Posudek vedoucího diplomové práce

**Jana Kučerová, Řešení soustav diferenčních rovnic pro sčítání a booleovské operace**

Práce se zabývá zobecněním algoritmu pro řešení jisté rovnice obsahující dvě grupové operace na binárních posloupnostech délky $n$ - operaci $xor$ a operaci modulárního sčítání modulo $2^n$. Tuto dvojici operací nazývá standardní grupový pár. Vzájemný vztah těchto operací je základem mnohých algoritmů pro symetrickou kryptografii.

Polynomiální algoritmus pro nalezení všech řešení rovnice

$$(x \; xor \; \alpha) + (y \; xor \; \beta) = (x+y) \; xor \; \gamma$$

kde $\alpha, \beta, \gamma$ jsou parametry, umožnil autorům Paulovi a Preneelovi oslabit proudové šifry jistého typu.

Autorka se v práci zabývá existencí polynomiálního algoritmu v obecnějším případě, kde místo operací xor a modulárního sčítání vystupují libovolné dvě abelovské grupové operace.

Za hlavní výsledky práce považují charakterizaci vzájemné polohy obou operací xor a + - Věta 2.7., popis všech možných hustých abelovských párů v Tvrzení 4.18. a celou část 4.2., ve které se autorka snaží přímo zobecnit algoritmus Paula a Preneela na husté abelovské páry.

Kapitola 2 je základ teorie trupových párů. Autorka používá definici grupového páru jakožto dvojice abelovských grup se společným neutrálním prvkem na stejné množině $X$. Později se ukázala jako mnohem vhodnější definice grupového páru jako algebry $(X,0,xor,+)$ s jednou konstantou $0$ a dvěma binárními operacemi $xor$ a + takovými, že každá operace zvlášť je abelovská grupová operace s neutrálním prvkem $0$. Vždy se předpokládá, že množina $X$ má mohutnost $2^n$. Definice používaná autorkou vede občas k problémům s přesnou formulací některých pojmů a tvrzení, například s definici řešení modulo společná kongruence obou grup v trupovém páru, definicí izomorfizmu trupových párů, systému reprezentantů podle společné kongruence trupového páru, apod.

V Kapitole 3 autorka uvádí algebraický pohled na algoritmus Paula a Preneela vycházející z toho, že ve standardním trupovém páru existuje řetěz společných kongruencí maximální možné délky. Zde zůstala na půli cesty v tom, že používá přespříliš systémy reprezentantů místo přímého počítání s kongruencemi.

Druhou vhodnější definici autorka zavádí na počátku Kapitoly 4, pak se ale zase v dalším vrací k původní definici z Kapitoly 2. Na počátku kapitoly autorka předpokládá, že grupový pár má svaz kongruencí maximální možné délky, tj. $n$. To je definice hustého abelovského páru, která je za vedena ale až později. Následuje obecná teorie hustých abelovských párů a poté v podkapitole 4.1. popis možné vzájemné polohy obou grup v hustém abelovském páru. Zde není dostatečně rozlišená role prvků $e_i+e_i$, případně $e_i \; xor \; e_i$, a role přechodových funkcí $f_i$. Zatímco prvky $e_i+e_i$ popisují grupovou operaci +, resp. její rozšíření z podgrupy $X_{i-1}$ na podrupu $X_i$, funkce $f_i$ slouží k popisu vzájemné polohy těchto operací. Tato část vrcholí Tvrzením 4.18., které také umožňuje spočítat, kolik hustých abelovských párů existuje s danou operací $xor$ .

K této části mám dotaz – je možné z Tvrzení 4.18 přímo odvodit jakým způsobem přeložit souřadnice daného prvku vzhledem k jedné operaci na souřadnice téhož prvku vzhledem ke