Návrh a kryptoanalýza šifier - Zadanie 7

Peter Čuřík

15. novembra 2021

1 AES-CTR-64

Parametre šifry

- blok: 64 bitov
- pole: $GF(2^4)$ realizované polynómom $x^4 + x^1 + 1$
- kolové konštanty: 0x01000, 0x0200, 0x0400, 0x0800, 0x0300, 0x0600, 0x0C00, 0x0B00, 0x0500, 0x0A00
- S-box: viď 1.1
- počet kôl: 10

1.1 S-box

S-box je použitý zo zadaní 4,5 a 6 a je definovaný nasledujúcou tabuľkou:

vstup	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
výstup	8	C	B	3	7	9	1	4	E	6	0	D	2	F	5	A

1.2 Tabuľka pre shiftRows

Tabuľka definuje pozíciu nibblu po aplikovaní shiftRows $GF(2^4)$:

vstup	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
výstup	0	D	A	7	4	1	E	B	8	5	2	F	C	9	6	3

1.3 Tabuľky na mixColumns

Tabuľky pre vstupný nibble určia výstupný nibble vynásobený konštantou v poli $GF(2^4)$. Napríklad tabuľka mul2 slúži pre násobenie dvomi a vyzerá nasledovne:

vstup	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
výstup	0	2	4	6	8	A	C	E	3	1	7	5	B	9	F	D

2 Implementácia

Vlastné riešenie v jazyku C. Dostupné z: `https://github.com/petercurikjr/Design-and-cryptanalysis-of-ciphers---Assignments/blob/master/07/aes-64bit/aes-64bit/main.c`

Symetrickosť šifry bola otestovaná na náhodnom 64 bitovom bloku. Blok bol zašifrovaný a dešifrovaný, pri použití rovnakého kľúča. Výsledná hodnota bola porovnaná s pôvodnou. Ak sa rovnali, šifru považujeme za symetrickú a funkčnú.

V prípade neúspechu tohto experimentu pomohlo postupné aplikovanie všetkých dvojíc šifrová operácia/inverzná šifrová operácia na daný blok. Nerovnosť vstupu voči výstupu ukázala, ktoré z operácií obsahovali chyby.

2.1 Konštanty

V kóde sú definované tabuľky predvypočítaných hodnôt, s ktorými algoritmus pracuje. Tými sú:

- tabuľka kolových konštánt. Vypočítané ručne.
- tabuľka S-boxu (viď 1.1) a inverzného S-boxu. Dané S-boxom zo zadaní 4,5 a 6.
- tabuľka permutácií (viď 1.2) a inverzných permutácií. Dané šifrou AES.
- tabuľky násobenia v poli $GF(2^4)$ hodnotami 1, 2 (viď 1.3), 3 na šifrovanie a hodnotami 9, 11, 13, 14 na dešifrovanie. Prebraté zo zdroja `http://www.ee.unb.ca/cgi-bin/tervo/galois3.pl?p=4`.

Tabuľky na základe nibble vstupu (0x0 - 0xF) vracajú nibble výstup (0x0 - 0xF).

2.2 Programovacie techniky

Každá operácia je izolovaná do samostatnej funkcie: `addRoundKey`, `shiftRows`, `subBytes`, `mixColumns`. Očakávajú 64 bitový blok ako vstup a vracajú modifikovaný 64 bitový blok.

V operáciách sa pracuje najmä s bitovými operáciami ako: `^`, `<<`, `>>`, `|`, či `&`. Niektoré výpočty sú ušetrené pomocou čítania z lookup tabuliek.

3 Merania

Šifra bola na účely meraní nastavená do módu CTR. Bolo vygenerovaných 100 prúdov dát o veľkosti 1MB. Prúd sa skladá zo 125 000 kusov 64 bitových blokov, teda dokopy 1 250 000 blokov. Jeden blok sa skladá z 32 bitov inicializačného vektora a 32 bitov počítadla módu CTR.

3.0.1 Výkonnostné testy

Kód bol skompilovaný kompilátorom gcc s prepínačom -03. Postupnosti bolo možné zašifrovať v čase 0.295 sekundy. Dešifrovanie trvalo 0.279 sekundy. Konzolový nástroj openssl je za rovnaký čas schopný šifrovať 855 012 kusov 128 bitových blokov, čo odpovedá objemu 13,68MB dát. Oproti 100MB vygenerovaných našou implementáciou je openssl 7,3 násobne pomalší.

Je ale dôležité podotknúť, že naša implementácia pracuje v menšom poli, s menším blokom a menším kľúčom. Openssl nepodporuje šifru AES-CTR s veľkosťou bloku 64 bitov a nepodporuje pole iné ako $GF(2^8)$. Úprava parametrov šifry by ukázala presnejšie časové porovnanie.

3.0.2 Štatistické testy

100 vygenerovaných postupností bolo vložených do softvéru paranoYa. Hľadali sme postupnosti, ktoré nespĺňali hladinu spoľahlivosti $\alpha = 0.01$, teda, zo všetkých testov neprešlo viac ako 4% postupností.

Výsledky neukázali žiadne také testy, ktoré by mali úspešnosť menšiu ako 96%. Najhoršie úspešnosti začínajú na práve 96%, v počte 1. Touto úspešnosťou disponuje Non-overlapping template matching test. Úspešnosť 97% dosiahli testy ako Random excursions variant test, či Linear comlexity test.

4 Záver

Výsledky štatistických testov potvrdzujú aspekt dostatočnej náhodnosti výstupov z AES tejto šifry za dostatočne bezpečnú. Prekvapivé je, že testy dopadli priaznivo napriek kryptograficky zraniteľnému S-boxu, ktorý bol v šifre použitý. Zraniteľnosť daného S-boxu sme dokázali v minulých zadaniach pomocou lineárnej a diferenciálnej kryptoanalýzy.