Diferenciální kryptoanalýza

Tomáš Chvosta

Listopad 2020

Zadání

Sestavte vlastní diferenciální 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 byla spočítána výsledná pravděpodobnost, která vyšla 81/4096, což je nepatrně horší výsledek než v případě ukázkové aproximace ze cvičení. 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, 0x78AF a 0x9443 a pro každý z nich byly pro výpočet postupně použity počty plaintextů 10000, 20000, 50000 a 100000. Pro usnadnění testování byly vytvořeny skripty `runDifferentialCode.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 0x78AF**	**klíč 0x9443**
10000 plaintextů	1. pozice	1. pozice	1. pozice
20000 plaintextů	1. pozice	1. pozice	1. pozice
50000 plaintextů	1. pozice	1. pozice	1. pozice
100000 plaintextů	1. pozice	1. pozice	1. pozice

V druhé tabulce jsou zmíněny pravděpodobnosti pro hledané klíče:

Table 2: Pravděpodobnosti u nalezených klíčů

	klíč 0x3B6C	**klíč 0x78AF**	**klíč 0x9443**
10000 plaintextů	0.0160	0.0212	0.0168
20000 plaintextů	0.0153	0.0240	0.0192
50000 plaintextů	0.0196	0.0173	0.0218
100000 plaintextů	0.0196	0.0197	0.0204

Podrobné výstupy z příkazové řádky lze najít v souboru `CMDOutputs.png`. Z výsledků vidíme, že ve všech případech byl útok úspěšný a hledané klíče jsou ve výsledcích vždy na 1. pozici. Co se týče pravděpodobností, dosahují lepších výsledků testy s počty plaintextů kolem 50000 (ve většině případů). Pro větší počty plaintextů nejsou naměřené hodnoty o moc lepší, navíc se doba výpočtu významně prodlužuje.