Oponentský posudek na bakalářskou práci

Adolf Středa: MQ problém

Práce se zabývá možností využití obtížnosti problému řešení soustavy kvadratických rovnic v kryptografických protokolech. Jedná se sice o NP úplný problém, ale to samo o sobě vhodnost pro asymetrickou kryptografii nezaručuje. Je třeba jednak zajistit generování náhodných těžkých instancí problému a na druhé straně umožnit za přítomnosti dodatečné informace (privátního klíče) tyto problémy naopak řešit efektivně. Jako řešení druhého z problémů jsou v literatuře navrženy varianty tzv. HFE (Hidden Field Equations) protokolu, ve kterém se systém kvadratických rovnic nad konečným tělesem zakóduje do polynomu v jedné neurčité nad tajným rozšířením tohoto tělesa.

Těžištěm práce je kromě základních fakt o MQ problému a HFE protokolech popis útoků na varianty HFE. U základní varianty HFE je zmíněn Kipnisův a Shamirův útok využívající faktu, že matice kvadratické formy používané polynomiální transformace má typicky nízkou hodnost, a též je nastíněn Faugèrův a Jouxův útok pomocí Gröbnerových bází. Hlavní pozornost je pak věnována Felkeho útoku na modifikaci HFE, při které se z kvadratické polynomiální transformace vyextrahuje opět matice příslušné kvadratické formy a problém se za pomoci Felkeho hypotézy převede na útok na základní verzi HFE.

Práce bezpochyby splnila zadání a je dobře pochopitelná, leč ke zpracování mám určité připomínky. Autor často jakoby předpokládal, že čtenář problematiku související s MQ problémem už zná. Některé věci jsou pak vysvětlovány pouze povrchně nebo alespoň ne od začátku. I když to možná nebylo těžištěm práce, vadila mi i přílišná povrchnost kapitoly 3. Hlavně konec části 3.2 je dosti uspěchaný a člověk se po slibném začátku nedozví, jak útok dokončit.

V práci se též vyskytují různé menší nepřesnosti a nekonzistence v používaných pojmech, které ubírají na srozumitelnosti. Ačkoli si dovedu představit, že těmito neduhy trpěly i používané zdroje, je škoda, že autor nevyužil příležitosti k jejich nápravě. Uvádím seznam konkrétních míst v textu:

1. V definici v kap. 1.2 je afinní transformace definována jako *bijektivní* zobrazení. V následujícím textu (v důkazu lemma 1.7, ale i jinde) je občas na tuto podmínku bez komentáře rezignováno. Možná by bývalo lepší definovat afinní zobrazení bez podmínky, že jde o bijekci, a bijektivitu vyžadovat jen tam, kde je opravdu třeba.

2. Formulaci „Nechť tedy máme systém $m \in \mathbb{N}$ rovnic .... Pak uvažme polynomy ...“ na začátku str. 6 považuji za matoucí.

3. Dosti nesrozumitelná mi přijde manipulace s ekvivalencí v kap. 2.1. Z použití dále je jasné, že polynomiální transformace z $\mathcal{MQ}(\mathbb{F}^n, \mathbb{F}^m)$ chceme považovat za ekvivalentní, pokud definují stejná zobrazení z $\mathbb{F}^n$ do $\mathbb{F}^m$. Definice se součtem koeficientů u $x_i x_j$ a $x_j x_i$ nedává moc smysl, protože pak jde o stejný vektor polynomů (protože $x_i x_j = x_j x_i$ v $\mathbb{F}[x_0, \dots x_{n-1}]$).

   Ještě více matoucí je situace u HFE polynomů. Tam by správná definice rovněž byla, že určují stejná zobrazení $\mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$. Ekvivalence se součtem koeficientů tak, jak je definována, opět nedává smysl v tom, že se v ní sčítají koeficienty u stejné mocniny X. Co naopak není ošetřeno, jsou relace $X^{q^n} \sim X$ (mocniny q v exponentech nejsou v definici HFE polynomu omezeny) a to, že pro $q = 2$ je $X^{q^i} + X^{q^i}$ vlastně lineární člen. V dalším textu jsou tyto vlastnosti pochopitelně používány.

4. To, co je v důkazu lemmatu 2.3 prezentováno jako důkaz jednoznačnosti, je spíš důkaz dobré definovanosti. Opravdový důkaz jednoznačnosti by měl obsahovat podobnou úvahu jako na konci důkazu lemmatu 1.7, tj. že nenulový polynom nad $\mathbb{F}_{q^n}$ stupně menšího než q^n nemůže být na $\mathbb{F}_{q^n}$ identicky nulový.

5. Formulace „Pro náhodné koeficienty $T_0, \dots, T_{n-1}$ bude očekávaná hodnost bilineární formy $WPW^\intercal$ velice blízká n“ na str. 14 mi přijde matoucí, neboť podle popisu výše $WPW^\intercal$ nezávisí na $T_0, \dots, T_{n-1}$.

6. Popis HFEz v kap. 4.1 není úplně dobře srozumitelný. Nejdříve se píše, že afinní transformace jsou nově nad $\mathbb{F}^{n+m}$, posléze se ukáže, že pouze jedna z nich. Jelikož jde pro další o klíčový pojem, přesnější popis pro neznalé by hodně pomohl. Z poznámky o porovnání s variantou HFEv, která nebyla nikde jinde ani slovem zmíněna, si nezasvěcený člověk rovněž příliš neodnese.

Na závěr si dovolím zapolemizovat z tezí ze závěru, že separace větví využívá poznatky o neasociativních algebrách. Možná Felkeho hypotéza využívá určitou intuici a definici centralizátoru, ale jinak je podle mého využita hlavně $\mathbb{F}_q$-bilinearita těchto binárních operací. Tady jde pouze o můj názor bez jakéhokoli vztahu k hodnocení práce.

Práci **doporučuji k obhajobě** a hodnocení přikládám zvlášť.

V Praze dne 20. 6. 2016 doc. RNDr. Jan Šťovíček, Ph.D.