Posudek vedoucího na bakalářskou práci

Ema Krejčová, Digitální peníze

Digitální peníze byly v kryptologii v módě zejména na počátku devadesátých let minulého století. Úkolem bakalářské práce Emy Krejčové bylo popsat základní kryptografické primitivy, které jsou v protokolech pro digitální peníze používány, uvést několik nejznámějších protokolů a vyjádřit se k jejich bezpečnosti. Práce v podstatě svůj účel splnila, pouze bezpečnost byla pojednána více než stručně.

V první kapitole jsou uvedené základní kryptografické jednosměrné funkce – diskrétní logaritmus a RSA funkce, dále něco málo o vlastnostech hašovacích funkcí a o symetrických a asymetrických šifrách. V některých okamžicích je popis až příliš volný, například u kolizí u hašovacích funkcí nejsou rozlišovány kolize prvního a druhého druhu, přitom rozdíl je důležitý např. pro platnost dřívějších elektronických podpisů v případě nalezení kolizí druhého druhu, tj. libovolných dvou vstupních vektorů, které mají stejnou haš. V takovém případě dřívější elektronické podpisy zůstávají i nadále v platnosti, neboť pro jejich popření je třeba k danému vstupu najít druhý vstup se stejnou hodnotou hašovací funkce.

Ve stručné druhé kapitole jsou uvedeni účastníci protokolů pro digitální peníze a ve čtvrté kapitole jsou uvedené různé požadavky, které jsou na tyto protokoly kladené.

Pátá kapitola obsahuje přehled kryptografických primitiv, které jsou pak v rozsáhlejší šesté kapitole používány ve třech základních protokolech pro digitální peníze. V páté kapitole je poněkud neorganicky v mírně stručnější podobě v části 5.4. uveden celý protokol, který je pak v šesté kapitole znovu podrobněji popsán v části 6.1. Šestá kapitola podle mého dost trpí tím, že autorka pouze uvádí, jaké vlastnosti každý z navržených protokolů má mít. Tyto vlastnosti v některých případech vyplývají z exaktních matematických úvah, které jsou založené na definicích základních primitiv, autorka však tyto exaktní úvahy povětšinou pomíjí.

Šestá kapitola končí krátkou poznámkou o osudu prvních firem, které se pokoušely prosadit s konceptem digitálních peněz a uvádí současnou situaci, která nepotvrzuje původní optimistické představy o možnostech rozvoje digitálního peněžnictví.

Sedmá kratičká kapitola pak v podstatě pouze konstatuje, že bezpečnost protokolů pro digitální peníze nebyla nikdy dokázána.

Práce splnila svůj účel, poskytla ucelený přehled o současném postavení digitálních peněz, o základních návrzích a požadavcích. Jedinou větší vadou je absence rigoróznějšího přístupu zejména v páté a šesté kapitole, zejména absence důkazů i v místech, která jsou obvykle v serióznější literatuře dokazována.

Práce určitě splňuje požadavky kladené na bakalářskou práci a navrhuji hodnocení

V Praze, 6.9.2006

Doc. RNDr. Jiří Tůma, DrSc.
Vedoucí práce