Posudek vedoucího na diplomovou práci Tomáše Kadlčka
Kryptografická schémata používající diskrétní logaritmus

Jak naznačuje název, práce představuje přehled využití problému diskrétního logaritmu v kryptografii. Po úvodu podává druhá kapitola seznam používaných základních matematických problémů souvisejících s umocňováním v dané grupě, jejichž obtížnost tvoří teoretický základ kryptografických schémat.

Třetí kapitola je velmi hutným exkursem do teorie eliptických křivek, jejím cílem je vysvětlit pojmy Tateovo a Weilovo párování. Tato kapitola svou obtížností převyšuje zbytek práce a může být čtenářem bez újmy na porozumění vynechána.

Čtvrtá kapitola obsahuje seznam schémat navržených v poslední době jako aplikace obtížných problémů popsaných ve druhé kapitole. Tomu předchází úvod do požadavků na bezpečnost těchto schémat.

Konečně pátá kapitola se vrací k základním matematickým problémům a ukazuje některé útoky na ně, tj. některé algoritmy, které dané problémy relativně úspěšně řeší.

Práce má převážně kompilační povahu. Student vypracoval práci zcela samostatně a za použití velkého množství literatury. Přínosem je přehledné zpracování témat roztroušených po kryptografické literatuře, známé svou ne zcela precizní formální úpravou, za použití jednotné terminologie. Student dále doplnil některé drobnosti, které jsou v literatuře vynechávány jako samozřejmé, ačkoli mohou působit nejasnosti. Vznikl tak skutečně použitelný přehled kryptografických aplikací diskrétního logaritmu.

Několik okolností zamýšlený účinek práce narušuje. Nejzávažnější z nich je toto:

- Nejednotnost terminologie v literatuře je jasně dokumentována skutečností, že Cheon ve svém článku [1], str. 3, definuje ℓ-silný Diffie-Hellmanův problém (ℓ-Strong Diffie-Hellmanův Problem, ℓ-SDH) jako problém, který je podle definicí studenta ekvivalentní s ℓ-slabým Diffie-Hellmanovým problémem (ℓ-Weak Diffie-Hellmanův Problem, ℓ-wDH). Cheonův ℓ-SDH je tedy něčím jiným než studentův. To není v diplomové práci vůbec uvedeno, což do značné míry znehodnocuje diskusi na str. 16 dole.
- Navíc to znamená, že použijeme-li terminologii diplomové práce, analyzuje Cheon navzdory názvu svého článku ℓ-slabý Diffie-Hellmanův problém, nikoli silný. Pokud mi něco neuniklo, je tedy Kapitola 5.1.3 zcela zavádějící. Celá záležitost je dosti matoucí, včetně otázky proč Cheon ignoruje velmi jednoduchou redukci uvedenou studentem v kapitole 2.5.

Další poznámky ke čtivosti:

- Práce kombinuje aditivní a multiplikativní notaci. Nevidím dostatečnou motivaci pro tento matoucí přístup, ačkoli je v úvodu na něj upozorněno.
- Student často přebírá anglickou terminologii a začleňuje ji do českého textu, což někdy působí poněkud barbarsky, např. „článek o traitor tracing schématu“, str. 11 dole. Tvrzení, že „označení Gap D-H groups už je [v češtině] zažité“ na str. 10 působí úsměvně vzhledem k tomu, že pojem byl v angličtině zaveden v roce 2001.
- Str. 12 nahoře: co je jednodušší problém?
- Nikde není řádně definováno, co znamená HIBE schéma, ani co je to prefix identity.

- Chce druhý odstavec na str. 25 prostě říct, že NM-CCA2 a IND-CCA2 jsou ekvivalentní?
- Výhoda útočníka na str. 26 by měla být definována jako pravděpodobnost vítězství minus $\frac{1}{2}$, nikoli prostě jako pravděpodobnost vítězství.
- Proč není kapitola 4.3 číslována jako podkapitola 4.2.16? Co v této kapitole znamená „klasická D-H dohoda“? Tento pojem nebyl definován.

Několik dalších drobností:

- „Computational Diffie-Hellman“ raději než „Computation Diffie-Hellman“, totéž pro decisional/decision.
- Str. 12, ř. 10: jejich ⟶ svého.
- Str. 14: jeden řádek výpočtu dvakrát zopakován.
- Str. 18, ř. 13 : tyto ⟶ tato.
- Str. 20, ř. 8 : doby ⟶ body.
- Str. 25, „dožaduje se podpisů“, nebo „dotazuje se na podpisy“.
- Str. 32, značení kolísá mezi C_K a C_M.
- Co znamenají tři tečky na druhém řádku kapitoly 5.1.3?

Celkové hodnocení. : Přes uvedené výhrady je text kvalitní a splňuje práce nároky na diplomovou práci.

Praha 2. září 2008

Reference

[1] Jung Hee Cheon. Security Analysis of the Strong Diffie-Hell
(Ed.): *EUROCRYPT 2006*, LNCS 4004, pp. 1-11, 2006.

navrhuji „výborně“