Rudolf Barczi: Důvěryhodnost prokazatelně bezpečné kryptografie
POSUDEK VEDOUCÍHO DIPLOMOVÉ PRÁCE

Předložená práce studuje důvěryhodnost prokazatelné bezpečnosti (*Provable Security*) na příkladě našich znalostí o bezpečnosti schématu OAEP, případně RSA-OAEP. Motivací k zadání této diplomové práce byla skutečnost, že jsou známy případy prokazatelně bezpečných, ale po své publikaci zlomených schémat. Další motivací byla snaha vyjasnit důvěryhodnost důkazů bezpečnosti na bázi náhodného orákula, případně jiných ideálních prvků. Se zúžením obsahu práce především na problematiku bezpečnosti OAEP jsem souhlasil vzhledem k náročnosti tématu, i vzhledem k tomu, že ve vývoji našich znalostí o bezpečnosti tohoto schématu se projevily všechny aspekty problematiky, kvůli kterým byla práce zadána. Jak plyne z motivace zadání, má tato práce kompilační charakter.

Za její nejdůležitější partie považuji ty, které se týkají důkazů bezpečnosti (RSA-)OAEP v modelu náhodného orákula a studium možnosti přechodu ke standardnímu modelu. Tvoří rovněž její převážnou část. Model náhodného orákula umožnil důkazy silných bezpečnostních vlastností efektivních schémat za poměrně slabých předpokladů, na druhé straně je za to zaplaceno kontraintuitivností těchto důkazů. To také vede ke vzniku psychologických bariér při jejich studiu a dále ke zvýšení rizika toho, že jsou chybné. V neposlední řadě zůstává stále otevřenou otázka jejich výpovědní hodnoty po záměně náhodného orákula prakticky použitelnou hašovací funkcí (tzv. *Instantialization*), tedy po přechodu k tzv. standardnímu modelu, který ideální prvky nepoužívá. Tuto problematiku považuji za velmi náročnou a jsem přesvědčen, že diplomant se jí zhostil se ctí.

Diplomová práce obsahuje jak výklad původního (chybného) důkazu bezpečnosti OAEP, tak i Shoupovy námitky a identifikaci chyby, které se autoři důkazu dopustili. Dále je v ní popsán korektní důkaz, který platí pouze pro „funkce jednosměrné na částech definičního oboru" (*Partial Domain One-Way Functions*) a je značně komplikovaný. Kvůli přehlednosti ho autoři zformulovali pomocí techniky „střídání her" (*Game Hopping*), přičemž vystřídali celkem 11 her (G_0 až G_{10}).

Za nejzajímavější a nejnáročnější část práce považuji její čtvrtou kapitolu věnovanou studiu bezpečnosti (RSA-)OAEP ve standardním modelu. Z hlediska dokazatelné bezpečnosti nejsou dosud známé výsledky příliš potěšující: V práci je vysvětlen důkaz nedokazatelnosti IND-CCA2 bezpečnosti OAEP (a podobných schémat) a to i při použití ideální jednosměrné permutace se zadními vrátky (místo RSA šifrování). Tvrzení „tím spíše platí" pro prakticky použitelnou permutaci. Doposud získané pozitivní výsledky jsou velmi slabé a naznačují, že bezpečnost schémat, dokázaná v modelu náhodného orákula, může být ve standardním modelu značně problematická. V práci je popsán nástin značně technického důkazu slabé neohebnosti při CPA útoku na OAEP po záměně obou orákul „reálnějšími objekty" (přechod do standardního modelu). Navíc byly pro důkaz požadovány velmi silné (ale v principu realizovatelné) bezpečnostní vlastnosti těchto „reálnějších objektů".

Práce rovněž obsahuje kapitolu věnovanou praktickým aspektům bezpečnosti RSA-OAEP. Je v ní vysvětlen problém nedostatečně přiléhavé redukce, důsledky použití nekvalitního generátoru náhodných čísel i implementační aspekty bezpečnosti související zejména s Mangerovým útokem na některé implementace.

K celkovému hodnocení diplomové práce: Má kompilační charakter, což je v souladu s jejím zadáním. Nejcennější jsou její nejrozsáhlejší části, kapitoly 2 a 4, které jsou rovněž značně technicky náročné. Posouzení problematiky důvěryhodnosti prokazatelné bezpečnosti na základě uvedených výsledků považuji za přínosné.

Doporučuji, aby práce byla uznána jako diplomová a hodnocena známkou VÝBORNĚ.

V Praze 9. 9. 2009

Bohuslav RUDOLF