Posudek

oponenta diplomové práce.

Autor: p.Marcel Šebek

Název práce: Deniable encryption

Jméno oponenta: Jan Krajíček

Matematická úroveň: velmi dobrá

Grafická, jazyková a formální úroveň: vynikající

Výsledky: původní i převzaté

Použité metody: standardní

Aplikovatelnost: nedovedu posoudit

Věcné chyby: téměř žádné

Tiskové chyby: téměř žádné

Celková úroveň práce: vynikající

Práci doporučuji uznat jako diplomovou. Návrh klasifikace přikládám na zvláštním papíru.

Připomínky a vyjádření oponenta:

Práce p.Šebka se zaobírá různými schématy tzv. popiratelného šifrování. Shrnuje a srozumitelně předkládá několik hlavních výsledků v této oblasti. Různá schémata vysvětluje ve společné formalizaci, což je užitečné pro jejich přímé porovnání.
Důležité myšlenky jsou vyloženy velmi pěkně a pečlivě a práce se dobře čte.

Pan Šebek též předkládá (v kap.2) vlastní modifikaci tzv. flexible-deniable schématu z práce [OPW11], v níž je vzájemný vztah parametrů konstrukce jiný než v původní konstrukci a která tedy v principu umožňuje jejich jiná nastavení (trade-off).
Pan Šebek též našel chybu v důkazu vlastností konstrukce tzv. fully-deniable schématu v [BNNO11] a poukázal na potenciální obtíže s její opravou (kap.2).

Hlavní těžiště práce je v kap.2, ale zbylé 3 kapitoly (byť velmi krátké, dohromady ani ne polovina rozsahu 2.kap.) obsahují též zajímavý materiál. Kap.3 na 3 stránkách stručně nastiňuje konstrukci tzv.plan-ahead a steganographic schémat založených na diskrétním logaritmu, v 5.kap. je podobně stručně (2 str.) pojednáno tzv. steganographic data storage; ani jedna z těchto dvou kapitol neobsahuje nějaké formální tvrzení.

Z těchto tří stručných kapitol je - aspoň pro mne - nejzajímavější 4.kap. pojednávající o konstrukcích využívajících tzv. lattice-based šifrování.

Domnívám se, že p.Šebek napsal velmi zdařilou diplomovou práci. Osobně bych uvítal, kdyby bylo více prostroru věnováno schématům z kap.3 a 4: schémata z kap.3 jsou zmíněna na str.59 jako nejpraktičtější a konstrukce nastíněná v kap.4 je zase matematicky nejhlubší. Při obhajobě by p.Šebek mohl pohovořit o problémech a nápadech, které zmiňuje v Remark 4.6 (str.56).

Místo, datum, podpis oponenta:

5.září 2012, Praha