# Posudek oponenta na diplomovou práci Davida Tvrdého nazvanou Cryptanalytic attacks on the cipher PRINCE

Větší část práce se týká popisu jak šifry, tak známých útoků na ní, které jsou typu Integral Attack a útok Meet-in-the-middle. Dále práce obsahuje technická zlepšení některých z těchto útoků a programové vybavení, které dokladuje správnost a funkčnost uvedeného.

Přikládáme seznam připomínek a hodnocení práce.

**Připomínky**
Na str. 6 v posledním řádku je „... if we change one bit of the key“, přesněji by mělo být „... if we change one bit of the first round key“

Na str. 7 je odstavec o konstrukci FX. Zde by měl být odkaz na literaturu (Kilian and Rogaway, CRYPTO 1996).

Na str. 8 je uveden příklad množiny otevřených textů {0, 1, ..., 15}, které mají být 64 bitové, ale uvedená množina obsahuje 4 bitové hodnoty. Autor má na mysli téměř jistě 4 bitové části otevřených textů, jinak by hádání 4 bitových hodnot klíče nemělo význam. Také by bylo dobré spojit pozici těchto 4 bitů s pozicí hádaného klíče.

Na str. 8 je uveden rok vzniku MITM 1997, má být 1977.

Na str. 9 ve třetím řádku shora má místo „decrypt“ být „encrypt“.

Na str. 11 je matoucí počet rund a jejich obsah. Mělo by být jasně deklarováno, co jsou prostřední dvě rundy, protože to ovlivňuje celý dasší text. Není jasné odkud kam je první a druhá z těchto rund. Vzhledem k tomu, že runda se má podle popisu na str. 11 sestávat z přičtení rundovního klíče a konstanty, jedné substituční a jedné lineární úrovně, je zde nejasnost, protože prostřední dvě rundy toto neobsahují. Poznamenejme, že nejednoznačnost způsobili přímo autoři šifry. K popisu šifry to není nezbytné, ale k popisu útoků by to bylo velmi žádoucí.

Na str. 16 ve 3. řádku zdola a dále je vhodné uvažovat hodnotu *l* nenulovou, jinak by definice na str. 17 byly sporné a neužitečné.

Není explicitně definováno, co se míní 2,5 nebo 3,5 nebo 4,5 rundovním distinguisherem.

Přínos práce v oblasti integrálního útoku vyplývá z možnosti ve 4,5 rundovním integrálním distinguisheru nahradit první čtyři vstupní nibbles A16,A16,A16,C hodnotami A16,A16,A2,A2. K tomu se využívá vlastnost, že matice M´ transformuje zpracovatelem nově navrženou množinu nibbles na výstup typu A16,A16,A16,A16 stejně jako původní množina nibbles. K tomu je v prvním případě potřeba uvažovat $2^4 * 2^4 * 2^4 * 1$ otevřených textů, zatímco v druhém případě $2^4 * 2^4 * 2 * 2$, tj. 4x méně otevřených textů. Tato vlastnost je klíčová, ale není dokázána. Je zde pouze uvedeno, že správnost tohoto kroku může být ověřena stejně jako v předchozím odstavci, kde ovšem tato transformace není použita. Dále je přirozené se ptát, proč by metoda nemohla být ještě dále 2x nebo 4x zlepšena pomocí nibbles A16,A16,C,C nebo A16,A16,A2,C. Důkaz by odhalil, zda lze nebo nelze metodu dále zlepšit.

V odstavci 3.3 Faster key recovery technique, se popisuje metoda z literatury [4] a realizuje se programem. Metoda je příliš úsporně popsaná, takže se čtenář musí poučit z originálu.

**Hodnocení**
Zpracovatel pochopil principy integrálního útoku a metodu rychlejšího hledání klíče a ověřil je programem. V případě integrálního útoku zlepšil jeho účinnost, sice o malý kousek, ale možná se tím dotkl hranice, za kterou daná metoda již nemůže být zlepšena. To je velmi pozitivní. Nedostatkem je však nezdůvodněný přechod mezi stavy šifry, na němž toto zlepšení stojí.

Podobně je to s popisem a zlepšením útoku Meet-in-the-middle. Zpracovatel pochopil princip tohoto útoku, popsal technické zlepšení a ověřil programem.

Celou prací se vine jedna vlastnost, která platí téměř pro všechna Observations i záznamy všech metod z literatury i vlastní příspěvky zpracovatele. Jedná se o velmi úsporná vyjádření, která jdou někdy až na hranici, kdy je nutné konzultovat s originály prací nebo ověřovat vlastnosti samostatně. Zhutnělé originální práce, z kterých se vychází, by naopak bylo vhodné dále komentovat a eventuelně doplnit vysvětlujícími komentáři, aby bylo dostatečně dobře vidět, v čem je přínos zpracovatele a zvýraznila se pointa původního útoku a její zlepšení zpracovatelem.

Pokud uvěříme zhutnělým důkazům a vysvětlením, je zřejmé, že zpracovatel zlepšil dosavadní útoky pomocí technických zeslabení původních požadavků útoků. Nejedná se o velká zásadní zlepšení, pouze pochopení stávajících útoků a vyhmátnutí posledních možností jak je zlepšit. To jednak dokazuje, že zpracovatel pochopil pointy útoků a nalezl možná poslední skulinky, jak je zlepšit. Proto nevadí relativně malé zlepšení útoků, velmi oceňuji nalezení oněch skulinek. Pokud by postupy autora byly podrobnější, mohlo by být vidět mnohem lépe, zdali jde skutečně o úplně poslední možnosti zlepšení.

Práci doporučuji uznat jako diplomovou.
Vlastimil Klíma, 1. 6. 2022