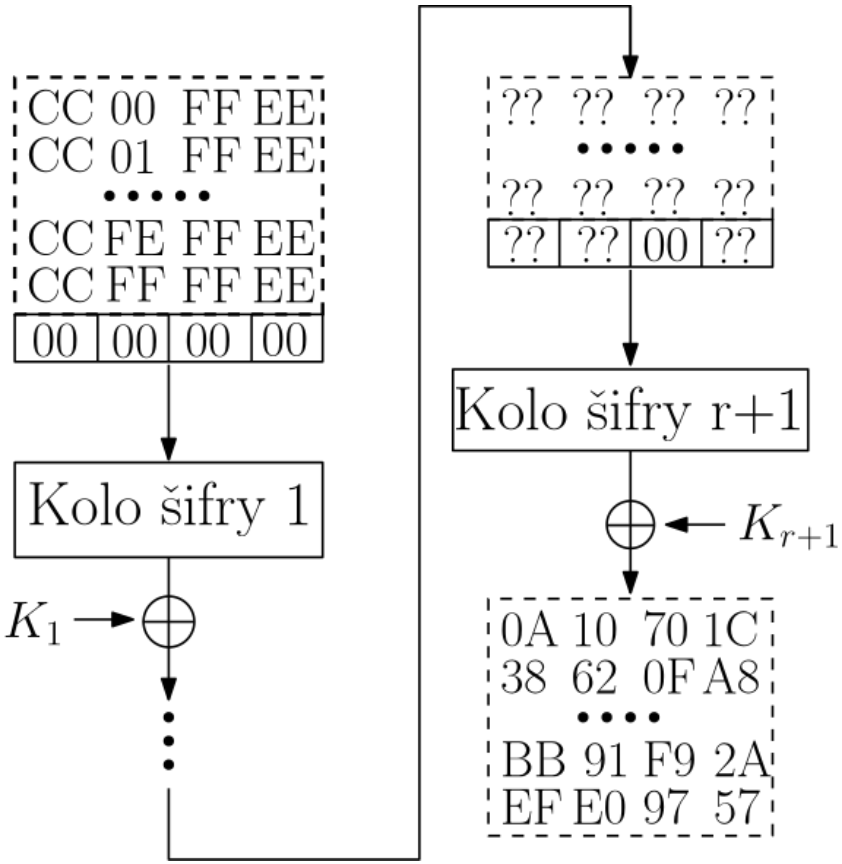
Integrálna kryptoanalýza a jej aplikácie

bc. Roman Števaňák
Školiteľ: doc. RNDr. Martin Stanek PhD.

21. februára 2020

Základy integrálneho útoku



- Útok typu CPA
- Aktívne bity
- Integrálny rozlišovač na r kôl a jeho použitie
- Cieľ - hľadať lepšie integrálne rozlišovače

Integrálny útok a derivácie

- Algebraický normálový tvar (ANF) pre booleanovskú funkciu $f(x_1, x_2, \ldots, x_n) = \bigoplus_{I \subseteq \{1,2,\ldots,n\}} a_I \bigwedge_{j \in I} x_j$
  - $\bigwedge_{j \in I} x_j$ nazývame *monomiál*
- n výstupných bitov šifry $\rightarrow$ n booleanovských funkcií šifrovania
- Sčítanie zašifrovaných textov je ekvivalentné derivácii šifrovacej funkcie vzhľadom na aktívne bity
- Booleanovská funkcia v ANF nemá monomiál obsahujúci všetky aktívne bity $\rightarrow$ funkcia po derivácii rovná 0

Príklad

- $f_1(x_1, x_2, x_3, x_4, k_1, k_2, k_3, k_4)$ je booleanovská funkcia šifrovania pre prvý výstupný bit, $x_1, ...x_4$ sú bity otvoreného textu a $k_1, ..k_4$ sú bity kľúča

$$f_1(x_1, x_2, x_3, x_4, k_1, k_2, k_3, k_4) = x_1x_2x_3k_2 \oplus x_2x_3x_4 \oplus k_1k_3k_4$$

- Derivácia vzhľadom na x_1 a x_4

$$(D_1 \circ D_4)f_1(x_1, x_2, x_3, x_4, k_1, k_2, k_3, k_4) = 0$$

- Derivácia vzhľadom na x_1 a x_2

$$(D_1 \circ D_2)f_1(x_1, x_2, x_3, x_4, k_1, k_2, k_3, k_4) = x_3k_2$$

Používanie konštánt na zlepšenie integrálneho útoku

- Funkcia f_1 v ANF pre r kôl, kde neexistuje rozlišovač
- Po derivácii ostali monomiály pôvodne obsahujúce všetky aktívne bity
- Konštantné bity sú arbitrárne $\Longrightarrow$ ak za ne zvolíme 0, môžeme sa zbaviť aj ďalších monomiálov
  - Nazveme ich modré bity
- V predchádzajúcom príklade zvoliť za x_3 nulu
- Môže pomôcť s komplexitou rozlišovača alebo počtu kôl

RES

- Jednoduchá šifra na testovanie
- Kolo z operácií:
  1. Pripočítanie kľúča
  2. Cyklický posun vľavo o počet bitov
  3. Modulárne pripočítanie konštanty k celému stavu
- 4 bitová verzia šifry
- Skúsené všetky konfigurácie

Zlepšenie použitím konštanty pri RES

Konfigurácia šifry		Počet kôl pre najlepší rozlišovač	
Cyklický posun	Konštanta	Solvatore[1]	Zlepšená metóda
1	2	7	8
1	10	7	8
2	1	3	5
2	2	5	7
2	9	3	5
2	10	5	7
3	6	7	9
3	14	7	9

[1] Z. Eskandari, A. Kidmose, S. Kölbl, T. Tiessen. "Finding Integral Distinguishers with Ease". In: *International Conference on Selected Areas in Cryptography*. Springer. 2018, s. 115–138.

Implementácia v Solvatore

- Solvatore[2] - Nástroj umožňujúci hľadanie integrálnych rozlišovačov
  - Používa opis šifry na vysokej úrovni
- Náš postup:
  1. Vytvorenie booleanovských funkcií pre prvé kolo pomocou Sympy[3]
  2. Explicitne dosadenie do premennej za modré bity → zjednodušenie funkcie
  3. V Solvatore nahradenie 1. kola špeciálnym, odsimulovanie vstavanými metódami

[2] Z. Eskandari, A. Kidmose, S. Kölbl, T. Tiessen. *Solvatore*. 20. jan. 2019. URL: https://github.com/kste/solvatore.

[3] A. Meurer et al. "SymPy: symbolic computing in Python". In: *PeerJ Computer Science* 3 (), e103. URL: https://doi.org/10.7717/peerj-cs.103.

Práca do budúcnosti

- Dokončiť implementáciu zlepšeného hľadania rozlišovačov pomocou konštánt v Solvatore[4]
- Zlepšiť spôsob hľadania rozlišovačov s použitím konštánt
- Použiť metódu na existujúce šifry
- Použitie modrého bitu v kľúči

[4] Z. Eskandari, A. Kidmose, S. Kölbl, T. Tiessen. *Solvatore*. 20. jan. 2019. URL: https://github.com/kste/solvatore.

Ďakujem za pozornosť