Posudek oponenta na diplomovou práci Petra Sušila
Nové návrhy hashovacích funkcí.

Práce psaná v angličtině se zabývá útoky na některé hashovací funkce.

Po stručném úvodu do problematiky v prvních dvou kapitolách se autor blíže zabývá ve třetí kapitole dvěma konkrétními hashovacími funkcemi používanými v autentizačních schématech. První z nich je funkce COMP-128 používaná v GSM technologii. Autor představuje dva útoky popsané v literatuře, které měly i jistý ohlas ze strany provozovatelů sítí GSM. Druhou je zbrusu nová hashovací funkce SQUASH, představená letos. Poslední kapitola shrnuje některé obecné principy útoků na libovolné hashovací funkce.

Práce vychází ze znalosti poměrně rozsáhlé literatury včetně, jak bylo řečeno, publikací zcela nedávných.

Hodnocení je třeba začít kritikou formálního zpracování práce. Chybí přehledný úvod i závěr, takže čtenář neví, co má od textu čekat. Práce má velmi neformální gramatickou (např. dosti nahodilé používání velkých písmen na začátku věty) i grafickou úpravu (autor z oponentovi neznámých důvodů používá velmi nezvyklý formát).

Závažnější je ovšem heslovité a selektivní zavádění pojmů. Výsledek se místy blíží situaci, kdy porozumět může jen ten, kdo již předem dobře věděl, o čem je řeč. Namátkou několik příkladů:

- Odstavec na str. 6 začínající *it is hard*, nedává dobrý smysl, zejména ne věta (?) obsahující „then". Pokud sdělení porozumíme, stále ještě chybí informace, že údaje o potřebném počtu dotazů jsou *průměrné* (resp. *očekávané*).
- Schémata konstrukcí kompresních funkcí na str. 11 nemají bez komentáře prakticky žádnou vypovídací hodnotu.
- V popisu VSH algoritmu není jasné, co jsou čísla p_i.
- Funkce VSH na str. 14 je zadána pouze pseudokódem algoritmu, bez jakéhokoli komentáře.
- Na straně 16 není definováno $x \wedge y$ a $x \vee y$.

Nejlépe čitelná je kapitola 4.

Vzhledem k nedostatku komentáře je také nutné se dohadovat, co je přínosem autora a co je pouze převzato z literatury. Často opakovaná věta „reader should refer to ..." sice upozorňuje na relevantní literaturu, ale to otázku na přínos studenta bez rozsáhlého studia nezodpovídá.

Např. jsem ověřil, že první část oddílu 2.5.2 je z článku [10] (dlužno přiznat, že řádně citovaného) přebrána zcela doslova, včetně poněkud nesrozumitelného „if any", s doplněným překlepem „through" $\rightarrow$ „though".

Naopak následující poměrně pěkné dovysvětlení důkazu je zřejmě vlastní (opět jen dohad).

Nejcennější se zdá být analýza některých potenciálních slabin hashovací funkce SQUASH, která byla navržena Adi Shamirem na únorovém workshopu Fast Software Encryption 2008 (FSE, nikoli FCE, str. 27). Autor podrobně analyzuje útok na tajný klíč za předpokladu nevhodné volby tzv. směšovací (mixing) funkce. Postup je poměrně elementární, ale ve svém celku rozhodně netriviální. Detaily důkazu jsem neověřoval, slibovanou implementaci jsem na přiloženém CD nenašel.

Celkové hodnocení. : Autor prokázal schopnost pracovat s literaturou i schopnost sám reagovat na aktuální podněty. Práce splňuje požadavky na diplomovou práci.

Hlavním nedostatkem práce je nedbalé a čtenářsky nepřívětivé zpracování.

Navrhuji známku *velmi dobře.*

Praha 31. srpna 2008

Mgr. Štěpán Holub, Ph.D.

[redacted]

Navrhuji „velmi dobře"