Romana Linkeová: *Diffie a Hellman si vyměňují matice nad grupovým okruhem*

Posudek oponenta bakalářské práce.

Práce se zabývá řešením problému diskrétního logaritmu v konkrétním případě násobení v okruhu matic nad grupovým okruhem. Práce je motivovaná zveřejněným návrhem použít násobení v okruhu $\mathrm{M}_k(\mathrm{GF}(p)[\mathrm{S}_n])$ pro malá n, p a k jako alternativu ke grupovým strukturám v současnosti používaným v Diffie-Hellmanově protokolu.

Díky volnému charakteru konstrukce grupového okruhu je výsledná velikost zkoumané pologrupy daleko za možnostmi běžných útoků. Přesto lze díky malým vstupním parametrům efektivně provádět výpočty v Diffie-Hellmanově protokolu, což byl zřejmě záměr autorů návrhu. Právě konstrukce grupového okruhu ale umožňuje řadu redukcí. V práci je vyřešen problém diskrétního logaritmu pro navrhovanou pologrupu a tím i Diffie-Hellmanův problém. Řešení používá teorii reprezentací když problém převádí na hledání diskrétních logaritmů v malé množině reprezentací nižších stupňů. Z rozboru výpočetní náročnosti hledání těchto logaritmů je vidět, že takový útok je zcela reálný.

V práci je také vyvrácena představa navrhovatelů modifikace DH protokolu, že algoritmus baby-step giant-step nelze v navrhované struktuře aplikovat pro jeho příliš velkou paměťovou náročnost.

Součástí práce je funkční implementace popsaného útoku v jazyce C++. Útok lze úspěšně provést v řádu dnů na jednom procesoru.

V práci lze samozřejmě nalézt některé nepřesnosti nebo překlepy, což ale nesnižuje její kvalitu. Také je v práci zmíněna možnost implementace útoku na grafických kartách, ale chybí zde podrobnější rozbor možností jeho paralelizace.

V práci je úspěšně analyzován - a také zlomen - publikovaný návrh kryptografického protokolu pomocí netriviálních metod teorie reprezentací. Jedná se o výborný původní výsledek dosažený nezávisle na později publikovaných pracech.

Předloženou práci navrhuji uznat jako bakalářskou s hodnocením *výborně*.

V Praze dne 18. června 2014 Mgr. Robert El Bashir, Dr.