O čem byl CHES a FDTC?

Jan Krhovják
Fakulta informatiky
Masarykova univerzita v Brně

Hlavní témata workshopů

- Cryptographic Hardware and Embedded Systems
  - Speciální hardware
  - Efektivní hardware
  - Nedostatek zdrojů
  - Hardwarové útoky a jejich prevence
  - Útoky postranními kanály
  - Trusted Computing
  - Aritmetika pro kryptografii a kryptoanalýzu
- Fault Diagnosis and Tolerance in Cryptography
  - Chybová analýza
  - Útoky a metody ochrany kryptografických klíčů
  - Útoky a metody ochrany zaměřené na RSA
  - Hodnotící modely

Speciální hardware I

- GNFS (General Number Field Sieve)
  - Asymptoticky nejlepší známý algoritmus pro faktorizaci velkých čísel s velkými faktory
    - Dvě části – prosévací a maticová
  - Existující HW implementace GNFS – TWINKLE, TWIRL
  - Navržen SHARK
    - Realizovatelné hardwarové prosévací zařízení
    - Prosévací část GNFS pro 1024 bitové číslo do 1 roku
    - Cena méně než 200 milónů dolarů
  - Navrženo zařízení urychlující maticovou část GNFS
    - Pomocí řešení řídkých systémů lineárních rovnic
    - Cena výrazně nižší než cena prosévacích zařízení

Speciální hardware II

- Testovatelný (a bezstavový) generátor skutečně náhodných čísel
  - Bezstavový digitalizovaný zdroj šumu
  - Bezstavová digitální jednotka
    - Zpracovává vygenerované bity
- Bezstavovosti dosaženo jejich pravidelným resetováním (každé v různých intervalech)
- Diskutovány i možné útoky a obrana proti nim
  - Přidání vlastního signálu na výstup dig. zdroje šumu
  - Vede k zvýšení intenzity zdroje => test intenzity zdroje

Efektivní hardware

- Dva návrhy implementací AES na FPGA
  - První zaměřen na rychlost
  - Druhý na úsporu plochy čipu a paměťovou nenáročnost
- Implementace kompaktního S-boxu
  - Úspora oproti nejlepší známé implementaci 20%
  - Snazší implementace AES do zařízení omezených plochou čipu
  - Snazší implementace více S-boxů
    - Zvýšení paralelismu
    - Úplný pipelining

Nedostatek zdrojů

- Energeticky nenáročné SW implementace
  - Na základě analýz vybraných instrukcí RISCových procesorů
  - Vytvořen model spotřeby energie
  - KCM násobení 1024bitového čísla – úspora energie 22 %
- Výkonná a paměťově nenáročná metoda výpočtu skalárního násobku na Koblitzových křivkách
  - Vhodná pro HW i SW implementace
  - Úspora oproti známým HW metodám 85 %
  - Úspora oproti známým SW metodám 70 %
- HW/SW implementace algoritmů pro práci s HECC
  - HW obstarával výpočet inverze a násobku v binárních polích

HW útoky a jejich prevence I

- DPA útok na maskovanou implementaci AES
  - Založeno na energetickém modelu odvozeném ze simulací
  - Simulace vytvořeny na základě podrobných specifikací čipu
    - K těm útočník v praxi většinou nemá přístup ☺
- Nový typ logiky odolné proti DPA útokům
  - MDPL (Masking Dual-Rail Pre-charge Logic)
    - Používá pro signály zdvojená vedení
    - Lze implementovat pomocí CMOS
    - Zvětšená plocha čipu, spotřeba energie a jen poloviční rychlost
  - WDDL (Wave Dynamic Differential Logic)
    - Podobný princip – chronologicky jde o předchůdce MDPL
    - Vytvořena testovatelná implementace AES
      - DPA útok neúspěšný ani s 1 500 000 naměřenými vzorky

HW útoky a jejich prevence II

- Maskování na úrovni hradel
  - Vytvořen teoretický model spotřeby energie
- Neinvazivní a semi-invazivní útoky
  - Cílem bylo získání vymazaných (přepsaných) dat z energeticky nezávislých pamětí (EEPROM, flash)
  - Mnohé útoky se však nepodařilo uskutečnit
    - Především útoky na moderní paměťové čipy
- Modely pro přímé vyhodnocování spotřeby energie v CMOS obvodu
  - Jejich pomocí lze simulovat odběrovou analýzu na mnoha existujících zařízeních

Útoky postranními kanály

- DPA útok na výpočet skalárního násobku bodu EC
  - Aplikovatelné právě na EC s parametry optimalizovanými pro snadnou implementaci do HW s omezenými zdroji
  - Útok překonává běžné anti-SPA a anti-DPA techniky obrany
- DPA útok obcházející náhodné maskování na SC
  - Využívá čipovou kartu s ovlivněným RNG jako vzor
- EM analýza Rijndaelu a ECC na PDA
- Bezpečnostní limity pro EM vyzařování
- Simulační metoda umožňující zjistit míru EM vyzařování v CMOS obvodech
  - Prakticky využitelná ve fázi návrhu čipu

Aritmetika v kryptologii

- Akcelerace modulárního násobení
  - Klasické metody
  - Rozdělení celého procesu na dvě paralelizovatelné části
- Akcelerace modulární inverze
  - Nahrazení rozšířeného Euklidova algoritmu
  - Použit (standardní) Euklidův algoritmus
  - Dvojnásobné zrychlení
  - Vhodné pouze pro implementace ECC do čipových karet s podporou hardwarové akcelerace RSA
- Nová varianta „Baby-step Giant-step“ algoritmu
- Analýza přínosu randomizačních technik

Chybová analýza

- Návrh využití robustních (n,k)-detekčních kódů
  - Schopny detekovat chyby rovnoměrněji než lineární kódy
- Implementace útoku na čipovou karu Silvercard
  - Pomocí výkyvu energie, redukován počet kol AES
- Nový útok na výpočet skalárního násobku v ECC
  - Výsledné body neopouštějí původní křivku
- Redundantní aritmetika v konečných polích
  - Použito k tvorbě asym. kryptosystému odolného proti chybám
- Metody zabezpečení CRT-RSA a klasického RSA
- Navržena verze RSA využívající detekčních kódů

Trusted computing etc.

- Problematika bezpečné správy dat
  - Životní cykly SW a HW
  - Identifikovány hlavní nedostatky
  - Představena (a navržena ke standardizaci) jejich řešení
- Rump session
  - Proč dále nerozbíjet již jednou rozbité kryptosystémy? ☺
- Zvané příspěvky
  - What Identity Systems Can and Cannot Do
  - Security of Identification Products: Wow to Manage
  - Trusted Computing in Embedded Systems

CHES 2006 – Yokohama