Oponenstký posudok bakalárskej práce

Názov práce: Důkazy bezpečnosti schémat symetrické kryptografie
Autor: Marie Švarcová

Oponent: RNDr. Martin Hlaváč

Práca sa zameriava na dokazovacie metódy pre obecné schémy používané v symetrickej kryptografii. Dokazy nie sú závislé na konkrétnych voľbách symetrických šifier, či hašovacích funkcií. Sú preto hodnotné i v prípade, že základné stavebné kamene týchto schém sú prelomené. V takom prípade postačuje zameniť stavebný prvok za iný, vhodnejší a dôkazy bezpečnosti bez zmeny aplikovať na nové schéma.

Spracovanie zadanej témy z dostupných podkladov je kvalitné a dokazuje, že autorka problematiku plne pochopila. Problémy sú dobre definované, tvrdenia a vety jasne formulované a dokázané. Občas by sa hodil vlastný neformálny komentár, ktorý by čitateľa jasne uistil v jeho domnienkach, napr. že z uvedených schém šifrovania s ochranou integrity je metóda Encrypt-than-MAC jednoznačne najbezpečnejšia a prípadné využitie inej metódy by malo byť v danej situácii jasne zdovodnené.

Obecne je v texte veľmi málo preklepov, či iných drobných chýb, z ktorých vyberám nasledovné

- s. 6 (Pojmy) Základné požadované vlastnosti pre symetrické šifry sú vymenované (nerozlíšiteľnost, nepozmenitelnosť a integrita), nie je ale jasne uvedený ich význam. Z následného textu je ale čitateľovi jasný, keďže vyplynie z definície roznych hier, ktorými útočník na schéma útočí.
- s. 7 Označenie pravoľavého orákula ako LR sa može javiť mätúce.
- s. 10 Shoupove lemma je vyslovené bez referencie, ktorú by bolo vhodné pre čitateľa uviesť.
- s. 14 (koniec dokazu) Tvrdí sa, že útočník B položí rovnaké množstvo dotazov ako útočník A. To nie je pravda, pretože ak je hodnota prvého bitu šifrového textu rovná jednej, môže útočník B odpovedať „zadarmo“ bez dotazu na orákulum. Platnosť dokazu týmto nie je ovplyvnená.
- s. 17 (obecná kompozícia) Z definície sa môže javiť, že množiny kľúčov pre šifrovacie a autentizačné schémy sú zhodné. To však obecne nie je pravda, čo je uvedené napr. v úvode podkapitoly 3.2.
- s. 26 Skúmanie bezpečnosti EtM s WUF-CMA bezpečným MACom by bolo vhodné (ako všetky ostatné tvrdenia v práci) uviesť formou vety s dokazom.
- s. 30 (Definícia 1) Funkcia MAC_k nie je definovaná.

Spracovanie témy jednoznačne spĺňa požiadavky kladené na bakalársku prácu. Doporučujem ho preto prijať a hodnotím známkou

výborne

V Prahe, 20.6.2010