Posudek oponenta k bakalářské práci 'Kryptografie založená na eliptických křivkách' Veroniky Heglasové

Předložená práce vysvětluje, jak lze pomocí eliptických křivek nad konečnými tělesy implementovat některé kryptografické systémy. V první kapitole je vysvětleno, jak na bodech eliptické křivky zavést strukturu abelovské grupy. Druhá kapitola představuje algoritmus, který převede zadanou zprávu na posloupnost bodů eliptické křivky. Dále jsou popsány některé kryptografické systémy (Diffie-Helmanova výměna klíče, Masseyův-Omurův a El Gamalův kryptografický systém), kde je možno eliptické křivky využít. Rovněž je diskutována volba klíčů z hlediska bezpečnosti. Třetí kapitola je popisem implementace El Gamalova systému, kterou autorka provedla v Mathematice 7.0.

Práce je sepsána velmi srozumitelně a poutavě. Obsahuje několik drobnějších nepřesností: V Poznámce 1.3 je nejspíše využíváno vztahu diskriminantu a normy derivace, tedy by tam mělo být $4a^3 + 27b^2$. V prvním odstavci sekce 1.3 se hovoří o neexistenci algoritmu. To může znamenat, že lze dokázat neexistenci algoritmu nebo že algoritmus není v současnosti znám. Z hlediska bezpečnosti je to podstatný rozdíl, zde je nezbytné vyjádřit se přesně. Algoritmus vysvětlený na straně 13 není ošetřen proti selhání, přestože je uvedeno, že selhat může. Podobnou výtku lze mít i k proceduře prevodX z implementace, i když zde je to možná ošetřeno omezením na uživatele (i to by ale stálo za zmínku). Na straně 21 tvrzení 'inverzní prvek neexistuje' není zcela srozumitelné. Pravděpodobně jde o problém se sčítáním B a $-B$. I zde by bylo možno implementaci vylepšit tak, aby formálně odstranila tento problém (přestože omezení na řád bodu B je z bezpečnostního hlediska rozumné). Kromě toho, jsou v práci ještě drobné překlepy, například ve vzorcích 1.5 a 1.6 má být x_P místo x_p.

Největší výhrady mám ale k rozsahu a náročnosti práce. Myslím, že nějaké tvrzení 'nad rámec této práce' mohlo být uvedeno alespoň s náznakem důkazu, nebo mohla být provedena analýza výpočetní složitosti provedené implementace.

Předloženou práci doporučuji k obhajobě, navrhuji hodnocení 'velmi dobře'.

V Praze, 20. června 2010,

Pavel Příhoda