Integrálna kryptoanalýza a jej aplikácie

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

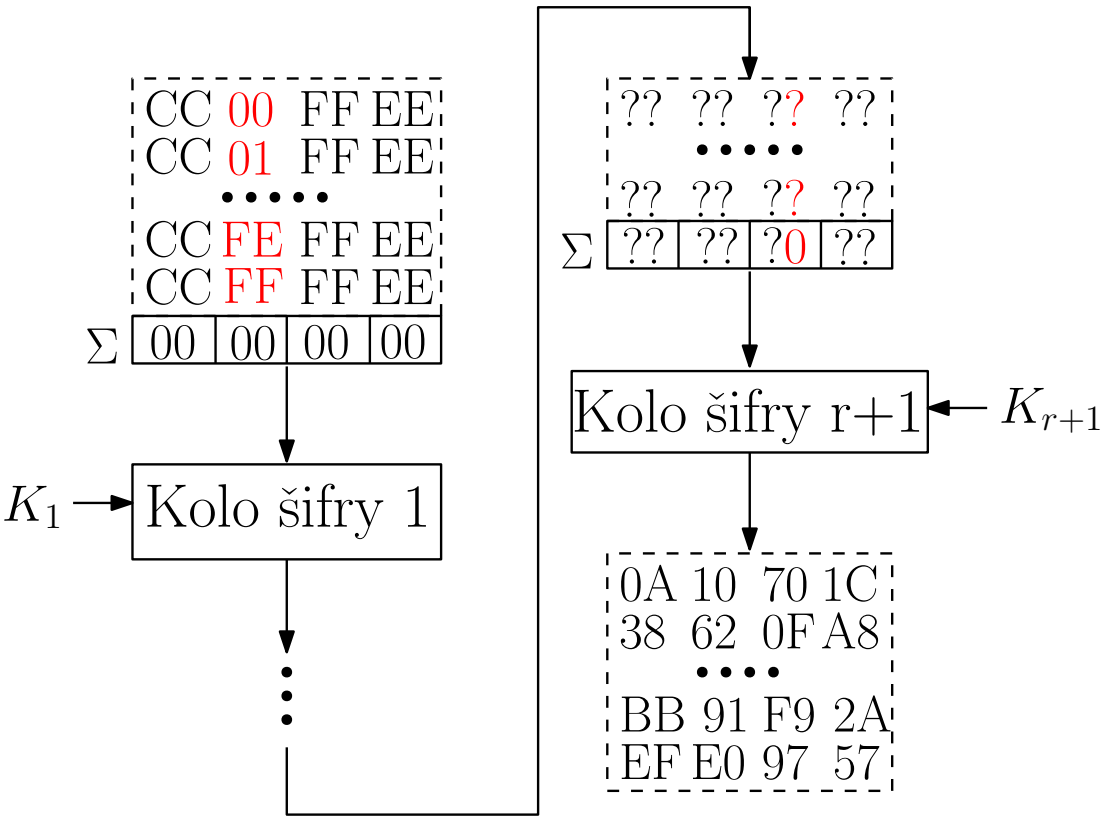
17. júna 2020

Integrálna kryptoanalýza

- Jeden zo základných kryptografických útokov
- Určité obdobie najlepší útok na šifru AES[1]
- Zameraný na blokové šifry
- Útok s možnosťou voľby otvoreného textu (Chosen Plaintext Attack)
- Cieľom útoku je odhaliť kľúč

[1] N. Ferguson et al. "Improved Cryptanalysis of Rijndael". In: *FSE*. 2001.

Základy integrálneho útoku



- Zameraný na bity
- Aktívne a konštantné bity
- Integrálny rozlišovač na r kôl a jeho použitie
- Cieľ – hľadať lepšie integrálne rozlišovače

Integrálny útok a derivácie

- Algebraická normálna forma (ANF) pre boolovskú funkciu

$$f(x_1, x_2, \ldots, x_n) = \sum_{I \subseteq \{1,2,\ldots,n\}} a_I \prod_{j \in I} x_j$$

  - $\prod_{j \in I} x_j$ nazývame *monóm*
- n výstupných bitov šifry $\Longrightarrow$ n boolovských funkcií šifrovania
- Sčítanie zašifrovaných textov $\Longleftrightarrow$ Dosadenie konštantných bitov do šifrovacích funkcií zderivovaných vzhľadom na aktívne bity
- Boolovská funkcia v ANF nemá monóm obsahujúci všetky aktívne bity $\Longrightarrow$ funkcia po derivácii rovná 0

Príklad

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

$$f(x_1, x_2, x_3, x_4) = x_1x_2x_3k_2 + x_2x_3x_4 + k_1k_3k_4$$

- Derivácia vzhľadom na x_1 a x_4

$$(D_1 \circ D_4)f(x_1, x_2, x_3, x_4) = 0$$

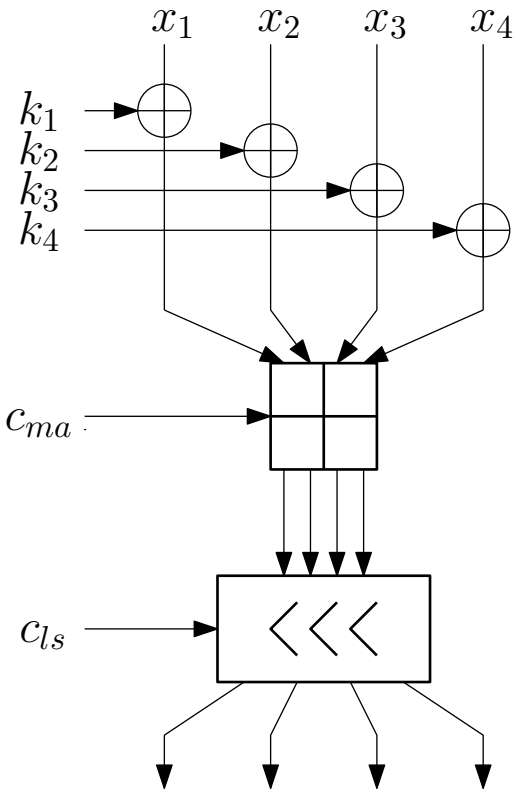
- Derivácia vzhľadom na x_1 a x_2

$$(D_1 \circ D_2)f(x_1, x_2, x_3, x_4) = x_3k_2$$

Používanie konštánt na zlepšenie integrálneho útoku

- Konštantné bity sú ľubovoľné
  - Dosadením hodnoty 0 za x_i budú aj všetky monómy obsahujúce x_i rovné 0
  - Dosadením hodnoty 1 za x_i sa môže monóm sčítať s iným
- Takéto bity nazveme *modré bity*
- Integrálne rozlišovače s modrými bitmi – *modré rozlišovače*

RES



- Jednoduchá šifra na testovanie
- Kolo z operácií:
  1. Pripočítanie kľúča
  2. Modulárne pripočítanie konštanty k celému stavu
  3. Cyklický posun vľavo o počet bitov
- 4 bitová verzia šifry
- RES(c_{ls}, c_{ma}, r) – RES s cyklickým posunom c_{ls}, pripočítavanou konštantou c_{ma} a r kolami

Modré rozlišovače pre RES

- Funkcia f v ANF pre 1. bit RES(3, 14, 9) po derivácii vzhľadom na 1. a 2. vstupný bit

$$f(x_1, x_2, x_3, x_4) = x_4 + x_3k_1 + x_3k_2 + x_3k_3 + x_3k_4 + x_4k_3$$

- Funkcia g v ANF pre 2. bit RES(2, 7, 5) po derivácii vzhľadom na 3. a 4. vstupný bit

$$g(x_1, x_2, x_3, x_4) = (k_1 + x_1k_1) + (k_3 + x_1k_3) + (k_1k_2 + x_2k_1k_2) + (k_2k_3 + x_2k_2k_3) + (x_1k_2k_4 + x_2k_2k_4)$$

Hľadanie integrálnych a modrých rozlišovačov analýzou ANF

- Testované všetky konfigurácie 4 bitovej verzie RES s konštantami c_{ls} a c_{ma}
  1. Vygenerovali sme funkcie v ANF pre RES(c_{ls}, c_{ma}, r) pre $r = 1$
  2. Pre všetky možné označenia bitov ako aktívne sme otestovali, či funkcie obsahujú monóm so všetkými aktívnymi bitmi
  3. Kým bol nájdený integrálny rozlišovač, iteratívne sme zvyšovali r
- Podobne pre modré bity
  - 2. krok bol skúšaný pre všetky variácie modrých bitov
  - Dosadili sa za ne hodnoty, potom sa skontrolovalo, či obsahuje daný monóm
- Výpočtovo nerealizovateľné pre väčšie šifry
  - Počet monómov môže byť exponenciálny od dĺžky bloku

Zlepšenie použitím modrých bitov pri RES

c_{ls} \ c_{ma}	0	1	2	3	4	5	6	7
0	∞	∞	∞	∞	∞	∞	∞	∞
1	∞	4	7+1	4+2	∞	4+2	7+1	4
2	∞	11+2	5+2	3+3	∞	3+3	5+2	11+2
3	∞	4	7+4	4+1	∞	4+1	7+4	4

c_{ls} \ c_{ma}	8	9	10	11	12	13	14	15
0	∞	∞	∞	∞	∞	∞	∞	∞
1	∞	4	7+1	4+2	∞	4+2	7+1	4
2	∞	11+2	5+2	3+3	∞	3+3	5+2	11+2
3	∞	4	7+4	4+1	∞	4+1	7+4	4

Solvatore

- Nástroj umožňujúci hľadanie integrálnych rozlišovačov[2]
- Možnosť jednoduchého opisu šifry
- Zjednodušenie výpočtu na určenie, či výsledná ANF má monóm obsahujúci všetky aktívne bity
- V našej práci – implementácia hľadania modrých rozlišovačov dvoma spôsobmi
  - Exponenciálna časová zložitosť v závislosti od dĺžky bloku
  - Testovanie všetkých označení vstupných bitov ako aktívne alebo modré

[2] Z. Eskandari et al. "Finding Integral Distinguishers with Ease". In: *SAC*. 2018.

Implementácia úpravou výpočtu

- Upravený spôsob počítania tak, aby bral do úvahy modré bity
- Žiadny vplyv, ak je použitý „key whitening“
- Otestované na šifre Speck
  - So skrátenou dĺžkou bloku na 16 bitov
  - S dĺžkou bloku 32 bitov, pre najviac 5 modrých bitov, alebo aspoň 27 modrých bitov
- V oboch prípadoch rovnaké výsledky ako pôvodné

Implementácia zjednodušením prvého kola

- Postup:
  1. Vytvoríme ANF funkcií pre 1. kolo šifrovania
  2. Do nich dosadíme za modré bity ich hodnoty
  3. Pomocou Solvatore simulujeme šifru, ktorá má upravené prvé kolo a ostatné pôvodné
- Pre všetky konfigurácie RES neboli nájdené modré rozlišovače pre viac kôl ako pôvodným spôsobom

Implementácia zjednodušením viacerých začiatočných kôl

- Zjednodušenie viacerých začiatočných kôl
- Pre RES bol nájdený modrý rozlišovač pre 20 z 28 konfigurácií šifry
- Vo väčšine prípadov bolo pre r kolový rozlišovač potrebné vytvoriť funkcie v ANF pre $r - 1$ kôl
  - Výpočtová náročnosť podobná analýze ANF

Prínos práce

- Formálne dôkazy niektorých implicitných tvrdení v práci opisujúcej Solvatore
- Na jednoduchej šifre ukázané, že použitie modrých bitov má význam
- Implementácia hľadania modrých rozlišovačov v rámci Solvatore dvoma spôsobmi
- Odhad časovej a priestorovej zložitosti integrálnej kryptoanalýzy aj s použitím modrých bitov

Práca do budúcnosti

- Zrýchlenie hľadania modrých rozlišovačov, aby bolo praktické aj pre šifry s väčšou dĺžkou bloku
- Použitie na praktické šifry
- Použitie modrých bitov v kľúči

Ďakujem za pozornosť