Posudek na bakalářskou práci

Jan Říha, Konstrukce a kryptoanalýza AES (Advanced Encryption Standard)

Práce začíná stručným popisem soutěže o návrh nové blokové šifry, která měla nahradit už nevyhovující DES. Poté pokračuje jejím podrobným matematickým popisem, implementacemi na různých platformách a nakonec velmi stručným úvodem do kryptoanalýzy AES. Šifra AES je v současné době nejvíce zkoumanou blokovou šifrou.

Popis konstrukce je poměrně přehledný, je třeba ale poznamenat, že autor mohl vycházet z řady velmi dobře použitelných zdrojů. K této části mám pouze několik poznámek.

- Na str. 9 dole v odstavci o polynomech s koeficienty v konečných tělesech je definice polynomů nejvýše třetího stupně bez explicitního uvedení, z jakého tělesa jsou koeficienty.
- Na str. 12 a 13, v části 2.5. při popisu transformace SubBytes mi dost schází obecná formule pro tuto operaci a její vztah k příslušnému S-boxu. Právě jednoduchost obecné formule pro operaci SubBytes bývá některými kryptology považována za potenciální slabinu AES.
- Expanzi klíče na str. 16 bych si představoval podrobněji popsanou a vysvětlenou, nejen uvedením pseudokódu.

Popis využití vlastností AES k optimalizaci implementací na různých platformách je stručný, ale pro účely práce dostatečný.

Jako jedinou větší slabinu vidím přílišnou stručnost kapitoly o kryptoanalýze. Kryptoanalýza AES je nyní jedním z hlavních témat kryptologie a shrnutí výsledků na pouhé 4 stránky je opravdu více než stručné. Na omluvu lze říct, že autor absolvuje hlavní kryptologické přednášky až v příštím roce. V této části mi také chybí přesné citace, autor vždy uvádí v textu pouze autora a název práce bez úplné citace, takže případný čtenář zajímající se o podrobnější popis naznačených útoků bude muset stejně všechny citace vyhledávat sám.

V každém případě je třeba konstatovat, že práce splnila svůj účel. Autor se podrobně seznámil s návrhem šifry AES, variantami jejích implementací na různých platformách a některými směry její kryptoanalýzy. Práce se může stát dobrým základem pro další studium a vlastní výzkum v kryptoanalýze šifry AES. Práce obsahuje pouze drobné nedostatky.

Navrhuji přijmout tuto práci jako práci bakalářskou a hodnotit ji známkou výborně

[redacted]

Doc. RNDr. Jiří Tůma, DrSc.
vedoucí práce

V Praze, 5.9.2006