Posudek vedoucího na diplomovou práci Martiny Válkové
Útoky založené na hardwarových chybách.

Práce rozebírá možnost netradičního útoku na některé bezpečnostní protokoly založeného na využití hardwarové chyby známé útočníkovi, ale nikoli držiteli klíče.

Myšlenka je převzata z literatury a je založena na hardwarových předpokladech, které nelze zcela vyloučit. Přesto se zřejmě jedná spíše o cvičnou hypotézu, kterou ovšem autorka analyzuje velmi pečlivě a s ohledem na praktické aspekty jejího možného využití. Zabývá se také možnostmi obrany proti takovému útoku.

Uchazečka pracovala na práci velmi samostatně. Její přínos spočívá v detailním upřesnění útoku ve výchozím článku pouze naznačeného a v analýze praktických ohledů implementace, pravděpodobnosti úspěchu útoku i některých jednoduchých otázek na úrovni práce procesoru. Teoretické výsledky byly také ověřeny softwarovou simulací. Matematická stránka práce je obsažena ve druhé kapitole a týká se výpočtu odmocnin v multiplikativní grupě $\mathbb{Z}_p^*$.

Nakolik mohu posoudit, zvládla autorka otázky související s hardwarovou implementací modulárního mocnění velmi dobře, její výklad je suverénní. To neplatí beze zbytku o části matematické, kde některé výklady působí trochu těžkopádně, a některé trochu začátečnicky až středoškolsky. Příkladem může být formulace Čínské věty o zbytcích (str. 12) nebo důkaz faktu, že $\alpha^i = \alpha^j$ implikuje v multiplikativní grupě $i = j$ (v důkazu Tvrzení 2.1.2, str. 16). Lituji, že se mi nepodařilo přesvědčit diplomantku o výhodách aditivního zápisu cyklické grupy. Domnívám se, že např. důkaz Tvrzení 2.1.3 by byl v aditivním zápisu průhlednější. Příliš laicky je mimo jiné podáno vysvětlení pojmu *těžký problém* na str. 25.

Práce je psána s minimálním počtem překlepů a je až na drobné výjimky (např. „kroce" namísto „kroku") jazykově povedená. V popisech útoků je někdy výklad příliš neformální, je např. nejasné, co znamená důkaz (resp. důkaz správnosti) problému (str. 53, 57). Je to důkaz správné identifikace problému, nebo důkaz správnosti jeho řešení? Nebo oboje?

Práci celkově považuji za zdařilou a doporučuji ji k obhajobě.

Praha 25. ledna 2011

Mgr. Štěpán Holub, Ph.D.