel Cryptoprocessor Architecture for the McEliece Public-Key Cryptosystem". In: *IEEE Trans. Computers* 59.11 (2010), pp. 1533–1546.

[38] Falko Strenzke. "A Smart Card Implementation of the McEliece PKC". In: *Information Security Theory and Practices. Security and Privacy of Pervasive Systems and Smart Devices, 4th IFIP WG 11.2 International Workshop, WISTP 2010, Passau, Germany, April 12-14, 2010. Proceedings.* 2010, pp. 47–59. DOI: 10.1007/978-3-642-12368-9_4. URL: http://dx.doi.org/10.1007/978-3-642-12368-9_4.

[39] M. Varchola et al. "Side Channel Attack on Multiprecision Multiplier Used in Protected ECDSA Implementation". In: *2015 International Conference on ReConFigurable Computing and FPGAs, ReConFig15, Cancun, Mexico, December 7-9, 2015.* IEEE.

[40] Michal Varchola, Miloš Drutarovský, and Marek Repka. "Robust FPGA based True Random Number Generator utilizing Oscillatory Metastability in Transition Effect Ring Oscillators - Invited Paper". In: *Proceedings of the 9th International Conference on Circuits, Systems, Signal and Telecommunications (CSST'15), Dubai, United Arab Emirates, February 22-24, 2015*. Ed. by Nikos E. Mastorakis and Zoran Bojkovic. WSEAS press, 2015, pp. 90–98.

[41] Serge Vaudenay. "Security Flaws Induced by CBC Padding - Applications to SSL, IPSEC, WTLS ..." In: *EUROCRYPT*. Ed. by Lars R. Knudsen. Vol. 2332. Lecture Notes in Computer Science. Springer, 2002, pp. 534–546. ISBN: 3-540-43553-0.