Lineární kryptoanalýza

Tomáš Chvosta

Listopad 2020

Zadání

Sestavte vlastní lineární aproximaci SPN šifry a připravte všechny potřebné informace, abyste mohli provést útok. Dále sestavenou aproximaci využijte k útoku na testovací implementaci SPN šifry.

Postup

Nejprve byla sestavena aproximace (obrázek a výpočet lze nalézt v souboru `Aproximace.png`). Následně byl spočítán bias, který vyšel -1/64, což je nepatrně horší výsledek než v případě ukázkové aproximace ze cvičení. Podle vzorců v dokumentaci `ldc_tutorial.pdf` bylo vypočítáno, že je potřeba alespoň 4096 plaintextů $(1/(1/64)^2)$. Následně byl proveden útok pomocí zdrojových kódů ze cvičení. Upravené zdrojové kódy pro vypočítanou aproximaci jsou ve složce `kody/`. Následně byly náhodně zvoleny testovací klíče 0x3B6C, 0xE486 a 0xA9E5 a pro každý z nich bylo vygenerováno postupně 10000, 20000, 50000 a 100000 plaintextů. Pro usnadnění testování byly vytvořeny skripty `runLinearCode.sh` a `runProcess.sh`, pomocí kterých lze celý proces testování spustit. Tyto skripty lze také nalézt ve složce `kody/`.

Výsledky

V následujících tabulkách jsou zobrazeny výsledky měření. V první tabulce jsou zmíněny pozice, na kterých byly nalezeny klíče (podklíče zasažených SBOXů):

Table 1: Pozice s nalezeným klíčem

	klíč 0x3B6C	**klíč 0xE486**	**klíč 0xA9E5**
10000 plaintextů	17.-20. pozice	Nenalezen	17.-20. pozice
20000 plaintextů	Nenalezen	Nenalezen	5.-8. pozice
50000 plaintextů	1.-4. pozice	1.-4. pozice	1.-4. pozice
100000 plaintextů	1.-4. pozice	1.-4. pozice	1.-4. pozice

V druhé tabulce jsou zmíněny biasy pro hledané klíče:

Table 2: Bias u nalezených klíčů

	klíč 0x3B6C	**klíč 0xE486**	**klíč 0xA9E5**
10000 plaintextů	0,0166	N/A	0,0135
20000 plaintextů	N/A	N/A	0,0131
50000 plaintextů	0,0154	0,0121	0,0120
100000 plaintextů	0,0170	0,0106	0,0120

Podrobné výstupy z příkazové řádky lze najít v souboru `CMDOutputs.png`. Z výsledků vidíme, že počty plaintextů 10000 a 20000 nejsou úplně dostačující. Od 50000 nejsou změny tak znatelné, navíc doba výpočtu se významně prodlužuje, proto vyšší počet plaintextů nemá příliš velký význam. Ani v jednom případě nebyl klíč jednoznačně určen (na 1. místě). Tato skutečnost může být způsobena zvolením ne příliš vhodné aproximace.