Posudek vedoucího diplomové práce

Petr Sušil, Nové návrhy hašovacích funkcí

Práci lze rozdělit zhruba do tří částí. První část (kapitoly 1 a 2) lze číst jako úvod do kryptografických hašovacích funkcí. Autor uvádí bezpečnostní požadavky na tyto funkce a nejčastěji používaný způsob jejich konstrukce z kompresní funkce doplněné o zesílení (Davies-Meyerovo nebo Miaguchi-Preneelovo) pomocí zesíleného Merkle-Damgardova zřetězení (jeho zesílení spočívá v přidání jednoho bloku ke zprávě, který předepsaným způsobem obsahuje informaci o délce zprávy). Základním konstrukčním kamenem každé hašovací funkce tak je kompresní funkce, která ze dvou vstupů – bloku pevné délky a inicializačního vektoru – vytvoří výstup délky inicializačního vektoru. Základním požadavkem na kompresní funkci je, aby fungovala jako náhodné orákulum.

Autoři navrhují hašovací funkce na základě vlastních zkušeností s využitím obecných principů symetrické kryptografie a bez velké teorie. Autorovo pojetí je obvyklé v kryptografii a informatice. Na některých místech by slušela o dost větší pečlivost formulací. Také v angličtině je řada nedostatků.

První část je zakončena příklady několika hašovacích funkcí. V současné době se objevuje řada návrhů nových hašovacích funkcí v souvislosti s celosvětovou soutěží o návrh nového hašovacího standardu, autor musel provést velký výběr.

V druhé části je zkoumána bezpečnost dvou hašovacích funkcí – COMP128 a SQUASH. První byla používána v mobilních sítí k autentizaci telefonu do sítě. Odhalené slabiny, které autor převzal z literatury, vedly k její změně. Druhou zkoumanou funkci představil Adi Shamir na konferenci FSE2008 počátkem tohoto roku, je určena k použití na RFID čipech. Část o SQUASH je velmi cenná, autor vysvětluje, proč je návrh formulovaným právě tímto způsobem, popis doprovází názornými obrázky (podobně jako u popisu COMP128). Adi Shamir ve svém článku důvody pro danou konstrukci často pouze naznačuje. Zkoumání bezpečnosti SQUASH vychází z drobné poznámky v článku Afino Shamira, že použití lineárního posuvného registru (v návrhu ve použit nelineární) by nebylo bezpečné, jak důmyslným argumentem ukázal Serge Vaudenay. Autorovi práce se podařilo slabinu použití lineárního posuvného registru ukázat. Tato část je psána přesným matematickým stylem, důkazy jsou správně.

Závěrečná třetí část je věnována generickým útokům na hašovací funkce ukazující neodstranitelné slabiny Merkle-Damgardova zřetězení. Hašovací funkce založené na tomto zřetězení se nechovají jako náhodné orákulum ani v případě, že samotná kompresní funkce tuto vlastnost má. Zde autor vychází z literatury, vlastní přínos je minimální.

K práci nemám zásadní připomínky, hlavní kritiku je třeba směřovat ke způsobu podání první části a k angličtině. Vlastní přínos ke studiu návrhu funkce SQUASH je výrazný.

Práce bohatě naplňuje požadavky kladené na diplomovou práci a proto ji navrhuji uznat jako diplomovou a hodnotit známkou

Výborně