Návrh a kryptoanalýza šifier - Zadanie 8

Peter Čuřík

28. novembra 2021

1 Štvorkolový Square Attack

Pre účely zadania bol vykonaný square útok na zmenšenú verziu šifry AES vytvorenej v zadaní 7 (dokumentácia zadania 7 dostupná z: `https://github.com/petercurikjr/Design-and-cryptanalysis-of-ciphers---Assignments/blob/master/07/finalreport.pdf`).

Oproti zadaniu 7 boli zmenené tieto parametre šifry AES:

- počet kôl: $10 \rightarrow 4$

2 Implementácia

Vlastné riešenie v jazyku C. Dostupné z: `https://github.com/petercurikjr/Design-and-cryptanalysis-of-ciphers---Assignments/tree/master/08/aes-64bit/aes-64bit`

Na začiatku je vygenerovaných 16 P-C párov, pričom prvý bajt v množine plaintextov je lambdaset a ostatné bajty sú nuly. Následne je vykonaný samotný útok.

2.1 Výpočet posledného kolového kľúča šifry AES

Pre každý nibble 64 bitového slova sa vyskúšajú všetky možné kolové kľúče na realizáciu posledného kola AES. Posledným kolom sa preženú všetky ciphertexty z vygenerovanej množiny. Sledujeme, či po poslednom kole (reverzný smer, teda ideme šifrou od ciphertextu k plaintextu a hádame kľúč) sa XOR sledovaného nibblu všetkých ciphertextov rovná nule. Ak áno, pozorovaný kolový kľúč je kandidát.

Po dokončení testov pre konkrétny nibble ciphertextov sa pozrieme, či je na daný nibble viac ako jeden kandidát kolového kľúča. Ak nie, vieme s istotou prehlásiť, čomu sa rovná daný nibble kolového kľúča posledného kola šifry AES. Ak je kandidátov viac, experiment opakujeme nasledovne:

- vygenerujeme novú množinu P-C párov, avšak tentokrát označíme iný bajt za lambdaset
- útok opakujeme a získavame nových kandidátov kolového kľúča
- cyklus opakujeme dovtedy, kým výsledkom prieniku všetkých kandidátov kolového kľúča pre všetky odskúšané P-C sety nie je práve jeden kolový kľúč

2.2 Výpočet všetkých zvyšných kolových kľúčov šifry AES a výpočet hlavného kľúča

Po získaní kolového kľúča posledného kola vieme reverzným key schedule mechanizmom získať kľúč po kľúči, až získame hlavný symetrický kľúč šifry AES.

3 Zložitosť

Pre každý nibble 64 bitového slova (dokopy 2^4 nibblov) sa vyskúšajú všetky možné kolové kľúče (2^4 možností na nibble) na realizáciu posledného kola AES. Daným kolom sa preženú všetky ciphertexty z vygenerovanej množiny (jej mohutnosť je 2^4). To je $2^4 \cdot 2^4 \cdot 2^4 = 2^{12}$ operácií.

V pamäti je v jednom čase vždy iba jeden P-C set o veľkosti $2 \cdot 2^4 = 2^5$. Zložitosť potrebná na pregenerovanie P-C setu v prípade viacerých kandidátov kľúča je zanedbateľná a preto ju do výpočtov nebudeme uvažovať.

Záverečná tabuľka:

Typ zložitosti	**Zložitosť**	**Poznámka**
Memory complexity	2^5	P-C set
Time complexity	2^{12}	Square attack

4 Realizácia útoku

Implementáciu je možné otestovať a útok realizovať v praxi. Po spustení programu sa na obrazovku vypíše hlavný kľúč odhalený funkciou `squareAttack()`. Hodnotu si je možné overiť s hodnotou kľúča používaného na šifrovanie (súbor `main.c`, riadok 24: `const uint64_t master_key = 0x2b7e151628aed2a6;`). Riadok je možné meniť a pozorovať, že square attack je úspešný aj pre iné hodnoty kľúča.

Výsledky sú uspokojivé, útok považujeme za úspešný. Týmto bol úspešne zostrojený štvorkolový rozlišovač šifry AES-64. Z tabuľky 1 v publikácii *Cryptanalysis of Reduced Variants of Rijndael* vyplýva, že útok sa dá optimalizovať. V tabuľke vidno, že autorom publikácie sa podarilo zostrojiť štvorkolový square útok s časovou komplexitou 2^9 a to pre 128 bitovú verziu šifry, čo je rýchlejšie ako v našom prípade (2^{12} pre 64 bitovú verziu).

Útok podľa unix príkazu `time` trval 0.001 sekundy.