

## O čem byl CHES 2005 a FDTC 2005?

Jan Krhovják, Fakulta informatiky, MU, Brno

([xkrhovj@fi.muni.cz](mailto:xkrhovj@fi.muni.cz))

*Tento článek stručně shrnuje několik hlavních témat (a do nich spadajících příspěvků) z workshopů Cryptographic Hardware and Embedded Systems (CHES) 2005 a Fault Diagnosis and Tolerance in Cryptography (FDTC) 2005, které proběhly na přelomu srpna a září ve skotském Edinburgu. Témata CHES pokrývají problematiku (bezpečného) hardware určeného pro kryptografické účely, jeho efektivitu, problémy spjaté s nedostatkem zdrojů, ale také útoky (nejen postranními kanály) na tento speciální hardware, či problémy související s aritmetikou používanou pro kryptografické operace. Témata FDTC pak pokrývají především útoky založené na chybové analýze a metody ochrany proti nim. Podrobné informace a kompletní příspěvky (v původním pořadí :-)) lze nalézt ve sbornících [CHES05, FDTC05].*

### Speciální hardware

Tento blok byl věnován specializovaným hardwarovým zařízením, která souvisejí jak s kryptografií tak také s kryptoanalýzou. První příspěvek pojednával o realizovatelném hardwarovém prosévacím zařízení SHARK, které by mělo být schopno uskutečnit prosévací část GNFS (General Number Field Sieve) pro 1024bitové číslo do jednoho roku. GNFS je (asymptoticky) nejlepší známý algoritmus pro faktorizaci velkých čísel s velkými faktory, který je složen z prosévací a maticové části (kde právě prosévací část je ta obtížnější). Cena takového zařízení je odhadnuta na méně než 200 milionů dolarů. Dále bylo popsáno hardwarové zařízení, které urychluje maticový krok GNFS pomocí řešení řídkých systémů lineárních rovnic. Jeho cena by měla být výrazně nižší než cena prosévacích zařízení. Na závěr byl představen návrh testovatelného (a bezstavového) generátoru skutečně náhodných bitů/sekvencí. Jako bezstavový je navržen jak digitalizovaný zdroj šumu, tak také digitální jednotka, která vygenerované bity zpracovává. Bezstavovosti je dosaženo pravidelným resetováním obou těchto hlavních částí generátoru (každé však v různých intervalech). Zváženy jsou také nejrůznější hypotetické možnosti útoků, jejich efektivní detekce a obrana proti nim.

### Efektivní hardware

Tématem této části byly efektivní hardwarové implementace a hardwarové akcelerátory. Byly představeny dva návrhy implementací AES (jeden zaměřen na rychlost a druhý na úsporu plochy čipu a paměťovou nenáročnost) určené pro FPGA (Field Programmable Gate Array). Oba tyto návrhy ukázaly kam až sahají hranice možností využití současné technologie FPGA pro implementaci AES. Dále byl popsán postup jak implementovat co nejkompaktnější S-Box pro AES. Redukce velikosti S-boxu je oproti předcházející nejlepší kompaktní implementaci celých 20%. To umožňuje jednak snazší implementaci AES do zařízení omezených plochou čipu (např. čipové karty), ale úspora místa může být u malých čipů také využita pro vytvoření více kopií S-boxu a tím i k zvýšení stupně paralelismu při provádění *SubByte*. Pro jednoduché zvýšení paralelismu je sice potřeba pouze 16 kopií S-boxu pro jedno kolo, ale kdybychom

chtěli (pro nezpětnovazební módy jako ECB a CTM) dosáhnout úplného pipelingu, bylo by zapotřebí minimálně 160 kopií S-boxů (pro AES s délkou klíče 128 bitů a tedy s 10 koly). Další dva příspěvky se zbývaly urychlením některých specifických algebraických operací (Tate pairing) nad konkrétními poli. Jejich hardwarová implementace je však náročná a lze zatím uskutečnit jen na zařízeních jako FPGA.

## Nedostatek zdrojů

Tento blok byl věnován problematice omezených zdrojů (např. energie či paměť). Úvodní příspěvek pojednával o vytvoření energeticky nenáročných softwarových implementací algoritmů pro práci s modulární aritmetikou. Na základě podrobných analýz vybraných instrukcí RISCových procesorů (např. *load*, *store*, *add*, *mul*) byl vytvořen model pro srovnání spotřeby energie softwarových implementací těchto algoritmů. Dále byla popsána výkonná, avšak paměťově nenáročná, metoda výpočtů skalárního násobku na Koblitzových křivkách. Úspora paměti je oproti doposud známým metodám v případě hardwarové implementace 85% a v případě softwarové implementace 70%. Na závěr pak byla představena kombinace hardwarové a softwarové implementace algoritmů pro práci s hypereliptickými křivkami (hardware obstarával výpočet inverze a násobků v binárních polích).

## Hardwarové útoky a jejich prevence

V této části byl prezentován úspěšný DPA (Differential Power Analysis) útok na maskovanou hardwarovou implementaci AES. Útok je založen na energetickém modelu odvozeném ze simulací, které byly vytvořeny na základě velmi podrobných specifikací čipu (na úrovni jednotlivých hradel). Oproti běžným DPA útokům nevyužívá tento útok výstupních hodnot uložených v registrech, ale právě výstupních hodnot logických hradel. Naštěstí, útočník v praxi nemá většinou přístup k podrobným specifikacím čipu, na jejichž základě by byl schopen vytvořit pro útok nezbytnou simulaci. Dále byl představen zcela nový typ logiky odolné proti DPA útokům – MDPL (Masking Dual-Rail Pre-charge Logic). Tato logika zajišťuje konstantní spotřebu energie tak, že používá pro přenášené signály zdvojené vodiče z nichž jeden (v závislosti na přenášené logické hodnotě) je v každém hodinovém cyklu nabit a vzápětí vybit. Výhodou je, že MDPL lze implementovat pomocí běžně používané CMOS technologie, nicméně cenou, kterou zaplatíme za ochranu proti DPA, je zvětšená plocha čipu, zvýšená spotřeba energie a pouze poloviční rychlost. Na podobném principu pracuje i logika WDDL (Wave Dynamic Differential Logic) na jejímž základě byla vytvořena a prakticky testována hardwarová implementace AES. Oproti klasické implementaci AES pomocí CMOS technologie, u níž se pomocí DPA a 8000 měření podařilo snadno získat 128bitový klíč, nebyl stejný útok na WDDL implementaci AES úspěšný ani s 1 500 000 měřeními (tj. v praxi by byl de facto neproveditelný). Byly navrženy také techniky vhodné pro technologii ASIC. V dalším příspěvku o maskování na úrovni hradel byl předveden nově vytvořený teoretický model spotřeby energie, který hrubě abstrahuje komplikovaný fyzikální proces rozptylování energie v aktivním CMOS obvodu. Poté byl prezentován popis několika pokusů o neinvazivní a semi-invazivní útoky, jejichž cílem bylo získání dat z vymazaných (nebo přepsaných) energeticky nezávislých paměťových modulů (jako např. UV EPROM, EEPROM či flash). Mnohé z útoků (především na nejnovější paměťové čipy) však byly neúspěšné. V dalším

příspěvku byly popsány modely pro přímé vyhodnocování spotřeby energie v CMOS obvodu. Jejich pomocí lze simulovat odběrovou analýzu na mnoha existujících zařízeních.

## **Útoky postranními kanály**

V tomto bloku byly představeny nové typy útoků postranními kanály. Prvním z nich je DPA útok na výpočet skalárního násobku bodu eliptické křivky. Tento útok je aplikovatelný bohužel právě na eliptické křivky, jejichž parametry jsou upraveny tak, aby umožnily snadnou implementaci do hardware s omezenými zdroji. Navíc překonává běžné anti-SPA a anti-DPA techniky obrany. Další DPA útok obchází ochranné náhodné maskování na čipové kartě tak, že využívá testovací kartu s ovlivněným RNG jako vzor k provedení útoku na kartu s perfektním RNG. Třetí DPA útok je zaměřen na blokové šifry (byl ověřen na hardwarové implementaci AES) a k zvýšení efektivity využívá speciálně navržený pravděpodobnostní model. Dalším typem útoku byla úspěšná EM analýza Rijndaelu a ECC implementovaných na PDA s podporou bezdrátového přenosu. Poté byly prezentovány bezpečnostní limity pro EM vyzařování (návrhy pro případný budoucí standard), jejichž dodržení by mělo zamezit únikům citlivých informací tímto postranním kanálem. A konečně, byla také navržena simulační metoda (založená na množství spotřebované energie a detailní znalosti čipu) pro zjišťování míry EM vyzařování v CMOS obvodech. Její praktická využitelnost je však především ve fázi návrhu čipu. Poslední dva příspěvky pak pojednávaly o DPA útocích vyšších řádů, kterým nelze zabránit ani často používanou ochranou maskováním.

## **Trusted computing**

Jediný příspěvek v této části se zaměřil na problematiku bezpečné správy dat (což pokrývá životní cykly software, ale i hardware). Byly identifikovány hlavní nedostatky ve specifikaci TCG, které způsobují v současné době největší překážky pro nasazení TC ve velkém měřítku, a byla představena (a navržena ke standardizaci) také řešení těchto nedostatků.

## **Aritmetika pro kryptografii a kryptoanalýzu**

První příspěvek tohoto bloku pojednával o nové rychlé metodě modulárního násobení. Ta umožňuje rozdělit celý proces násobení na dvě nezávislé části, které pak mohou být prováděny paralelně (čímž lze v multiprocesorovém prostředí teoreticky zdvojnásobit rychlost výpočtu). Dále bylo prezentováno několik dalších urychlení pro modulární násobení (která již nevyužívala paralelismu) a navržena byla také nová modifikace algoritmu pro urychlení modulární inverze. Změna při výpočtu inverze spočívá v nahrazení běžně používaného rozšířeného Euklidova algoritmu standardním (nerozšířeným) Euklidovým algoritmem. Tím je dosaženo dvojnásobného zrychlení. Nevýhodou této optimalizace je, že je určena výhradně pro implementaci ECC do čipových karet navržených pro hardwarovou akceleraci RSA (kterých je ale na druhou stranu v současné době na trhu dostatečné množství). Prezentována byla i nová varianta „Giant-Step Baby-Step“ algoritmu, která ve speciálních případech umožňuje efektivnější výpočet diskrétního logaritmu. Na závěr byl pak představen mechanismus, umožňující analyzovat přínos randomizačních technik použitých k prevenci útoků postranními kanály.

## Chybová analýza

Závěrečná část tohoto článku se zabývá útoky založenými na chybové analýze a metodami ochrany proti nim. Jako první byl prezentován návrh využití robustních nelineárních  $(n, k)$ -detekčních kódů, které jsou oproti lineárním kódům se stejným  $n$  a  $k$  schopny detekovat chyby mnohem rovnoměrněji (a zcela nezávisle na rozložení chyb). Tím je výrazně snížena pravděpodobnost, že útočník bude schopen nějakým způsobem vyvolat v systému nedetekovanou chybu. Dále byla popsána praktická realizace útoku na běžně dostupnou čipovou kartu Silvercard (založenou na čipu PIC16F877 firmy Microchip), kde byl pomocí výkyvu v přísunu energie redukován počet kol naivní implementace AES. Navržen byl také nový typ útoku na skalární násobení v ECC, který dokáže oproti předcházejícím útokům (ty vytvářely body ležící na kryptograficky slabé křivce a byly snadno detekovatelné) vytvořit bod neopouštějící původní křivku. Zajímavý přístup založený na redundantní aritmetice v konečných polích byl použit při tvorbě asymetrického kryptosystému odolného proti chybám. Dále byly prezentovány metody možného zabezpečení jak na CRT založené implementace RSA, tak i klasické implementace RSA. Navržena byla dokonce verze RSA využívající detekčních kódů a pozornosti neunikly ani kryptosystémy založené na párování, které doposud z pohledu chybové analýzy nikdo nestudoval. Několik zbývajících příspěvků se také zabývalo metodikou hodnocení útoků chybovou analýzou a jejich protiopatřeními (např. vzájemné porovnání existujících metod, vytvoření vhodného modelu útočníka apod.).

## Reference

- [CHES05] Proceedings of the 7<sup>th</sup> International Workshop on Cryptographic Hardware and Embedded Systems (CHES) 2005, volume 3659 of Lecture Notes in Computer Science, Springer Verlag, 2005. ISBN 3-540-28474-5.
- [FDTC05] Proceedings of the 2<sup>nd</sup> International Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC) 2005, Edinburgh, Scotland, 2005.