# POSUDEK OPONENTA NA BAKALÁŘSKOU PRÁCI: *EMA KREJČOVÁ, DIGITÁLNÍ PENÍZE*

Práce představuje systémy pro elektronickou realizaci (více či méně) anonymního oběhu peněz. Obsahuje přehled některých matematických nástrojů, popis základních kryptografických primitivů a protokolů a nakonec přehled tří v literatuře navržených systémů.

Práce trpí dvěma základními obecnými problémy, které spolu vzájemně souvisí:

1. Autorka nerozlišuje dostatečně mezi různými vrstvami problematiky: matematickými tvrzeními, kryptografickými primitivy, protokoly a obecnými úvahami. To je charakteristický nešvar popularizačního přístupu ke kryptografii, kterému by se měla odborná práce pokud možno vyhýbat. Bakalářská práce by se měla podle názoru oponenta zaměřit na porozumění a srozumitelné představení základních principů dané problematiky, spíše než na opisování komplikovaných detailů jednotlivých protokolů z literatury.

2. Tvrzení s matematickým obsahem jsou často formulována nejasně. I tam, kde je možný korektní výklad, není jisté, zda autorka má tento výklad na mysli.

*Konkrétní výtky:*

- s. 6 a s. 7. Popis pojmu *jednosměrná funkce*: Není výslovně řečeno, že není známo, zda jednosměrné funkce existují, není ani zmíněna souvislost s problémem P $\stackrel{?}{=}$ NP. Definice je korektní pouze pro injektivní funkce, protože invertující algoritmus je úspěšný, pokud nalezne libovolné $y \in f^{-1}(x)$.

  Zatímco nejasnost ohledně pořadí kvantifikátorů v definici zanedbatelné funkce je ještě možno považovat za nedbalost, v definici jednosměrné funkce už lze tvrdit, že je chybné.
- Definice diskrétního logaritmu je neobratná, opakuje dvakrát totéž.
- s. 7 c). „Z toho plyne, že $x^{ed} = x \mod n$": Má to čtenář vidět?
- s. 7: Vztah mezi invertováním RSA a faktorizací je popsán velmi chaoticky (nepravdivé tvrzení je dodatečně zpochybněno v následujícím odstavci).
- „Bezkolizní hašovací funkce je jednosměrná": To je v rozporu s výše uvedeným faktem, že jednosměrná funkce je definována jen pro injektivní funkce. Pokud se definice opraví, má být toto tvrzení zřejmé?
- s. 8 dole: Mělo by být řečeno, že „zadními vrátky" je klíč $s_B$ a že k tomuto klíči existuje funkce $F'_{s_B}$, která je (se znalostí $s_B$) polynomiální a je inverzní k $F_{v_B}$.
- s. 9: protokol není „záznam" o kommunikaci, ale seznam pravidel, podle kterých kommunikace probíhá.
- Kapitola 5, *Metody a procedury*: Definice pojmů by si zasloužily větší přesnost. Měl by se jasněji oddělit požadavek na funkci primitivu (např. digitálního podpisu) a návrhy na realizaci konrétními protokoly (v ideálním případě s uvedením předpokladů pro správnost protokolu).
- odstavec „Bitový závazek pomocí symetrické kryptografie" na s. 14 je nesrozumitelný. Postup je rozhodně chybný pro některé symetrické šifry (např. pro jednorázový klíč - one time pad).
- „cut and choose" znamená „jeden půlí, druhý volí", nikoli „jeden půlí, druhý dělí" (chybný překlad se opakuje v celé práci). Především ale metoda není popsána, namísto toho je uvedeno její použití v konkrétních protokolech pro elektronické peníze.

- Rovněž oddíl 5.5 „Jednoduchá mince“ vybočuje ze seznamu primitivů. Naopak by tam patřil nahodilý podpis, který je zařazen pod 5.5.
- Směšováním různých úrovní výkladu je také věta na s. 17 dole: „...každá mince obsahuje mnoho informací - kvůli zachování anonymity a bezpečnosti obsahuje mnoho identifikačních řetězců zákazníka, které určují směrnice přímek.“ O jakých přímkách je tu řeč?
- Řadu nepřesných, spíše žurnalistických formulací obsahuje závěrečná kapitola o bezpečnosti (faktorizace např. není „obtížně invertovatelná funkce“). Především by měla být jasněji vyložena myšlenka dokazování bezpečnosti pomocí redukce, která je pro matematické pojetí bezpečnosti klíčová, jakož i důvod, proč je takto dokázaná bezpečnost nedostatečná (to úzce souvisí s výše zmíněným neuspokojivým výkladem o RSA na straně 7).

**Celkové hodnocení.** Domnívám se, že předložená práce se pohybuje na hranici požadavků kladených na bakalářskou práci. Doporučuji ji přijmout s hodnocením *dobře*.

Praha 6. září 2006

Štěpán Holub