Oponentní posudek disertační práce

Využití algebraických a kombinatorických metod při studiu hašovacích funkcí

Autor práce, RNDr. Daniel Joščák předloženou disertaci sestavil ze tří článků přijatých k prezentaci na prestižních kryptologických konferencích, doplněných kapitolou o obecné problematice diferenční kryptoanalýzy rovnic typu „AX". Posudek se bude následně postupně věnovat každé z těchto kapitol.

Rovnice kombinující operace modulárního součtu celých čísel a operace XOR (eXclusive OR) binárních reprezentací celých čísel označujeme v kryptografii jako AX (čili ADD-XOR). Rovnice AX jsou v teoretické i aplikované kryptografii oblíbenými stavební bloky současných algoritmů. Je to jednak díky jejich snadné a rychlé realizaci v HW na jedné straně, jednak díky solidním vlastnostem nelinearity a difuze – definice jsou zde pro přehlednost vynechány – na straně druhé. Hledání řešení či rozhodování o řešitelnosti rovnic AX má v současné kryptologii zásadní význam, neboť tato úloha úzce souvisí s útoky založenými na takzvané diferenční kryptoanalýze.

Autor předložené práce v první kapitole popisuje přehlednou algebraickou platformu pro studium rovnic AX. Konkrétně se přitom zaměřuje na tvary AX, které se často vyskytují v teoreticky významných kryptografických algoritmech současnosti. Svou uceleností se jedná o ojedinělou studii tohoto druhu, která jistě najde uplatnění a odezvu u návrhářů i analytiků bezpečnostních algoritmů.

Druhá kapitola předložené práce prezentuje prolomení určitého typu zodolnění obecného schématu Merkle-Damgård, o kterém se nějaký čas uvažovalo jako o efektivní „záplatě" dříve prolomené funkce MD5. Předložený obecný útok ukázal, že zodolnění označované konkrétně jako 3C a 3C+ nemůže samo o sobě napravit slabiny dané kompresní funkce. Popsaný útok je kromě obecného důkazu dále předveden v konkrétní podobě na hypotetickém posílení funkce MD5. Celkově lze výsledky prezentované v této kapitole označit za velmi významné pro další směrování teoretické kryptografie.

Ve třetí kapitole autor vypracoval nástroj pro porovnání složitosti tří, svým způsobem populárních algoritmů pro hledání kolizí hašovací funkce MD5, přičemž jeden z těchto algoritmů pochází přímo z diplomové práce autora. Srovnávací model dovedně kombinuje přístupy obecné teorie složitosti s pravděpodobnostními modely obvyklými ve finanční matematice (cena, střední hodnota nákladů, atp.). Díky této kombinaci jsou výsledky porovnání jednak rigorózní, jednak prakticky snadno interpretovatelné. Další část této kapitoly rezonuje s předchozím útokem na zodolnění typu 3C a 3C+, kde autor prezentuje v jistém smyslu doplněný pohled na využití obecného útočného algoritmu k prolomení schématu 3C s kompresní funkcí dle MD5. Vzhledem k významnosti obecného postupu popsaného v kapitole číslo dva je toto doplnění velmi užitečné. Nakonec je zde předveden ještě útok na další, dříve zamýšlené zodolnění označované jako SFRI/MFRI (Single/Multiple Feedback Ring-Iterative). Celkově lze uvést, že tato kapitola nahlíží problematiku hledání kolizí MD5 a příbuzných schémat z několika úhlů, přičemž výsledky jsou velmi užitečné pro další výzkum i výuku nových talentů v oblasti kryptologie.

V poslední kapitole autor ukazuje nový typ dvoublokové kolize pro MD5. Pro její nalezení byly zkombinovány dva trendy ve výzkumu zranitelností MD5 – akcelerace stávajících postupů a hledání nových diferenčních cest pro nové typy kolizí. Tím příspěvek vhodně rozšiřuje jak poznání o funkcích typu MD5, tak i o vlastnostech algoritmů, které byly sestaveny k jejímu prolomení.

Závěrem posudku si dovoluji připomenout, že tři ze čtyř výše popsaných kapitol (konkrétně kapitola druhá, třetí a čtvrtá) byly v podobě samostatných článků prezentovány na prestižních mezinárodních vědeckých konferencích o kryptologii, což evidentně podtrhuje význam jejich obsahu.

Celkově práci hodnotím jako vynikající díky jejímu hlubokému a zároveň ucelenému záběru. Prolomení funkce MD5 je v kryptologii epochální skutečností, která s sebou bohužel nutně přinesla i řadu nejasných výroků a unáhlených závěrů. To ji v důsledku učinilo z dnešního pohledu poněkud nepřehlednou. Předložená disertační práce přitom zcela zásadně přispěla k vyjasnění a prohloubení poznatků, které si jako kryptologové můžeme z celé této události odnést.

Podle mého názoru práce jednoznačně prokazuje předpoklady autora k samostatné tvořivé práci.

Vypracoval: Ing. Tomáš Rosa, Ph.D.

Praha, 26. srpna 2015