DIFFERENTIAL CRYPTANALYSIS

Ondřej ZIMOLA, Master Degree Programme (4)
Dept. of Information Systems, FIT, BUT
E-mail: xzimol02@stud.fit.vutbr.cz

Supervised by: Dr. Daniel Cvrček

ABSTRACT

In this paper, we present a differential cryptanalysis, the most significant attack applicable to symmetric-key block ciphers. The intent of the paper is to present a lucid explanation of the attack, detailing the practical application of the attack to a cipher in a simple, conceptually revealing manner for the novice cryptanalyst.

1 ÚVOD

Symetrické šifrovací algoritmy jsou založeny na sdíleném tajemství. Komunikující strany se dohodnou na stejném tajném klíči, který je použit pro šifrování i dešifrování. Útokem na šifru se snažíme dokázat slabinu, která může být zneužita k snížení bezpečnosti. Diferenciální kryptoanalýza využívá vysoké pravděpodobnosti výskytu určitých diferencí nešifrovaného textu a k nim příslušných diferencí šifrovaného textu.

2 ANALÝZA ŠIFRY

Blokové symetrické šifry pracují na principu substituce a permutace nad blokem dat v několika úrovních (kola šifry). Šifrování jednoho bloku dat se provádí tak, že v prvním kole se provede substituce podle předpisu, který je realizován tzv. S-boxem (vyhledávací tabulka), poté se provede permutace dat v bloku přehozením pořadí bitů a sloučení s klíčem, nejčastěji operací exklusive or. Výsledný blok tvoří vstup dalšího kola a postup se opakuje.

Dešifrování se provádí stejným způsobem pouze v opačném pořadí provádění operací(nebo jen aplikace klíče) a začátek je v posledním kole šifry a postupuje se z konce na začátek. Odtud tedy název symetrické šifry.

Pro nás je důležitou částí substituce, kdy S–box provádí nelineární mapování. Hlavním důvodem je, že aplikace S-boxu je jediná operace vnášející nelinearitu. Při kryptoanalýze je třeba nelinearitu nějakým způsobem eliminovat. Diferenciální kryptoanalýza hledá nejvyšší pravděpodobnost výskytu diference výstupu na diferenci vstupu pro všechny dvojice vstupů s konstantním rozdílem. Diferenciální analýza je útok zvoleným textem což znamená, že útočník zná šifrovaný text a odpovídající otevřený (nešifrovaný) text, který si mohl zvolit a snaží se zjistit klíč. Zvoleným textem tedy budou dvojice vstupních dat.

2.1 ANALÝZA S-BOXU

S-box bývá implementován vyhledávací tabulkou, příklad S–boxu pro 4 bitový vstup je na obr. 1. Nejprve tedy najdeme diferenci pro dvojice vstupních textů, která indukuje určitou výstupní diferenci s největší pravděpodobností. Zkoumáme tedy diference všech možných vstupů ΔX S-boxu a k nim příslušné výstupní ΔY diference. Diference získáme operací exklusive or pro dva bloky dat.

$$\Delta X = X_1 \oplus X_2$$
$$\Delta Y = Y_1 \oplus Y_2$$

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

Obr. 1: *Příklad S–boxu*

Získaná data můžeme zapsat do tabulky, čímž vytvoříme Distribuční tabulku diferencí pro daný S-box, kde řádky vyjadřují vstupní diferenci a sloupce výstupní diferenci. Každý prvek tabulky udává počet výskytů příslušné hodnoty diference výstupu při vstupní diferenci. V ideálním případě by měla být pravděpodobnost výstupní diference na vstupní diferenci rovna $1/2^n$ kde n je počet bitů vstupu. To ovšem není možné a diferenciální kryptoanalýza právě využívá vhodného páru vstupní a výstupní diference, kdy je tato pravděpodobnost daleko vyšší.

2.2 KONSTRUKCE DIFERENCIALNÍ CHARAKTERISTIKY

Jakmile máme k dispozici informace o diferencích S-boxů daná šifry, můžeme vytvořit vhodnou diferenciální charakteristiku celé šifry. Dalším krokem je útok na šifru odhalením klíče v posledním kole šifry. Zvolíme tedy takový pár (ΔX, ΔY) diferencí pro který je nejpravděpodobnější jejich výskyt. Ten nalezneme v Distribuční tabulce.

		Output Difference															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Input Difference	0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	1	0	0	0	2	0	0	0	2	0	2	4	0	4	2	0	0
	2	0	0	0	2	0	6	2	2	0	2	0	0	0	0	2	0
	3	0	0	2	0	2	0	0	0	0	4	2	0	2	0	0	4
	4	0	0	0	2	0	0	6	0	0	2	0	4	2	0	0	0
	5	0	4	0	0	0	2	2	0	0	0	4	0	2	0	0	2
	6	0	0	0	4	0	4	0	0	0	0	0	0	2	2	2	2
	7	0	0	2	2	2	0	2	0	0	2	2	0	0	0	0	4
	8	0	0	0	0	0	0	2	2	0	0	0	4	0	4	2	2
	9	0	2	0	0	2	0	0	4	2	0	2	2	2	0	0	0
	A	0	2	2	0	0	0	0	0	6	0	0	2	0	0	4	0
	B	0	0	8	0	0	2	0	2	0	0	0	0	0	2	0	2
	C	0	2	0	0	2	2	2	0	0	0	0	2	0	6	0	0
	D	0	4	0	0	0	0	0	4	2	0	2	0	2	0	2	0
	E	0	0	2	4	2	0	0	0	6	0	0	0	0	0	2	0
	F	0	2	0	0	6	0	0	0	0	4	0	2	0	0	2	0

Obr. 2: *Příklad distribuční tabulky diferencí pro daný S–box*

2.3 ZÍSKÁNÍ KLÍČE

Jakmile máme diferenciální charakteristiku šifry můžeme se pokusit odhalit část klíče v posledním kole. Zvolíme nejvhodnější pár vstupní a výstupní diference (ΔX, ΔY), jejichž pravděpodobnost výskytu je nejvyšší. Volíme vhodné data tak aby jejich diference odpovídala ΔY. Poté šifrujeme data s pomocí hádaného klíče. Procházíme tedy vždy všechny kombinace pro určitou část klíče. Po šifrování porovnáváme, zda výstupní diference odpovídají pravděpodobnostem z distribuční tabulky. Testujeme zde jsme získali očekávanou diferenci - ΔX, nebo ne. Stejný postup opakujeme pro další klíče pro dostatečné množství dvojic zpráv.

Dobrým pravidlem pro počet párů zpráv je $N_D = c / p_D$, kde pD je diferenciální charakteristika pravděpodobnosti výskytu správného páru a c je nějaká malá konstanta.

Po provedení dostatečného množství šifrování bude klíč s nejvyšší hodnotou nejpravděpodobněji náš hledaný klíč. Pravděpodobnost pak lze vyjádřit vztahem

$$prob = count / N_D$$

kde count je počítadlo pro každý klíč.

2.4 SKUTEČNÁ ŠIFRA

U skutečných šifer je třeba se vyrovnat s relativně velkým počtem S-boxů, které mohou být i mnohem větší, než je uvedený příklad. S tím souvisí volba vstupních dvojic textů tak, aby se nám podařilo aktivovat při šifrování ty S-boxy, s těmi vstupy, které jsou nejvhodnější pro diferenciální kryptoanalýzu.

3 ZÁVĚR

V této práci byl popsán útok na blokovou symetrickou šifru diferenciální analýzou. Tento princip může být použit pro libovolnou substitučně-permutační šifru. Rozdílem obvykle bývá pouze délka klíče a lepší implementace S-boxu, která se snaží minimalizovat pravděpodobnost výskytu páru vstupních a výstupních diferencí a tudíž i bezpečnost algoritmu tím že řešení se stává výpočetně příliš náročné.

V rámci řešení ročníkového projektu budu implementovat algoritmus, který na vstup dostane popis libovolné blokové šifry, provede diferenciální analýzu a pokusí se odhalit pravděpodobný klíč.

LITERATURA

[1] Heys, H. M.: A Tutorial on Linear and Differential Cryptanalysis, http://www.engr.mum.ca/~howard/PAPERS/ldc_tutorial.pdf

[2] Stinson, S. D.: Cryptography : Theory and Practice, CRC Press, 2002 http://isg.rhul.ac.uk/msc/teaching/opt8/2001-2002/DiffLinHandout.pdf