Posudek vedoucího bakalářské práce
Diffie a Hellman si vyměňují matice nad grupovým okruhem
Romany Linkeové

Diffieho-Hellmanův protokol patří k nejznámějším schématům kryptografie s veřejným klíčem. Protokol by měl zajistit způsob, kterým mohou dva uživatelé pomocí veřejného kanálu sdílet nějakou tajnou informaci. Jako platforma se typicky bere multiplikativní grupa tělesa prvočíselného řádu, v takovém případě je pro větší prvočísla komunikace nezvladatelná pro přístroje s menší výpočetní kapacitou. Toto omezení vedlo Kahrobaeiho, Koupparise a Shpilraina k návrhu varianty protokolu, který využije jako platformu (multiplikativní) pologrupu okruhu $\mathrm{M}_3(\mathbb{Z}_7S_5)$. Protokol byl zveřejněn v časopise Groups, Complexity and Cryptology. Ushakov a Myasnikov publikovali v Journal of Symbolic Computation útok, který vnořením okruhu $\mathrm{M}_3(\mathbb{Z}_7S_5)$ do $\mathrm{M}_{360}(\mathbb{Z}_7)$ převede tak pologrupový problém na problém diskrétního logaritmu v multiplikativní grupě konečného tělesa.

Předložená práce jde ještě dále. S využitím teorie reprezentací grupy S_5 je $\mathrm{M}_3(\mathbb{Z}_7S_5)$ vnořen do součinu maticových okruhů nad $\mathbb{Z}_7$. Rozměry matic pak umožňují provést úspěšný útok na protokol na běžném počítači. Stejnou myšlenku využívá i preprint Neuselové a Monica, tato práce ale nebyla při návrhu útoku využita (preprint na internetu má datum 28. 4. 2014).

Autorka dále pečlivě analyzuje jednotlivé kroky výpočtu. Nakonec je ukázáno, jak lze spočítat periodu prvku $\mathrm{M}_3(\mathbb{Z}_7S_5)$ a pomocí ní vylepšit algoritmus typu Baby steps - Giant steps z původního článku (jde spíše o zajímavost, z praktického hlediska tento algoritmus smysl nemá).

Celková úroveň práce je velmi dobrá, i když některé nepřesnosti by bylo ještě třeba odstranit. Implementaci útoku šlo napsat obecnější, ale vzhledem k obvyklému rozsahu bakalářských prací ji považuji za dostatečnou. Spokojen jsem byl s celkovým přístupem, Romana pracovala s velkým zaujetím. Při řešení některých problémů bych ale očekával větší samostatnost.

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

V Hradci Králové, 22. 6. 2014

Pavel Příhoda