Vylepšení rychlosti kryptoanalýzy asymetrických kryptosystémů na FPGA pomocí pravidel dělitenosti

David Salač <david.salac@tul.cz>, Ing. Martin Rozkovec, Ph.D.

V rámci výzkumu možností kryptoanalýzy asymetrických kryptosystémů se nám podařilo zrychlit tzv. sieving proces díky využití základních pravidel dělitelnosti ve dvojkové soustavě. Tato část kryptoanalytického procesu je nejvíce časově náročná, tudíž i dílčí vylepšení vede k zásadnímu dopadu na celkovou rychlost procesu. Při výzkumu jsme vyšli z jednoduchých matematických pravidel pro určení, zdali je dané číslo zapsané ve dvojkové soustavě (resp. jeho bitová reprezentace) dělitelné určitým předem známým prvočíslem. Podobná pravidla existují a jsou dobře známá i při dělení v desítkové soustavě, například číslo v desítkové soustavě je dělitelné 7, pokud rozdíl součtu lichých a sudých trojic cifer je dělitelný sedmi.

Klíčová slova: pravidla dělitenosti, kryptoanalýza, asymetrické kryptosystémy, Sieving proces, Numerické metody

Úvod

Při procesu kryptoanalýzy asymetrických kryptosystémů je jedna z klíčových úloh určit kanonický rozklad daného vstupního celého čísla (mezivýstupu numerické metody) na omezené množině prvočísel (resp. určit hodnotu exponentů pro danou množinu prvočísel, na které je vstup hladký). Při určení hodnoty exponentu se nabízí jako vhodný postup vypočítat zbytek po dělení daným číslem pomocí jednoduché děličky (pokud je zbytek roven nule, je toto číslo dělitelné daným prvočíslem a je možné určit hodnotu exponentu u daného prvočísla).

Metodika

Režie na hardwarovou realizaci běžných děliček je značná a to zejména při práci s celými čísly bitové velikosti přes 512 bitů (což je cca. minimální velikost využitelná při řešení reálného kryptografického problému). Z tohoto důvodu je vhodné množství děliček maximálně snížit a optimalizovat jejich vytížení.

Pro tento účel jsme navrhli elementy pro testování dělitenosti při využití pravidel dělitelnosti ve dvojkové soustavě, které jsme navrhli a implementovali na Xilinx Artix-7 FPGA.

Princip těchto elementů je postaven na následující kongruenci. Předpokládejme, že máme bitovou reprezentaci daného n-bitového čísla, jejíž jednotlivé bity jsou ze strany LSB indexovány jako d_1, d_1 až d_n. Vytváříme pravidlo pro dělitelnost prvočíslem p:

$$d_1 2^0 + d_2 2^1 + \cdots + d_n 2^{n-1} \equiv d_1(2^0 \bmod p) + d_2(2^1 \bmod p) + \cdots + d_n(2^{n-1} \bmod p) \pmod p \quad (1)$$

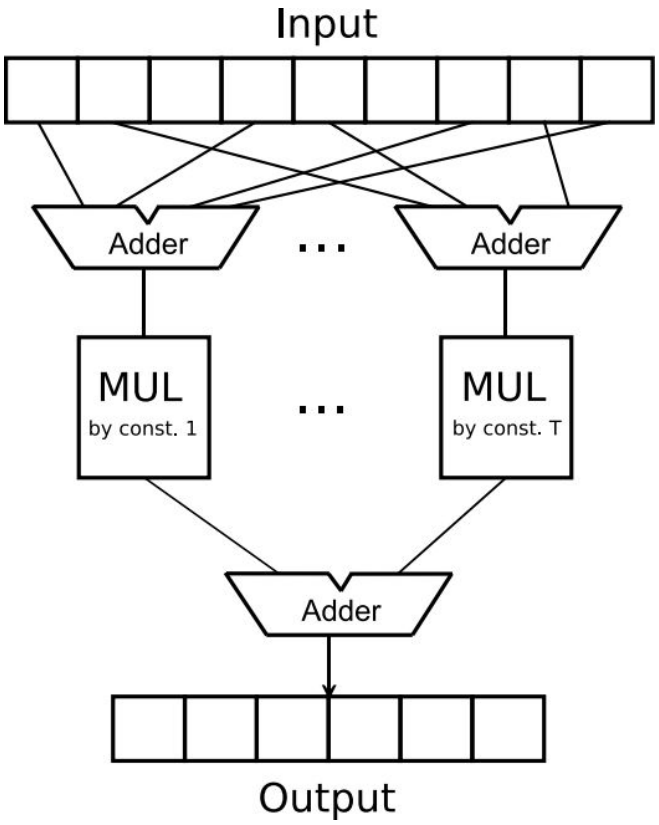
Pravá strana kongruence (1) má stejný zbytek po dělení prvočíslem p jako levá. Celková velikost čísla po prostém výpočtu pravé strany kongruence je výrazně nižší, nežli původní velikost vstupního čísla. Pro určení, zda-li je dané číslo dělitelné určeným prvočíslem stačí pouze využít malou děličku (resp. děličku s menším vstupem pro dělitel), která má značně nižší hardwarovou režii, nežli původní dělička pro n-bitový vstup. Další možností je rekurzivní aplikace popsaného postupu.

Pro určení, zda-li je dané n-bitové číslo s ciframi d_i dělitelné prvočíslem p se využívá následující algoritmus:

1. Vytvoř pomocnou celočíselnou proměnnou t a nastav ji na nulu.
2. Projeď všechny cifry d_i čísla; pokud je daná cifra rovna jedné (bit na dané pozici je 1), pak přičti k proměnné t hodnotu ($2^i \bmod p$), jež se dá snadno předem vypočítat.

3. Na konci zkontroluj dělitelnost proměnné *t*. Pokud je *t* dělitelné prvočíslem *p*, je i vstup dělitelný tímto prvočíslem. (Navíc je zbytek po dělení obecně stejný).

Takový algoritmus se dá snadno implementovat v FPGA. Operativně jsme komponentu realizující popsaný algoritmus nazvali příznačně *A divisibility checking element* (ACE).



Obrázek 1: Schéma ACE (*A divisibility checking element*)

Na Obrázku 1 je znázorněno vnitřní zapojení DSP. Perioda T, která je ve schématu zjištěna představuje maximální periodu, se kterou se čísla (2^i mod *p*) v kongruenci (1) vyskytují. Perioda T dosahuje velikosti nejvýše *p* - 1.

Výsledky a diskuze

Zjistili jsme, že celková hardwarová režie na realizaci ACE je nižší, nežli na realizaci obyčejné děličky. Latence ACE je taktéž nižší, nežli u obyčejné děličky (na principu radix-2). Na druhou stranu je propustnost ACE značně vyšší, na čemž budeme dále pracovat.

Z výše uvedeného jasně vyplývá, že na stejné ploše (resp. se stejnými hardwarovými prostředky, které jsou k dispozici), je možné realizovat podstatně více ACE, nežli je tomu u obyčejných děličeк. Kvantitativně se jedná o nejméně desetkrát více ACE, než děličeк.

Závěr

Podařilo se nám vylepšit proces tzv. sievingu u používaného u kryptoanalýzy asymetrických kryptosystémů (zejména u numerických metod jako NFS, QS, Index Calculus a jiných).

Jako další výzkum je možné hledat další vhodná využití popsaného elementu, jako je například optimalizace řešení obecných kongruencí mod *p* na FPGA.

Poděkování

Tato práce byla podpořena z projektu Studentské grantové soutěže (SGS) na Technické univerzitě v Liberci v roce 2018.

Reference

[1] Aoki K., Franke J., Kleinjung T., Lenstra A.K., Osvik D.A. (2007) A Kilobit Special Number Field Sieve Factorization. In: Kurosawa K. (eds) Advances in Cryptology – ASIACRYPT 2007. ASIACRYPT 2007. Lecture Notes in Computer Science, vol 4833. Springer, Berlin, Heidelberg

[2] S. Bai, C. Bouvier, A. Kruppa and P. Zimmermann, "Better polynomials for GNFS", Mathematics of Computation, vol. 85, no. 298, pp. 861-873, 2015.

[3] Laurence T. Yang, Gaoyuan Huang, Jun Feng, Li Xu, Parallel GNFS algorithm integrated with parallel block Wiedemann algorithm for RSA security in cloud computing, Information Sciences, Volume 387, 2017, Pages 254-265, ISSN 0020-0255, https://doi.org/10.1016/j.ins.2016.10.017.

[4] Laurence T. Yang, Ying Huang, Jun Feng, Qiwen Pan, Chunsheng Zhu, An improved parallel block Lanczos algorithm over GF(2) for integer factorization, Information Sciences, Volume 379, 2017, Pages 257-273, ISSN 0020-0255,