doc. Ing. Miloš DRUTAROVKÝ, CSc.

Téma a tézy inauguračnej prednášky

Odbor: 5.2.15 Telekomunikácie

„Náhodnosť a jej využitie vo vstavaných kryptografických systémoch“

V súčasnom období je kryptografická ochrana spracovávaných, uchovávaných a prenášaných dát jedným z kľúčových faktorov umožňujúcich nasadenie moderných informačno-komunikačných technológií. V dnešnej dobe nie je využitie kryptografických metód výsadou len drahých a zložitých systémov. Práve naopak, jednou z najdynamickejšie sa rozvíjajúcou oblasťou v súčasnosti je nasadenie kryptografických metód v lacných vstavaných systémoch. Typickým príkladom sú senzorové siete a ich využitie v rámci koncepcie Internetu vecí (IoT), kde je potrebné kryptografickú podporu integrovať do lacných vstavaných zariadení s relatívne obmedzenou výpočtovou kapacitou. Vo všeobecnosti je kryptografická ochrana vytváraná zo základných stavebných blokov (kryptografických primitív) ako sú symetrické a asymetrické šifry, hašovacie funkcie a generátory náhodných čísel. Pre také scenáre sú napr. vyvíjané aj špecializované stavebné bloky, ktoré zaradzujeme do kategórie tzv. ľahkej kryptografie. Ich úlohou je zabezpečiť dostatočnú bezpečnosť aj pri zníženej výpočtovej kapacite cieľového systému.

Je doporučovanou zásadou (pokiaľ neexistujú veľmi špecifické požiadavky, ktoré tomu bránia) používať len overené stavebné kryptografické bloky. Tieto sú predmetom rôznych medzinárodne akceptovaných štandardov. Do tejto klasifikácie však nezapadajú kryptografické stavebné bloky využívajúce náhodnosť. Typickým predstaviteľom je generátor skutočne náhodných čísel (TRNG – True Random number Generator), ktorý sa využíva predovšetkým na generovanie kryptografických kľúčov pre symetrické a asymetrické šifrovacie algoritmy, ale tiež napr. na generovanie náhodných dát použitých na maskovanie aktuálne vykonávaných (deterministických) kryptografických operácií s cieľom znížiť únik informácie a znížiť tak efektívnosť útokov na kryptografický hardvér s využití postranných kanálov (Side Channel Attacks). TRNG vo vstavaných systémoch typicky využívajú fyzikálne vlastnosti hardvérovej platformy ako napr. šumy a ich rôzne externé prejavy – nestabilitu hodinových signálov, neurčitosť začiatočného stavu bistabilných obvodov v pamäťových elementoch a pod. Na TRNG sú v kryptografii kladené extrémne nároky, keďže ich nefunkčnosť typicky vedie k prelomeniu celej kryptografickej ochrany. Ďalším, relatívne novším stavebným blokom, ktorý má podobnú väzbu na cieľový hardvér je PUF (Physical Unclonable Function) funkcia. Tento stavebný blok využíva náhodnosť výrobných polovodičových procesov tak, že s využitím PUF funkcií je možné napr. s dostatočnou pravdepodobnosťou identifikovať konkrétny kus cieľového hardvéru (napr. konkrétny mikropočítač, obvod FPGA, ASIC obvod) bez nutnosti vkladať do každého zariadenia jedinečný identifikátor alebo kľúč. PUF funkcie tak umožňujú realizovať napr. vzdialenú autentifikáciu vstavaného systému prípadne aktualizáciu jeho firmvéru bez nutnosti ukladať do vstavaného zariadenia špecifické kľúče. Vzhľadom na povahu TRNG a PUF blokov je zrejmé, že tieto bloky nie je možné štandardizovať a ich vývoju je vo svete venovaná trvale veľká pozornosť.

Cieľom inauguračnej prednášky je prezentovať dlhoročný výskum, vývoj a návrhy v oblasti TRNG a PUF blokov pre kryptografické aplikácie, ktoré je možné zhrnúť do nasledujúcich téz:

- Základné princípy TRNG a PUF blokov pre kryptografické aplikácie.
- Typické príklady využitia uvedených blokov vo vstavaných systémoch a aplikáciách.
- Originálne návrhy TRNG pre rekonfigurovateľné obvody na báze FPGA obvodov.

- Originálny návrh stavebného bloku s integrovanou funkciou TRNG a PUF.
- Pedagogické aktivity.
- Vedecko-výskumné aktivity.

V Košiciach 22. 5. 2017

doc. Ing. Miloš Drutarovský, CSc. v.r.