TECHNICKÁ UNIVERZITA V LIBERCI
Fakulta mechatroniky, informatiky
a mezioborových studií

SKFM 2018
Studentská konference Fakulty mechatroniky, informatiky a mezioborových studií

Optimalizace kryptoanalýzy asymetrických systémů na FPGA pomocí pravidel dělitenosti

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

ABSTRAKT

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.

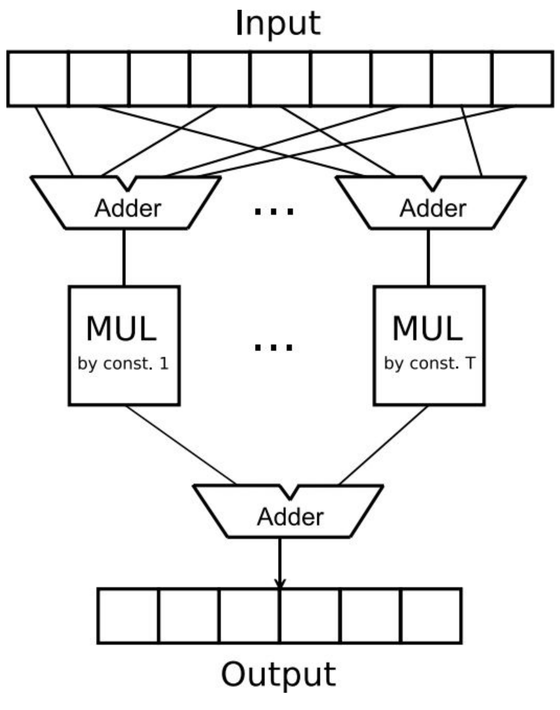
ÚVOD

V rámci tzv. sieving procesu, který se vyskytuje v numerických metodách pro řešení kryptoanalýzy se často vykytuje rozklad na součin konečně mnoha předem definovaných prvočísel a jejich exponentů.

METODIKA

Princip vylepšení spočívá v nahrazení děliček, které se běžně pro výpočet exponentů využívají za elementy, které nejdříve otestují dělitelnost daného čísla daným prvočíslem a až poté děliček pro přesné určení hodnoty exponentu.

Veškerá logika navrženého hardware (tzv. ACE) je zobrazena na obrázku (1) níže.



Obrázek 1: schéma elementu pro testování dělitelnosti daným prvočíslem (ACE).

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 děliček. Kvantitativně se jedná o nejméně desetkrát více ACE, než děliček.

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.

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