POSUDOK VEDÚCEHO NA BAKALÁRSKU PRÁCU:

Jakub Töpfer

Rotační kryptoanalýza ARX šifer

Práca Jakuba Töpfera sa venuje funkciám, ktoré je možné vyjadriť pomocou modulárneho sčítania, XORu a rotácie. Takéto funkcie sa označujú skratkou ARX, prípadne iba AX pri vynechaní rotácie. V prvej časti práce autor popisuje obecné výsledky týkajúce sa ARX a AX funkcí. Ukazuje napríklad, že ľubovoľnú funkciu je možné zapísať pomocou týchto troch operácii a operácie pričítania konštanty. V druhej časti práce je popísaná rotačná kryptoanalýza. Tá využíva propagáciu takzvaného rotačného páru a jeho zachovanie operáciami XOR a rotáciou. Autor popisuje využitie rotačnej kryptoanalýzy na šifru Threefish a ako vlastný výsledok uvádza jej aplikáciu na šifry TEA a XTEA. Na konci práce je stručne popísaný rozpínavý rotačný útok.

Práca je síce prevažne rešeržného charakteru, autor ale vytvoril veľmi dobrý prehľad danej problematiky. Okrem vlastných výsledkov popísaných v kapitolách 1.5 a 3.2, ktoré pozostávajú z jednoduchej aplikácie popisovanej teórie, by som vyzdvyhol rozpísanie zaujímavých, a len nedávno publikovaných výsledkov týkajúcych sa AX funkcí v kapitole 1.4. Matematická, ako aj formálna úroveň práce sú výborné. Prácu preto doporučujem prijať ako bakalársku a hodnotiť ju známkou *výborně*.

Praha, 14.6.2012 Michal Hojsík