Posudek oponenta k diplomové práci
Útoky založené na hardwarových chybách
Martiny Válkové

Předložená práce zkoumá následující problém: Předpokládejme, že máme zařízení, které počítá součiny w-bitových čísel, přičemž pro právě jednu dvojici čísel $(a, b), a \neq b$ dává špatný výsledek. Práce se zabývá otázkou, zda je možné takovou chybu využít pro útok na kryptografická schémata, která jsou založena na počítání mocnin modulo nějaké velké číslo. Zde jde konkrétně o symetrické schema Pohlig-Hellman a nesymetrickou šifru RSA.

Základní myšlenka je převzata z článku Biham, Carmeli, Shamir: *Bug Attacks*, jde o vyvolání chyby v jednom konkrétním kroku algoritmu pro modulární umocňování. Chyba ovlivní výstup způsobem, kdy jsme schopni detekovat bit, či blok bitů tajného klíče.

V práci jsou diskutovány dva typy umocňování algoritmy LTOR a RTOL, které lze použít pro výpočet mocnin. Navrhované útoky se pak liší podle toho, který z algoritmů a v jaké implementaci chybové zařízení používá. V kapitole 5 jsou diskutovány 2 základní typy útoků: Chybový útok (zjišťuje se zda došlo k chybě) a útok s chybovým faktorem (chybový výsledek je porovnán se správným). Pro útoky na systém Pohlig-Hellman je aplikován algoritmus pro odmocňování v $\mathbb{Z}_p^*$ podrobně rozebraný v kapitole 2.

Možnost eliminace chyb, které vznikají v nežádoucích krocích algoritmu, je diskutována v šesté kapitole. Problémy, které vystanou při praktické realizaci, jsou spolu s dalšími variantami útoku pro různé implementace LTOR probírány v kapitole 7. Kapitola 8 pak diskutuje varianty útoku na RSA, pokud jsou užité nějaké optimalizační metody (např. Montgomeryho násobení). Devátá kapitola komentuje simulaci útoků, které autorka provedla v Mathematice 7.0. Je docela zajímavé, že chybový útok na Pohlig-Hellmanovo schéma využívající LTOR pro dlouhé klíče ztroskotal, protože k výpočtu odmocniny v $\mathbb{Z}_p^*$ bylo třeba faktorizovat dlouhé číslo, zatímco útoky na RSA proběhly úspěšně. Soubor se simulací útoku je přiložen, bohužel jsem ho nebyl schopen prohlédnout.

Práce je sepsána pečlivě a poutavě, našel jsem jen minimum překlepů (např. v Algoritmu 7 krok (f) má být k místo l). Z hlediska srozumitelnosti bych měl nějaké výhrady. Obecně mi přijde, že některé argumenty týkající se pravděpodobnosti jevů nejsou přesné. Nejspíše to má nějaký důvod, který ale není explicitně vysvětlen. Například proč v Pozorování 4.2.1 předpoklad nezávislosti jednotlivých cyklů nezkreslí odhad. Dále důkaz Pozorování 4.2.2 využívá několika faktů, které by potřebovaly vysvětlit - nezávislost b_C a b_{zC}, rovnost $P(a_{z^2}) = P(a)$. V důkazu Pozorování 6.2.1 je tvrzení o malé pravděpodobnosti vzniku náhodné chyby vpodstatě konstatováno bez nějakého odhadu.

Asi by bylo dobré podotknout, že chybový faktor β v Algoritmu 7 by měl mít dostatečně velký řád (pokud by byl řád 2, dozvíme se jenom u_0). Dále by bylo dobré okomentovat na straně 46 zmíněný problém diskrétního logaritmu v kroku 1.(e), zde je asi důležité, že známe $2^r d'$. Podobně by se měla ošetřit možnost, kdy C_0 z Algoritmu 8 bude mít malý řád, jinak by nemusela proběhnout inicializace.

Nakonec, asi není dobré v důkazu tvrzení uvádět, kudy cesta nevede (důkaz Tvrzení 4.1.1). Myslím, že lepší by bylo uvést pouze správný důkaz a pod něj případně připojit poznámku.

Celkově mi práce přijde zajímavá, myslím, že autorka problematice rozumí. Navrhuji proto hodnocení *výborně*.

V Praze, 21. 1. 2011

Pavel Příhoda