Oponentský posudek bakalářské práce

Marek Zpěváček: Audiovizuální kryptografie

V práci Marka Zpěváčka je představena audiovizuální kryptografie, což je část kryptografie, která se zabývá rozdělením (tajné) zprávy mezi několik účastíků tak, aby bylo možné tuto zprávu zkrekonstruovat z předem daného počtu částí jen za pomoci zraku či sluchu.

Práce je rozdělena na čtyři části. V první jsou zavedeny definice a dokázáno klíčové tvrzení pro šifrování černobílých obrázků. Ve druhé jsou představena čtyři konkrétní schémata včetně důkazů jejich bezpečnosti a správnosti rekonstrukce. Ve třetí jsou pak obecné konstrukce schémat (opět s důkazy). V poslední kapitole je pak zlehka naznačeno rozšíření pro šifrování zvuku a obrázků v odstínech šedi.

Práce má charakter spíše kompilační, text vychází převážně z článků *Visual cryptography* od Naora a Shamira a *New results on visual cryptography* od Drosta. Doplňuje je ale o detailní důkazy všech lemmat a tvrzení; některé definice jsou zobecněny. Právě doplnění důkazů ke tvrzením (Tvrzení 4, Lemma 3), které v literatuře nejsou dokázány, považuji za hlavní přínos práce. Ve formální úpravě práce jsem žádné nedostatky nenašel.

Jediné, co práci mohu vytknout je její krátkost (18 stran čistého textu) a nevyužití plné obecnosti nových definic. Definice byly rozšířeny na obecné přístupové struktury a libovolná pravděpodobnostní rozdělení, ale všechna tvrzení a lemmata byla dokázána pouze pro rovnoměrné rozdělení a nejjednodušší přístupové struktury.

Během prezentace by student mohl vysvětlit jak vzniklo $(4, 4)$-schéma z části 2.4. To má parametry $(m = 9, d = 9, \alpha = 1/9)$, ale konstrukce obecných (k, k)-schémat ze sekce 3.1 poskytuje parametry $(m = 8, d = 8, \alpha = 1/8)$.

Navrhuji, aby práce byla přijata jako práce bakalářská a hodnocena stupněm *velmi dobře*.

V Praze dne 20. června 2016 Milan Boháček