POSUDEK VEDOUCÍHO NA BAKALÁŘSKOU PRÁCI
ANNY GODUŠOVÉ
DŮKAZY BEZPEČNOSTI DIGITÁLNÍCH PODPISŮ

Jedná se o práci z oblasti teoretické kryptografie věnované bezpečnosti kryptografických schémat. Konkrétně se jedná o podpisová schémata využívající jednosměrné permutace se zadními vrátky a náhodné orákulum.

Formálně je to práce kompilační. Čerpá ze dvou odborných článků, jejichž výsledky jsou kromě převodu do slovenštiny představeny způsobem přístupnějším méně pokročilému čtenáři, což jako obvykle vyžaduje doplnění různých drobných kroků, případně opravu některých nepřesností.

Rozsah práce je skromnější než by bylo možné a zřejmě i vhodné, protože současná podoba nezohledňuje motivaci pro zavedení pravděpodobnostního schématu (kapitola 4) a ospravedlnění předpokladu multiplikativity, totiž využití jednosměrné permutace založené na RSA, což je důležitou složkou druhého článku (na tom nese část viny vedoucí práce).

Výsledná podoba práce je vcelku čitelná s několika stylistickými neobratnostmi, které mohou být zavádějící (útočník I např. asi nebude spouštět generátor $\mathcal{G}$ až potom, co dostal výzvu invertovat y). Po jistém úsilí se podařilo srozumitelně definovat většinu základních pojmů a představit důkazy s komentářem základních myšlenek. Je škoda, že podobné pasáže tří uvedených důkazů jsou prakticky doslovně zopakovány, namísto nějakého jejich vstřícnějšího zpracování.

Konkrétní výtky:

- Některé pojmy jsou stále formulovány nešikovně až může vznikat otázka, zda jim autorka rozumí, např. definice 1^k na str. 1 nebo definice uniformní distribuce na str. 3;
- Tvrzení 2.1.1 (jedno z hlavních tvrzení práce) je formulováno nesmyslně.
- Jako jeden z konkrétních úkolů se v průběhu přípravy práce objevil požadavek jasně vysvětlit předpoklady na souvislost mezi dotazy na hashovací funkci a na podpisové orákulum a vliv těchto předpokladů na platnost důkazu. To není v práci provedeno uspokojivě. Není např. jasné, proč by útočník I měl dodatečně hashovat dotazy na podpisovací orákulum (str. 10). Podobně nejasná je formulace na str. 16.
- V důkazu Tvrzení 3.3.1 je nutné pracovat s nerovnostmi, nikoli s rovnostmi.
- Omezení z posledního řádku důkazu na str. 12 by si zasloužilo komentář (přísně vzato činí tvrzení neplatným).
- V důkazu Tvrzení 4.1.1 není komentována možnost, že algoritmus selže ve smyčkách „... **until** prvý bit u_i je 0“.
- V definice pravděpodobností na str. 18 jsou někde zaměněny hashovací požadavky a požadavky na podpis.

Přes uvedené výtky práce splňuje požadavky kladené na bakalářskou práci a doporučuji ji k obhajobě.

Praha 16. ledna 2012 Štěpán Holub