Číslicový návrh spojující odolnost proti útokům a odolnost proti poruchám

Vojtěch Miškovský
1. ročník, prezenční studium
Školitel: Hana Kubátová, školitel specialista: Martin Novotný

České vysoké učení technické v Praze, Fakulta informačních technologií
Thákurova 9, 160 00 Praha 6
miskovoj@fit.cvut.cz

***Abstrakt*—Tento výzkum se zabývá možnostmi, jak zkombinovat metody číslicového návrhu pro odolnost proti poruchám a odolnost proti útokům. Tyto vlastnosti se mohou často navzájem potlačovat, jejich dosažení je navíc často doprovázeno výrazným zvýšením plochy a spotřeby. V současné době se výzkum zaměřuje na vzájemný vliv obou vlastností, v budoucnu bude cílem vytvořit návrhovou metodu zlepšující obě vlastnosti současně.**

***Klíčová slova*—odolnost proti útokům, odolnost proti poruchám, FPGA, DPA, AES, spolehlivost, bezpečnost**

I. Úvod

Častým požadavkem na číslicový návrh je odolnost proti poruchám. Za tímto účelem bylo vymyšleno velké množství návrhových metod [1], [2] Dalším důležitým aspektem je bezpečnost. V případě číslicového návrhu se bezpečností rozumí zejména odolnost proti útokům postranními kanály. I pro ni existuje dostatek návrhových technik, např. [3], [4].

Cílem tohoto výzkumu je vyšetřit vliv návrhových technik pro odolnost proti poruchám na odolnost proti útokům a opačně. Na základě získaných poznatků by pak měly vzniknout nové metody pro číslicový návrh zvyšující odolnost proti útokům i proti poruchám, které by oproti kombinaci současných technik měly snížit režii plochy a spotřeby. Výsledky by tedy měly být využitelné pro návrh bezpečnějších a spolehlivějších kryptografických systémů s nižšími náklady.

V současné době se zabýváme zejména vlivem pasivní hardwarové redundance na odolnost proti diferenciální příkonové analýze (Differential Power Analysis - DPA). Tato skupina spolehlivostních technik se vyznačuje tím, že využívá více shodných funkčních modulů, jejichž výstupy porovnává, díky čemuž může dojít k detekci či zamaskování poruchy. Zároveň však dochází k několikanásobnému zvýšení plochy a zejména spotřeby, což může ovlivnit právě odolnost proti útoku pomocí DPA.

Vyhodnocení tohoto vlivu je realizováno pomocí šifry AES implementované v FPGA. Vzhledem k tomu, že nelze dostatečně přesným způsobem modelovat chování spotřeby FPGA (ať už z důvodu jejich komplexnosti či nedostatečné zdokumentovanosti), měřímě tento vliv experimentálně. Konkrétně jde o vyhodnocení závislosti počtu měření spotřeby nutných k získání šifrovacího klíče na využitých spolehlivostních návrhových metodách.

Článek se bude věnovat nejprve představením současných technologií (sekce II), dále si popíšeme implementaci šifrovacího zařízení, na které budeme útočit (sekce III), ukážeme si platformu pro realizaci útoku (sekce IV) a na závěr si ukážeme samotné výsledky měření (sekce V), vyvodíme závěry (sekce VI) a nastíníme možná budoucí pokračování výzkumu (sekce VII).

II. Současné technologie

V této sekci se seznámíme s existujícími technikami a technologiemi: návrhovými metodami pro odolnost proti poruchám, šifrou AES, diferenciální příkonovou analýzou.

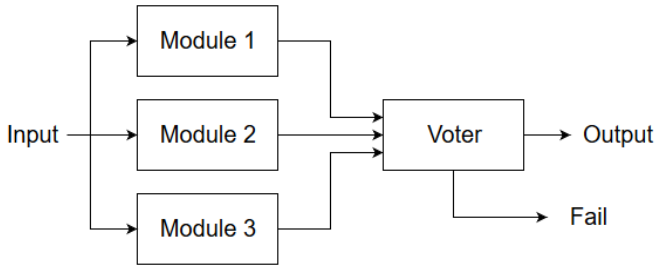
A. Návrhové metody odolné proti poruchám

Jak bylo zmíněno v úvodu, zabýváme se pasivní hardwarovou redundancí, zejména pak duplexem, TMR a NMR.

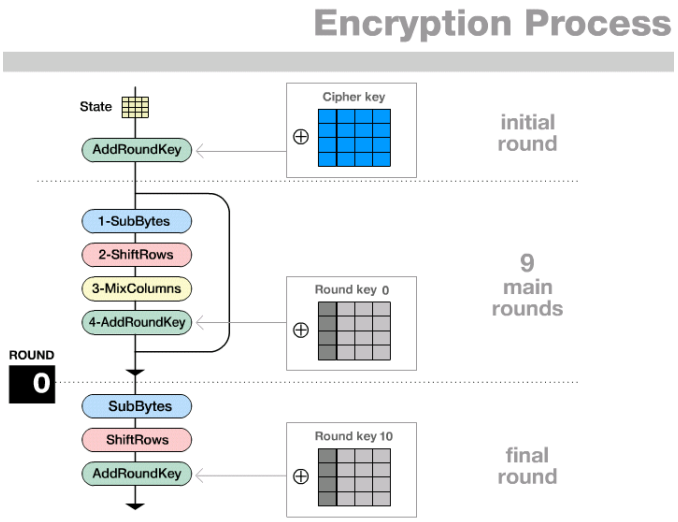
1) Duplex: Nejjednodušší spolehlivostní metoda, která funguje tak, že funkční modul je v zařízení umístěn dvakrát a výstupy obou kusů jsou porovnávány. V případě, že se vstupy neshodují, došlo na jednom z modulů k poruše. Z toho tedy vyplývá, že duplex slouží pouze pro detekci poruchy jednoho modulu, nebo i obou za předpokladu, že se nejedná o shodné poruchy.

2) TMR: TMR, anglicky Triple Modular Redundancy, je metoda využívající tři shodné funkční moduly a takzvaný majority voter. Ten vyhodnocuje výstupy všech tří modulů a volí z nich takový, který je shodný nejméně pro dva moduly. Tato metoda tedy dokáže zamaskovat poruchu jednoho z modulů a detekovat poruchy ve více modulech, pokud tyto poruchy nejsou shodné. Schéma TMR naleznete na obrázku 1.

3) NMR: NMR (N-Modular Redundancy) je v podstatě zobecněním TMR. Pro tuto metodu potřebujeme $N = k \times 2 + 1$ modulů. V tomto případě majority voter vybere takový výstup, který je shodný pro $k + 1$ modulů. Dokáže tedy zamaskovat poruchu v k modulech.



Obrázek 1. Schéma TMR



Obrázek 2. Schéma AES se 128bitovým klíčem

B. AES

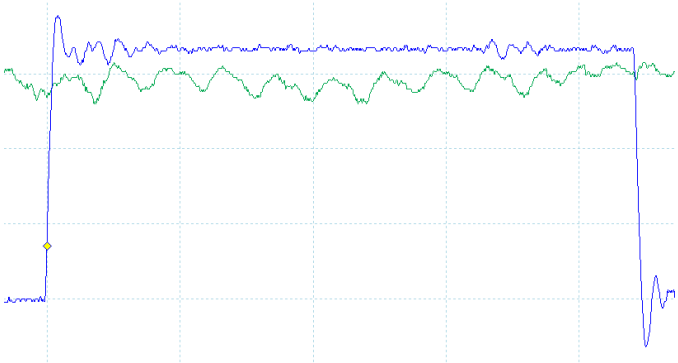
Jako šifru, na kterou budeme útočit, jsme použili AES. Jedná se o nejčastěji používanou blokovou šifru, která se používá například pro zabezpečení bezdrátových sítí Wi-Fi. Šifra využívá pevnou velikost bloku 128 bitů. Existují tři varianty lišící se délkou klíče - 128 bitů, 192 bitů a 256 bitů. Pro naše účely jsme zvolili tu nejjednodušší, 128bitovou.

AES s délkou klíče 128 bitů se skládá z deseti rund a jedné inicializační rundy. Pro použití DPA je důležité, že inicializační runda pouze aplikuje funkci XOR na otevřený text s klíčem. Další rundy se skládají z několika dílčích funkcí a využívají rozdílné rundovní klíče odvozené z původního klíče. Pro nás je důležitá funkce SubBytes. To je nelineární bijektivní funkce, čehož lze s výhodou využít při DPA, jak si ukážeme později. Schéma celého šifrovacího procesu je na obrázku 2.

Kompletní popis šifry lze dohledat ve specifikaci [5].

C. Differential Power Analysis

DPA patří mezi útoky postranními kanály. Tyto útoky jsou specifické tím, že neútočí na kryptografické principy šifry, ale na její implementaci. DPA je založeno na analýze průběhu spotřeby. Pro provedení útoku je zapotřebí znalost otevřeného textu nebo šifrovaného textu. Celý útok bychom mohli rozdělit na tři fáze:



Obrázek 3. Graf průběhu spotřeby v čase jednoho šifrování na FPGA (zeleně) a triggeru (modře)

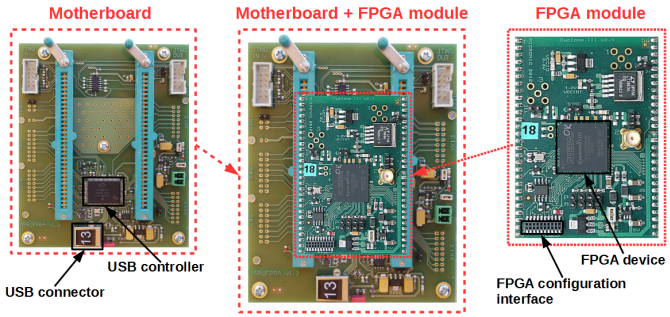
Měřící
: V této fázi je třeba změřit průběh spotřeby šifrovacího zařízení pro různé otevřené texty. Množství těchto průběhů potřebných k získání klíče je jeden z ukazatelů odolnosti proti DPA. Příklad grafu jednoho průběhu spotřeby je na obrázku 3.

Hypotetická
: Pro všechny naměřené průběhy je potřeba spočítat hypotetickou hodnotu, na které je přímo závislá spotřeba, která by tedy pro velké množství průběhů měla se spotřebou korelovat. Obvykle se bere hodnota závislá na jednom bytu klíče a jednom bytu otevřeného textu. V našem případě počítáme hammingovu váhu funkce SubBytes aplikované na otevřený text XOR šifrovací klíč, což odpovídá inicializační rundě a prvnímu kroku první rundy AES. Tato hodnota je tedy závislá na klíči i otevřeném textu, navíc je funkce SubBytes nelineární, díky čemuž nebude spotřeba korelovat se sousedními hodnotami klíče. Hypotetickou hodnotu musíme spočítat pro každou možnou hodnotu klíče (0-255) a každý byte klíče (1-16).

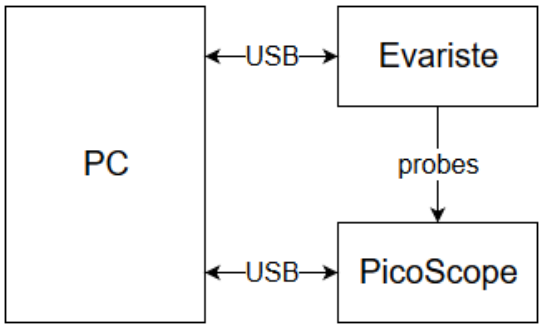
Výpočetní
: Nyní je potřeba najít korelaci mezi reálnou spotřebou a hypotetickou spotřebou. Z prvních dvou fází jsme získali matice reálné spotřeby (otevřené texty $\times$ měření v čase) a hypotetických hodnot (možné hodnoty klíče $\times$ otevřené texty). Výpočtem korelace (Pearsonova korelačního koeficientu) mezi vektory těchto matic získáme matici korelací (možné hodnoty klíče $\times$ měření v čase), kde nejvyšší absolutní hodnota by měla odpovídat danému bytu klíče a času, kdy se tento nejvíce projevil na spotřebě. Toto musíme provést pro každý byte klíče. [6],[7]

III. Implementace

Pro implementaci útoku byla zvolena platforma Evariste III [8] s využitím FPGA modulu s čipem Altera Cyclone III. Tato platforma byla vytvořena pro vytváření generátorů náhodných čísel, ale také pro analýzu spotřeby. Zařízení obsahuje USB



Obrázek 4. Platforma Evariste III



Obrázek 5. Hardwarové schéma měření

řadič, který je využit pro nahrávání klíče a otevřeného textu. Platforma Evariste III je zobrazena na obrázku 4.

Pro účely měření jsem vytvořil vlastní implementaci šifry AES v jazyce VHDL a dále moduly pro implementaci variant odolných proti poruchám, duplex TMR a NMR.

IV. Měření

Popis měření můžeme rozdělit na hardwarovou část a softwarovou část.

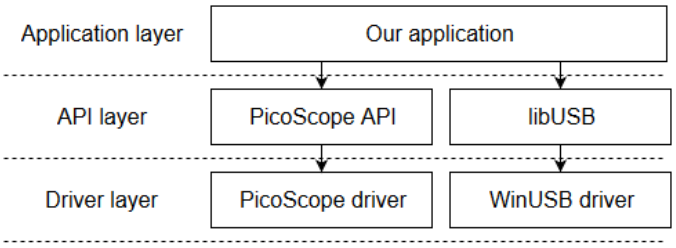
A. Hardware

Měření spotřeby bylo prováděno pomocí osciloskopu PicoScope 6404D. Tento osciloskop podporuje až 2,5GS/s. Data z osciloskopu byla získávána prostřednictvím USB. Taktéž pomocí USB probíhala komunikace se zařízením Evariste. Schéma hardwarové platformy je vyobrazeno na obrázku 5.

B. Software

Nejprve bylo pro měření využíváno PicoScope software dodávaného s osciloskopem a pro výpočty Wolfram Mathematica 10. Tuto kombinaci využíváme na fakultě pro DPA na SmartCard, ovšem pro potřeby FPGA, kde je pro získání klíče potřeba daleko více průběhů (otevřených textů), se ukázalo být nedostatečné, bylo tudíž potřeba vytvořit jiné řešení.

Pro měření i výpočet jsem naprogramoval aplikaci v C++, která využívá PicoScope API pro komunikaci s osciloskopem prostřednictvím jeho ovladače a knihovnu libusb pro komunikaci se zařízením Evariste za použití ovladače WinUSB. Tato architektura je znázorněna na obrázku 6.



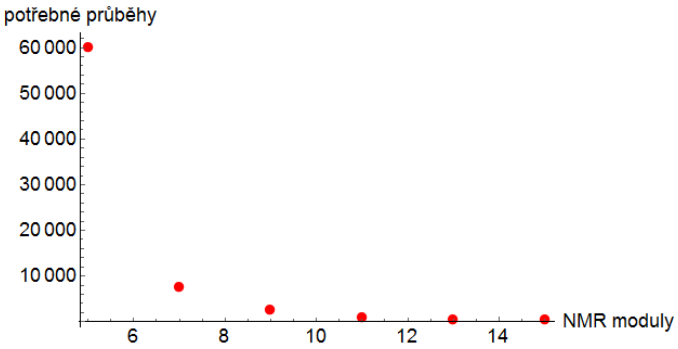
Obrázek 6. Sotwarové schéma měřicí aplikace

Tabulka I
Porovnání času v sekundách potřebného pro výpočet DPA při použití různého sotfwaru pro různé počty měření

	100	1,000	10,000	100,000	1,000,000
Math.&Pico.	28	266	7,496	n/a	n/a
C++ app	1	12	118	1,729	21,361

Tabulka II
Závislost počtu naměřených průběhů spotřeby nutných k získání klíče pro různé počty modulů v NMR

počet modulů v NMR	5	7	9	11	13	15
počet měření	60,000	7,500	2,500	800	500	495



Obrázek 7. Graf závislosti počtu naměřených průběhů spotřeby nutných k získání klíče pro různé počty modulů v NMR

Aplikace využívá pro výpočet Pearsonova korelačního koeficientu jednoduchý sekvenční algoritmus, který je urychlen předpočítáním průměrů a rozptylů jednotlivých sloupců matic, neboť tyto jsou využívány opakovaně.

Naše aplikace, ač neoptimalizovaná, se ukázala být několikanásobně rychlejší než využití kombinace PicoScope software a Wolfram Mathematica, jak ukazuje tabulka I.

V. Výsledky

V současné době se nám podařilo získat šifrovací klíč pouze při nasazení NMR pro 5 a více modulů. Počet naměřených průběhů nutný pro získání klíče naleznete v tabulce II. Čím více potřebných průběhů, tím je aplikace odolnější proti útoku.

Z grafu na obrázku 7 se zdá, že závislost počtu potřebných měření na počtu modulů je exponenciální. To lze snadno vysvětlit. Aby se do zařízení vešel potřebný počet modulů, byla použita implementace pouze části šifry, konkrétně inicia-

lizační XOR otevřeného textu a klíče a dále funkce SubBytes, což je přesně ta část šifry, na kterou útočíme pomocí DPA. Bohužel to také znamená, že výstupem této části šifry je právě ta hodnota, kterou počítáme v hypotetické fázi útoku (viz II-C). Tento výstup se následně propaguje do majority voteru, který má faktoriální plochu (porovnává všechny $(N-1)/2$ velké podmnožiny výstupů modulů) a tedy zřejmě i spotřebu. Toto je nejpravděpodobnější vysvětlení exponenciálně vypadající závislosti, která je ve skutečnosti spíše faktoriální. Tyto výsledky ovlivněné neúplnou implementací AES tedy mají nízkou vypovídající hodnotu.

Pro řešení této situace bude potřeba výstup před vstupem do voteru zamaskovat nelineární funkcí (například aplikací funkce SubBytes podruhé) a měření provést znovu, aby výsledky lépe odpovídaly reálné implementaci. Je bohužel velmi pravděpodobné, že změna způsobí výrazný nárůst potřebného počtu měření, které tedy bude potřeba optimalizovat.

VI. Závěr

Aplikace vytvořená pro urychlení měření i výpočtu diferenciální příkonové analýzy se ukázala být více než desetinásobně rychlejší oproti kombinaci softwaru dodávaného s osciloskopem a Wolfram Mathematica, čímž plní svůj účel. Toto zrychlení je zřejmě způsobeno vyšší rychlostí kompilovaného programu oproti Mathematicou interpretovanému skriptu. S ohledem na velký rozdíl mezi náročností DPA na FPGA a SmartCard však bude vhodné provést další optimalizace této aplikace, zejména s ohledem na paralelizmus a efektivní využití pamětí cache procesoru. Vzhledem k povaze výpočtu lze zvážit i využití výpočtů na GPU.

Naměřené výsledky pro NMR s různým počtem modulů vykazují zdánlivě exponenciální závislost počtu potřebných naměřených průběhu na počtu modulů. Vysvětlení této závislosti je navrženo v sekci V. Pro získání relevantních dat bude třeba měření upravit a zopakovat. Výsledky těchto nových měření by měly být součástí prezentace.

Ačkoli tedy výstupem práce zatím nejsou zcela relevantní výsledky, lze na základě naměřených dat odhadovat, že základní metody pasivní redundance opravdu snižují odolnost proti diferenciální příkonové analýze, i když zřejmě méně, než by se zdálo na základě dosavadních měření.

VII. Budoucí práce

Pro získání dalších výsledků bude potřeba optimalizovat naši aplikaci pro DPA. Pak bude možné získat výsledky nejen pro NMR, ale i pro jeden modul AES, což je pro další posun nezbytné. S vylepšenou aplikací se pak budeme moci zaměřit na další návrhové metody pro odolnost proti poruchám.

DPA není jediným útokem postranními kanály, tudíž by bylo vhodné se věnovat i ostatním, například diferenciální chybové analýze (Differential Fault Analysis - DFA). Díky rozšířenému okruhu uvažovaných útoků získáme relevantnější informace o tom, které spolehlivostní návrhové metody mají jaký vliv na odolnost proti útokům.

Další možností pokračování výzkumu je zkoumat vliv návrhových metod pro odolnost proti útokům na odolnost proti poruchám. Tím získáme náhled z opačné strany a budeme moci určit, které metody jsou vhodné pro použití ve spolehlivých systémech.

Finálním cílem celého výzkumu je využít data získaná v předchozích krocích a vytvořit metody číslicového návrhu zvyšující odolnost proti útokům a odolnost proti poruchám současně, ať už se bude jednat o úpravu některých současných metod, či zcela nové návrhové metody.

Poděkování

Tento výzkum byl podporován grantem GA16-05179S Grantové agentury České Republiky, „Výzkum vztahů a společných vlastností spolehlivých a bezpečných architektur založených na programovatelných obvodech“ (2016-2018) a projektem SGS16/042/OHK3/1T/18 ČVUT.

Literatura

[1] D. Pradhan, *Fault-tolerant computer system design*. Upper Saddle River, N.J: Prentice Hall PTR, 1996.

[2] I. Koren, *Fault-tolerant systems*. Amsterdam Boston: Elsevier/Morgan Kaufmann, 2007.

[3] K. Tiri and I. Verbauwhede, “A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation,” in *Design, Automation and Test in Europe Conference and Exhibition, 2004. Proceedings*, vol. 1, Feb 2004, pp. 246–251 Vol.1.

[4] S. Yang, W. Wolf, N. Vijaykrishnan, D. N. Serpanos, and Y. Xie, “Power attack resistant cryptosystem design: a dynamic voltage and frequency switching approach,” in *Proceedings of the conference on Design, Automation and Test in Europe-Volume 3*. IEEE Computer Society, 2005, pp. 64–69.

[5] F. I. P. S. P. F. 197), “Advanced Encryption Standard (AES),” 2001.

[6] C. Paar, *Implementation of Cryptographic Schemes 1*, Ruhr University Bochum, 2015.

[7] L. T. McDaniel III, “An investigation of differential power analysis attacks on FPGA-based encryption systems,” Ph.D. dissertation, Virginia Polytechnic Institute and State University, 2003.

[8] V. Fischer, F. Bernard, and P. Haddad, “An open-source multi-FPGA modular system for fair benchmarking of true random number generators,” in *Field Programmable Logic and Applications (FPL), 2013 23rd International Conference on*. IEEE, 2013, pp. 1–4.