POSUDOK OPONENTA NA BAKALÁRSKU PRÁCU:
Monika Sayedová
Nová varianta Diffie-Hellmanova problému

Diffie-Hellmanov problém (DH) je výpočetný problém často využívaný v kryptografii, kde sa za predpokladu jeho zložitosti dokazuje bezpečnosť rôznych kryptografických primitív. V dôkazoch bezpečnosti niektorých asymetrických schém (napríklad v predloženej práci popísaný hash ElGamal) voči útočníkovi s volnou šifrového textu je ale nutný silnejší predpoklad - zložitosť DH problému pre útočníka s prístupom k rozhodovaciemu DH orákulu, tzv. silný DH predpoklad.

Predložená bakalárska práca je čisto kompilačná. Popisuje zdvojený Diffie-Hellmanov problém (2DH), uvádza vetu o ekvivalencii silného 2DH problému a DH problému a popisuje dve kryptografické schémy založené na 2DH spolu s dôkazmi ich bezečnosti v daných modeloch.

Z nedostatkov by som práci vytkol napríklad:

- 7. riadok abstraktu: Fráza „pri útoku vybraním zašifrovaného textu“ je trochu zavádzajúca. Bolo by vhodnejšie použiť štandardnú formuláciu „útok s volbou šifrového textu“.
- V úvode práce je viacero nejasných formulácii (napríklad strana 2, 5. riadok: „bezpečný pri nespoľahlivých kanáloch“, 14. riadok: „meniť správanie účastníkov“).
- Popis CCA útoku v druhom odstavci na strane 4 je málo zrozumiteľný.
- Pojem „adaptívne kladené otázky“ použitý napríklad v bode 2 na strane 5 nie je v práci vysvetlený.
- Problém diskrétneho logaritmu definovaný na strane 10 mohol byť uvedený v obecnejšom znení. Taktiež by bolo vhodné popísať vzťah medzi DH a problémom diskrétneho logaritmu.
- Strana 10, 12. riadok: Namiesto „Je veľmi pravdepodobné“, by bolo vhodné presne popísať prípady kedy nastane $\hat{m} = m$.

V práci sú uvedené dôkazy využívajúce tzv. bezpečnostné hry (napríklad dôkaz vety 6 na strane 20). Prosím, aby bol pri obhajobe stručne popísaný obecný princíp týchto dôkazov.

Až na drobné nedostatky je práca na dobrej úrovni a ukazuje, že autorka popisovanej problematike porozumela. Prácu preto doporučujem prijať ako bakalársku.

Praha, 15.6.2012 Michal Hojsík