Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

POSUDEK OPONENTA DIPLOMOVÉ PRÁCE

Student: **Bc. David TŘÍSKA** **Oponent:** **Doc. Karel BURDA, CSc.**

Studijní program: **Inženýrská informatika**
Studijní obor: **Informační technologie**
Akademický rok: **2010/2011**

Téma diplomové práce: **Ochrana utajovaných informací pomocí kvantové kryptografie**

Hodnocení práce:
Zadání diplomové práce bylo aktuální a poměrně obtížné. Obtížnost zadání spočívala v nedostatku a v převážně vědeckém charakteru dostupné literatury. Požadavky zadání byly splněny.

Diplomant zadání práce vyřešil tím, že prostudoval dostupnou literaturu, konzultoval problematiku se specialisty a následně získané poznatky shrnul, utřídil a zobecnil. V této souvislosti oceňuji snahu autora získat maximum informací k dané problematice.

Práce pokrývá všechny významné části kvantové kryptografie. Přínosem diplomanta je skutečnost, že v práci poukázal na specifika, která aplikaci kvantové kryptografie v praxi dosti zužují (s. 46-47). Tato specifika nejsou v odborné literatuře prakticky vůbec uváděna.

Nedostatkem práce je skutečnost, že některé složitější aspekty (například qubit na s. 23) jsou popsány dosti povrchně. Autor také často v textu nevysvětluje obrázky (např. obr. 8 na s. 15). V práci se rovněž vyskytují drobné chyby. Autor například uvádí jednu možnou reprezentaci hodnot bitů pomocí polarizace fotonů v tab. 2 na s. 38 avšak u obr. 16 na s. 40 z neznámých důvodů používá reprezentaci přesně opačnou. Popis protokolu BB84 na s. 42 je poněkud matoucí a není zcela přesný. Autor například v prvním kroku protokolu nezdůrazňuje, že Alice nejprve vygeneruje náhodnou posloupnost bitů a že při jejím vysílání náhodně mění polarizační bázi. Ve třetím kroku informuje o posloupnosti polarizačních bází Bob a nikoliv Alice, atd.

Po formální stránce je práce na dobré úrovni. Za jediné významnější nedostatky považuji některé nekvalitní obrázky (např. obr. 15 na s. 38), nadměrnou velikost rovnic (např. s. 27) a občas chybějící odkazy (např. tvrzení v posledním odstavci na s. 24 je bez odkazu).

Dotazy k obhajobě diplomové práce:
1. Proč v protokolu BB84 informuje o posloupnosti použitých bází Bob?
2. Může být soudobá kvantová kryptografie provozována bez podpory klasické kryptografie?

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Celkové hodnocení práce:
Známku uvede vedoucí dle svého uvážení dle klasifikační stupnice ECTS:
A – výborně, B – velmi dobře, C – dobře, D – uspokojivě, E – dostatečně , F – nedostatečně.
Stupeň F znamená též „nedoporučuji práci k obhajobě“.

Předloženou diplomovou práci doporučuji k obhajobě a navrhuji hodnocení

B - velmi dobře.

V případě hodnocení stupněm „F – nedostatečně“ uveďte do připomínek a slovního vyjádření hlavní nedostatky práce a důvody tohoto hodnocení.

Datum 25.5.2011 Podpis oponenta diplomové práce