Pokročilá kryptologie

Lineární kryptoanalýza

prof. Ing. Róbert Lórencz, CSc.

České vysoké učení technické v Praze
Fakulta informačních technologií
Katedra informační bezpečnosti

Obsah přednášky

- Klíče
- Kryptoanalýza
- Druhy útoků
- Lineární kryptoanalýza (LK)
- Základní vlastnosti

Klíče

Slabý klíč

Klíč, jehož zvláštní matematické vlastnosti umožňují snadné prolomení šifry.

Slabý klíč v DES

Zvolme např. klíč $k = (0101010101010101)_{16}$. Všechny rundovní (pod)klíče generované z k jsou stejné. Protože DES je algoritmus Feistelova typu, vzájemně se působení podklíčů vyruší a $E_k(\mathrm{OT})=\mathrm{OT}$!

Poloslabý klíč v DES

Klíče $k_1 \neq k_2$, jsou poloslabé, platí-li:

$$E_{k_1}(E_{k_2}(OT)) = OT\ .$$

Kryptoanalýza

Kryptoanalýza

Věda o zkoumání a prolamování šifer bez znalosti k. Blokové šifry nejčastěji analyzujeme pomocí lineární a diferenciální kryptoanalýzy.

Lineární kryptoanalýza

Hledá lineární závislosti (aproximace) k jednotlivým akcím šifer.

Diferenciální kryptoanalýza

Hledá závislosti (rozdíly) mezi vstupy a výstupy šifer.

Druhy útoků

- Útok hrubou silou — zkoušíme všechny možné klíče, a právě z tohoto důvodu bývá často nereálný. U DES nutno zkusit až $2^{56} = 64P \approx 7.2 \cdot 10^{16}$ klíčů!
- Útok se znalostí šifrového textu — známe jen ŠT. Tento útok může uspět, je-li je k nebo OT předvídatelný. V opačném případě jde o velmi složitý proces.
- Útok se znalostí otevřeného textu — máme vzorky jak ŠT, tak korespondujících OT, z nichž se snažíme nalézt k, nebo další informace o šifrovacím systému.
- Útok se znalostí vybraných otevřených textů — máme vzorky ŠT pro libovolný, i námi zadaný, OT. Cílem tohoto útoku je získání informací o slabinách šifrovacích procesu.
- Útok se znalostí vybraných šifrových textů — máme ŠT a k nim získáme OT bez znalosti k, který se snažíme nalézt.

Lineární kryptoanalýza (LK)

Základní vlastnosti

- LK používaná pro kryptoanlýzu blokových šifer.
- LK využívá vysokou pravděpodobnosti výskytu lineárních vyjádřeních zahrnujících bity OT, bity ŠT a bity podklíčů pro danou rundu.
- LK hledá lineární závislosti mezi vstupy a výstupy S-boxů.
- LK je útok ze znalosti OT a odpovídajícího ŠT, nemůžeme si je ale zvolit.
- Základní myšlenka je aproximovat operace částí šifry s výrazem, který je lineární. Operace mezi jednotlivými bity jsou bitovými operacemi exclusive-OR "$\oplus$"modulo 2. Obecně můžeme vyjádřit výraz ve formě:

$$X_1 \oplus X_2 \oplus \ldots \oplus X_u \oplus Y_1 \oplus Y_2 \ldots \oplus Y_v = 0, \qquad (1)$$

Lineární kryptoanalýza (LK)

Základní vlastnosti

- kde X_i je i-tý bit vstupu $X = [X_1, X_2 \ldots X_u]$ a Y_j je j-tý bit výstupu $Y = [Y_1, Y_2 \ldots Y_v]$
- Celá rovnice vyjadřuje sumu exkluzívních součtu modulo 2 vstupních bitů a výstupních bitů.

Cíl LK

Nalézt taková vyjádření, které jsou ve tvaru (1) a mají vysokou či naopak nízkou pravděpodobnost výskytu.

Příklad:

- Mějme libovolné 2 náhodné bity a a b.
- Pravděpodobnost, že bude platit $a \oplus b = 0$ je $1/2$.
- Pokud však neplatí, že jsou náhodné je možné zjistit odchylku v pravděpodobnosti $1/2$.
- Této skutečnosti využívá LK.

Lineární kryptoanalýza (LK)

Odchylka lineární pravděpodobností - linear probability bias (LPB)

- Pokud máme pravděpodobnost p toho, že platí libovolně zvolený výraz (1), pak odchylku *LPB* spočítáme jako $p - 1/2$.
- Její velikost je potom $|p - 1/2|$.
- Čím je větší velikost *LPB*, tím lze lépe analyzovat danou šifru.
- $p = 1$ implikuje, že lineární výraz (1) je perfektní reprezentací chování šifry a že šifra má katastrofické slabiny.
- Když $p = 0$ potom výraz (1) reprezentuje afinní závislosti v šifře a také indikuje katastrofické slabiny šifry.
- Pro modulo 2 operace je afinní funkce jednoduše komplementární k lineární funkci.
- Jak lineární, tak také afinní aproximace chování šifry indikuje pro $p > 1/2$ nebo $p < 1/2$ snadnou proveditelnost LK. Pro oba případy budeme používat lineární aproximaci - výraz (1)

Lineární kryptoanalýza (LK)

Otázka: Jak zkonstruovat výraz, který je "silně lineární"a jak to využít?

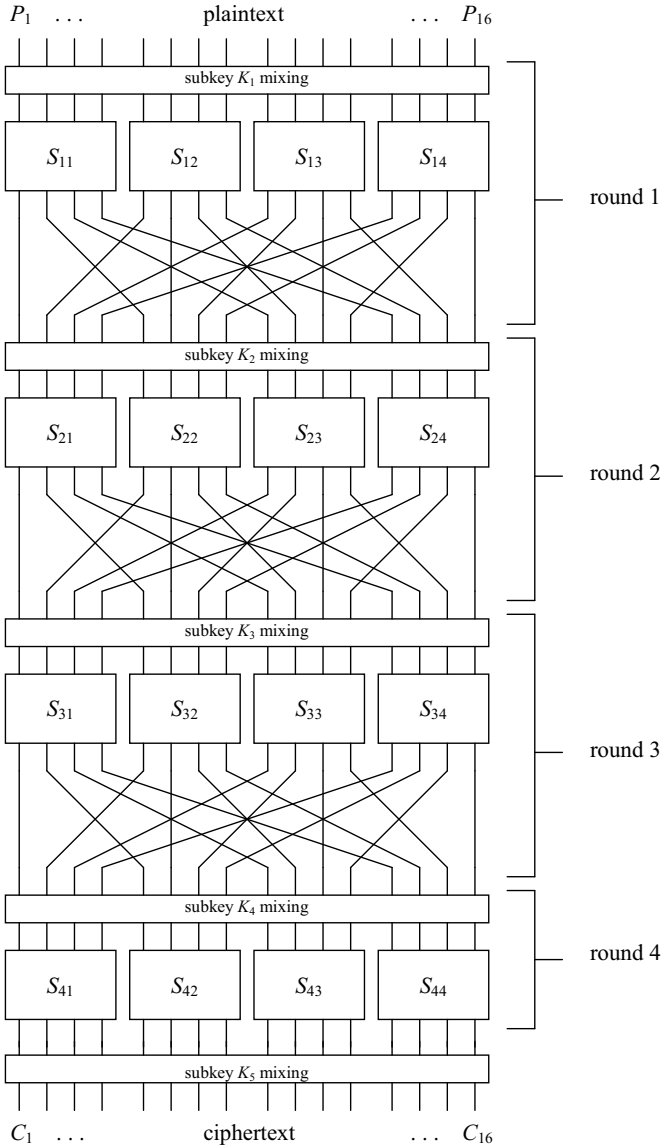
- Uvažujeme vlastnosti nelineárních součástí šifer: S-boxů.
- Pokud jsou lineární vlastnosti S-boxu "zjistitelné", potom je možné vytvořit lineární aproximace mezi vstupními a výstupními bity S-boxu.
- Následně je možné zřetězit lineární aproximace S-boxů takovým způsobem, že se můžou vyrušit "mezilehlé"bity (bity prostupující mezi S-boxy).
- Potom lineární výraz popisující chování šifry obsahuje jen bity OT a bity poslední rundy a má velký *LPB*.
- Bity podklíčů jednotlivých rund jsme přesunuli na pravou stranu lineárního výrazu s tím, že v sumě můžou mít hodnotu "0"nebo "1". To způsobuje jen změnu znaménka u *LPB*. Při hledání vhodné lineární aproximace nás zajímá ale jenom velikost *LPB*, tj. její absolutní hodnota.

SPN

Substituční a permutační síť (SPN)

- Mějme základní Substituční a permutační síť na obrázku (následující slide).
- SPN je šifrou obsahující substituční bloky, transpoziční propojovací sítě a operace pro generování podklíčů.
- SPN má 16-bitové slovo, tj. vstupní a výstupní blok je délky 16 bitů.
- SPN je jednoduchá bloková šifra, na které lze ukázat základní principy LK. Tyto principy lze zobecnit na složitější blokové šifry, jako jsou: DES, AES atd.
- SPN rozděluje 16bitový blok do čtyř 4bitových podbloků. Každý podblok vstupuje do S-boxu, kde je provedená substituce 4 bitů na 4 bity.
- Velmi důležitou vlastnosti S-boxu je nelineární mapování vstupu na výstup, tj. výstupní bity nemůžou být reprezentovány jako nějaká lineární operace vstupních bitů.

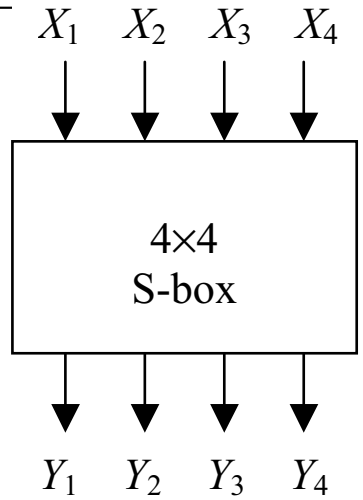
Substituční a permutační síť (SPN)



SPN

S-box

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



Permutace

Vstup	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Výstup	1	5	9	13	2	6	10	14	3	7	11	15	4	8	12	16

SPN

Substituční a permutační síť (SPN)

- SPN používá stejné S-boxy pro každé podslovo a v každé rundě (rozdíl oproti DES).
- Substituce je odvozená z S-boxu DES
- Permutace v jednotlivých rundách je stejná. Provádí jednoduchou transpozici bitů nebo permutaci pozici bitů. Permutace je dána permutační tabulkou.
- Permutace v poslední rundě nemá opodstatní a proto není prováděná.
- Podklíče jsou přičítány operaci XOR v každé rundě k prostupujícímu 16 bitovému slovu a také na konci 4. rundy z důvodu zabezpečení poslední substituce.
- Pro dešifrování se používá SPN v zpětném chodu. Znamená to, že S-box má inverzní substituci a tím musí byt zabezpečené i bijektivnost zobrazení S-boxem.

Piling-Up princip

- Ke konstrukci vztahu (1) je potřeba uvést některé základní principy.
- Uvažujme 2 náhodné proměnné X_1 a X_2.
- Nechť $X_1 \oplus X_2 = 0$ (ekvivalent $X_1 = X_2$) je lineární výraz.
- $X_1 \oplus X_2 = 1$ (ekvivalent $X_1 \neq X_2$) je afinní výraz.
- Předpokládejme, že pravděpodobnostní rozdělení pro X_1 je.

$$\Pr(X_1 = 0) = p_1 \quad \text{a} \quad \Pr(X_1 = 1) = 1 - p_1$$

- Dále předpokládejme, že pravděpodobnostní rozdělení pro X_2 je.

$$\Pr(X_2 = 0) = p_2 \quad \text{a} \quad \Pr(X_2 = 1) = 1 - p_2$$

Piling-Up princip

- Pokud jsou X_1 a X_2 vzájemně nezávislé, potom
  $\Pr(X_1 = 0, X_2 = 0) = p_1 p_2$,
  $\Pr(X_1 = 0, X_2 = 1) = p_1(1 - p_2)$
  $\Pr(X_1 = 1, X_2 = 0) = (1 - p_1)p_2$,
  $\Pr(X_1 = 1, X_2 = 1) = (1 - p_1)(1 - p_2)$.
- A můžeme psát:

$$\begin{aligned} \Pr(X_1 \oplus X_2 = 0) &= \Pr(X_1 = X_2) \\ &= \Pr(X_1 = 0, X_2 = 0) + \Pr(X_1 = 1, X_2 = 1) \\ &= p_1 p_2 + (1 - p_1)(1 - p_2). \end{aligned}$$

- Pokud si označíme $p_1 = 1/2 + \varepsilon_1$ a $p_2 = 1/2 + \varepsilon_2$, kde ε_1 a ε_2 jsou pravděpodobnostné odchylky a platí $-1/2 \leq \varepsilon_1, \varepsilon_2 \leq 1/2$, můžeme psát: $\Pr(X_1 \oplus X_2 = 0) = 1/2 + 2\varepsilon_1\varepsilon_2$

Piling-Up princip

- a LPB $\varepsilon_{1,2}$ výrazu $X_1 \oplus X_2 = 0$ je $\varepsilon_{1,2} = 2\varepsilon_1\varepsilon_2$.
- Tento závěr je možné rozšířit na víc než 2 náhodné proměnné . Pro proměnné od X_1 do X_n, které mají pravděpodobnosti $p_1 = 1/2 + \varepsilon_1$ až $p_2 = 1/2 + \varepsilon_n$ a pravděpodobnosti výrazu $X_1 \oplus \ldots \oplus X_n = 0$ platí tzv Piling-Up věta.

Piling-Up věta

Pro n nezávislých a náhodných binárních proměnných $X_1, X_2, \ldots, X_n$ platí

$$\Pr(X_1 \oplus X_2 \oplus \ldots \oplus X_n = 0) = 1/2 + 2^{n-1} \prod_{i=1}^{n} \varepsilon_i$$

nebo

$$\varepsilon_{1,2,\ldots,n} = 2^{n-1} \prod_{i=1}^{n} \varepsilon_i,$$

kde $\varepsilon_{1,2,\ldots,n}$ reprezentuje *LPB* výrazu $X_1 \oplus X_2 \oplus \ldots \oplus X_n = 0$.

Piling-Up princip

- Když $p_i = 0$ nebo $p_i = 1$ pro všechny i platí $\Pr(X_1 \oplus \ldots \oplus X_n = 0) = 0$ nebo 1.
- Když je jenom jedno $p_i = 1/2$ potom $\Pr(X_1 \oplus \ldots \oplus X_n = 0) = 1/2$.

Příklad:

- Při konstrukci lineární aproximaci šifer budou hodnoty X_i ve skutečnosti reprezentovat lineární aproximaci S-boxu.
- Mějme 4 nezávislé náhodné proměnné X_1, X_2, X_3 a X_4.
- Nechť $\Pr(X_1 \oplus X_2 = 0) = 1/2 + \varepsilon_{1,2}$ a $\Pr(X_2 \oplus X_3 = 0) = 1/2 + \varepsilon_{2,3}$.
- Dále uvažujme, že suma $X_1 \oplus X_3$ je vytvořena sečtením $X_1 \oplus X_2$ a $X_2 \oplus X_3$.
- Platí

$$\Pr(X_1 \oplus X_3 = 0) = \Pr([X_1 \oplus X_2] \oplus [X_2 \oplus X_3] = 0)$$

.

Piling-Up princip

- Sloučením 2 lineárních výrazů jsme dostali nový lineární výraz.
- Pokud předpokládáme, že náhodné proměnné $X_1 \oplus X_2$ a $X_2 \oplus X_3$ jsou nezávislé, můžeme použít Piling Up větu:

$$\Pr(X_1 \oplus X_3 = 0) = 1/2 + 2\varepsilon_{1,2}\varepsilon_{2,3}$$

- a tedy $\varepsilon_{1,3} = 2\varepsilon_{1,2}\varepsilon_{2,3}$.
- Jak ukážeme později, výrazy $X_1 \oplus X_2 = 0$ a $X_2 \oplus X_3 = 0$ jsou analogické lineární aproximaci S-boxu a výraz $X_1 \oplus X_3 = 0$ je analogický šifrové aproximaci, kde mezihodnota X_2 je eliminována.
- Reální analýza bude složitější vzhledem k počtu S-boxu, které jsou do ní zahrnuté.

Analýza šifrových součástí

- Uvažujme námi navrhnutý S-box, který má vstup $X = [X_1, X_2, X_3, X_4]$ a výstup $Y = [Y_1, Y_2, Y_3, Y_4]$.
- Všechny lineární aproximace můžou být vybrané pro tvorbu linearizační funkce a proto provedeme výpočet pravděpodobnosti *LPB* každou z nich.

Příklad:

- Pro S-box naši šifry uvažujme lineární výraz $X_2 \oplus X_3 \oplus Y_1 \oplus Y_3 \oplus Y_4 = 0$ nebo psáno $X_2 \oplus X_3 = Y_1 \oplus Y_3 \oplus Y_4$.
- Pokud postupně za X dosadíme všechny možné kombinace a z S-boxu získáme k daným vstupům všechny hodnoty Y pozorujeme, že pro 12 výstupů ze všech 16 možností náš výraz je pravdivý.
- Proto *LPB* je rovno $12/16 - 1/2 = 1/4$ (viz tabulka).

Lineární aproximace S-boxu

X_1	X_2	X_3	X_4	Y_1	Y_2	Y_3	Y_4	$X_2 \oplus X_3$	$Y_1 \oplus Y_3 \oplus Y_4$	$X_1 \oplus X_4$	Y_2	$X_3 \oplus X_4$	$Y_1 \oplus Y_4$
0	0	0	0	1	1	1	0	0	0	0	1	0	1
0	0	0	1	0	1	0	0	0	0	1	1	1	0
0	0	1	0	1	1	0	1	1	0	0	1	1	0
0	0	1	1	0	0	0	1	1	1	1	0	0	1
0	1	0	0	0	0	1	0	1	1	0	0	0	0
0	1	0	1	1	1	1	1	1	1	1	1	1	0
0	1	1	0	1	0	1	1	0	1	0	0	1	0
0	1	1	1	1	0	0	0	0	1	1	0	0	1
1	0	0	0	0	0	1	1	0	0	1	0	0	1
1	0	0	1	1	0	1	0	0	0	0	0	1	1
1	0	1	0	0	1	1	0	1	1	1	1	1	0
1	0	1	1	1	1	0	0	1	1	0	1	0	1
1	1	0	0	0	1	0	1	1	1	1	1	0	1
1	1	0	1	1	0	0	1	1	0	0	0	1	0
1	1	1	0	0	0	0	0	0	0	1	0	1	0
1	1	1	1	0	1	1	1	0	0	0	1	0	1

Analýza šifrových součástí

- Pro rovnici $X_1 \oplus X_4 = Y_2$ je $LPB = 0$, viz tabulka: $8/16 - 1/2 = 0$.
- Pro rovnici $X_3 \oplus X_4 = Y_1 \oplus Y_4$ je $LPB = 2/16 - 1/2 = -3/8$.
  V tomto případě nejlepší aproximací je afinní aproximace vzhledem k znaménku $-$.
- Úspěch útoku je založený na velikosti LPB.
- Je zřejmé, že afinní aproximace může být použitá jako ekvivalent k lineární aproximaci.
- Úplné vyčíslení všech lineárních aproximací našeho S-boxu je uvedeno v následující tabulce.
- Každý element v tabulce reprezentuje počet shod mezi lineární rovnici reprezentovanou v hexadecimálním formě jako "Input Sum"a sumou výstupních bitů reprezentovaných v hexadecimální formě jako "Output Sum"mínus "8".

Lineární aproximační tabulka

Input Sum	Output Sum 0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	+8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	−2	−2	0	0	−2	+6	+2	+2	0	0	+2	+2	0	0
2	0	0	−2	−2	0	0	−2	−2	0	0	+2	+2	0	0	−6	+2
3	0	0	0	0	0	0	0	0	+2	−6	−2	−2	+2	+2	−2	−2
4	0	+2	0	−2	−2	−4	−2	0	0	−2	0	+2	+2	−4	+2	0
5	0	−2	−2	0	−2	0	+4	+2	−2	0	−4	+2	0	−2	−2	0
6	0	+2	−2	+4	+2	0	0	+2	0	−2	+2	+4	−2	0	0	−2
7	0	−2	0	+2	+2	−4	+2	0	−2	0	+2	0	+4	+2	0	+2
8	0	0	0	0	0	0	0	0	−2	+2	+2	−2	+2	−2	−2	−6
9	0	0	−2	−2	0	0	−2	−2	−4	0	−2	+2	0	+4	+2	−2
A	0	+4	−2	+2	−4	0	+2	−2	+2	+2	0	0	+2	+2	0	0
B	0	+4	0	−4	+4	0	+4	0	0	0	0	0	0	0	0	0
C	0	−2	+4	−2	−2	0	+2	0	+2	0	+2	+4	0	+2	0	−2
D	0	+2	+2	0	−2	+4	0	+2	−4	−2	+2	0	+2	0	0	+2
E	0	+2	+2	0	−2	−4	0	+2	−2	0	0	−2	−4	+2	−2	0
F	0	−2	−4	−2	−2	0	+2	0	0	−2	+4	−2	−2	0	+2	0

Analýza šifrových součástí

- Pokud podělíme hodnoty v tabulce číslem 16 dostaneme *LPB* pro jednotlivé lineární kombinace podle vstupních a výstupních bitů.
- Hexadecimální hodnoty reprezentují sumu, kde binární hodnoty vyjadřuji, které proměnné jsou zahrnuté do sumy.
- Pro lineární kombinací vstupních proměnných reprezentovaných jako $a_1 \cdot X_1 \oplus a_2 \cdot X_2 \oplus a_3 \cdot X_3 \oplus a_4 \cdot X_4$, kde $a_i \in 0, 1$ a "$\cdot$"je binární AND, je hexadecimální hodnota reprezentována binární hodnotou $a_1 a_2 a_3 a_4$ (a_1 je MSB).
- Analogický pro lineární kombinací výstupních bitů $b_1 \cdot Y_1 \oplus b_2 \cdot Y_2 \oplus b_3 \cdot Y_3 \oplus b_4 \cdot Y_4$, kde $b_i \in 0, 1$, hexadecimální hodnotu reprezentuje vektor $b_1 b_2 b_3 b_4$.
- *LPB* lineární rovnice $X_3 \oplus X_4 = Y_1 \oplus Y_4$ (hexadecimální vstup 3 a hexa výstup 9) je $-6/16 = -3/8$ a pravděpodobnost, že lineární rovnice je pravdivá je $1/2 - 3/8 = 1/8$.

Základní vlastnosti vyjádřené lineární aproximační tabulkou

- První řádek a sloupec tabulky má $LPB = 0$ kromě vstupu "0"a výstupu "0"(proč?).
- Suma libovolného řádku a sloupce je vždy rovná $+8$ nebo -8 (proč?).

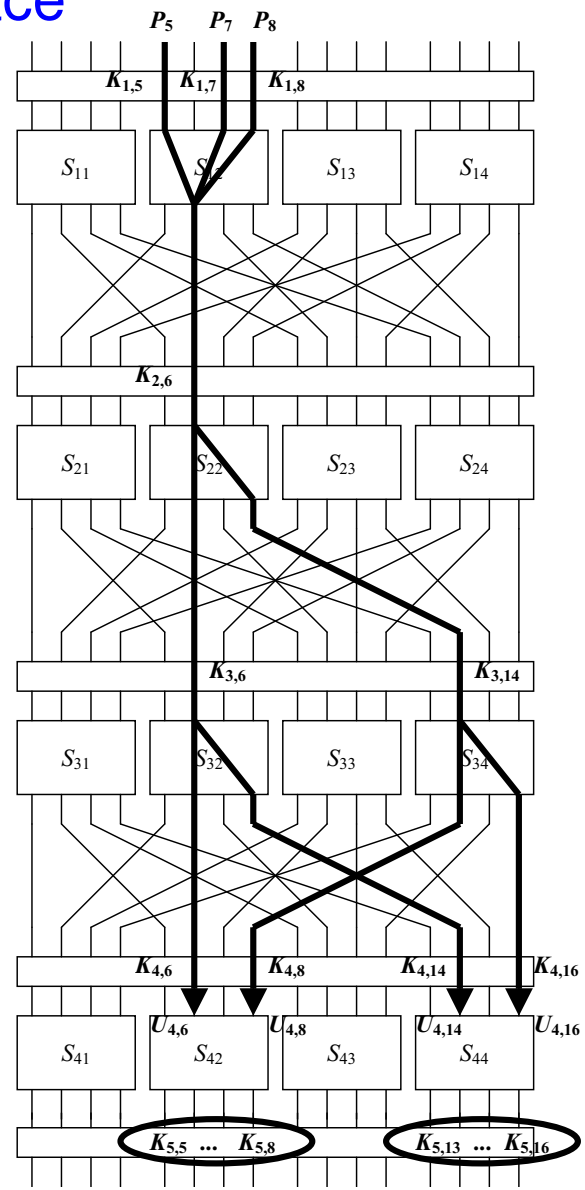
Vytvoření lineární aproximace pro SPN

- Postupným vytvářením lineárních aproximací pro jednotlivé S-boxy dostáváme data, které nám umožňují vytvářet lineární aproximací celé SPN ve formě (1).
- S vytvářením lineární aproximace zahrnující bity OT a datové bity z výstupu předposlední rundy S-boxů nám umožňuje provést útok na bity podklíče v následující rundě (poslední).
- Viz následující příklad.

Příklad lineární aproximace SPN

- Uvažujme aproximaci zahrnující $S_{1,2}, S_{2,2}, S_{3,2}, S_{3,4}$ tak jak je to zobrazené na následujícím obrázku.
- Obrázek znázorňuje vývoj lineárního výrazu pro první 3 rundy SPN (ne pro 4 rundy).
- V následujícím si ukážeme jakým způsobem budou odvozeny bity podklíče po poslední rundě.
- Použijeme následující aproximace S-boxů:
  - $S_{12} : X_1 \oplus X_3 \oplus X_4 = Y_2$ s pravděpodobností $12/16$ a $LPB = +1/4$
  - $S_{22} : X_2 = Y_2 \oplus Y_4$ s pravděpodobností $4/16$ a $LPB = -1/4$
  - $S_{32} : X_2 = Y_2 \oplus Y_4$ s pravděpodobností $4/16$ a $LPB = -1/4$
  - $S_{34} : X_2 = Y_2 \oplus Y_4$ s pravděpodobností $4/16$ a $LPB = -1/4$
- $P = [P_1, P_2, \ldots, P16]$ je 16 bitový OT. $U_i(V_i)$ je 16-bitový blok bitů vstupu (výstupu) rundy i S-boxu a $U_{i,j}$ ($V_{i,j}$) jsou j-ty bit bloku $U_i(V_i)$ (kde bity jsou číslované od 1 do 16 zleva doprava - viz obrázek).

Ukázka lineární aproximace



Příklad lineární aproximace SPN

- Dále nechť K_i reprezentuje bity podklíče bloku, které jsou xorované se vstupem do rundy i, s výjimkou toho, že K_5 je klíč xorovaný s výstupem rundy 4.
- $U_1 = P \oplus K_1$. S použitím lineární aproximace 1. rundy můžeme psát:

$$V_{1,6} = U_{1,5} \oplus U_{1,7} \oplus U_{1,8} = (P_5 \oplus K_{1,5}) \oplus (P_7 \oplus K_{1,7}) \oplus (P_8 \oplus K_{1,8}) \quad (2)$$

  S pravděpodobnosti $3/4$.
- Pro aproximaci ve 2. rundě:

$$V_{2,6} \oplus V_{2,8} = U_{2,6} = V_{1,6} \oplus K_{2,6}$$

  S pravděpodobnosti $1/4$.

LK II

- Dosazením za $V_{1,6}$ z rovnice (2) s pravděpodobností $3/4$ dostáváme rovnici:

$$V_{2,6} \oplus V_{2,8} \oplus P_5 \oplus P_7 \oplus P_8 \oplus K_{1,5} \oplus K_{1,7} \oplus K_{1,8} \oplus K_{2,6} = 0, \quad (3)$$

  pro kterou platí pravděpodobnost $1/2 + 2(3/4 - 1/2)(1/4 - 1/2) = 3/8$, která plyne z Piling Up věty. $LPB = -1/8$.
- Předpokládáme, že aproximace S-boxů jsou nezávislé. Tento předpoklad není úplně korektní, co ale nemá vliv při použití na většinu šifer.
- Pro 3. rundu platí:

$$V_{3,6} \oplus V_{3,8} = U_{3,6} \text{ a } V_{3,14} \oplus V_{3,16} = U_{3,14}$$

  oba s pravděpodobností $1/4$.

LK III

- Pro $U_{3,6} = V_{2,6} \oplus K_{3,6}$ a $U_{3,14} = V_{2,8} \oplus K_{3,14}$ z předchozích dvou rovnic dostáváme:

$$V_{3,6} \oplus V_{3,8} \oplus V_{3,14} \oplus V_{3,16} \oplus V_{2,6} \oplus K_{3,6} \oplus V_{2,8} \oplus K_{3,14} = 0 \quad (4)$$

  s pravděpodobnosti $1/2 + +2(1/4 - 1/2)^2 = 5/8$ a $LPB = 1/8$
- Sloučením (3) a (4) dostáváme:

$$V_{3,6} \oplus V_{3,8} \oplus V_{3,14} \oplus V_{3,16} \oplus P_5 \oplus P_7 \oplus P_8 \oplus K_{1,5} \oplus$$

$$\oplus K_{1,7} \oplus K_{1,8} \oplus K_{2,6} \oplus K_{3,6} \oplus K_{3,14} = 0$$

- Platí: $U_{4,6} = V_{3,6} \oplus K_{4,6}$, $U_{4,8} = V_{3,14} \oplus K_{4,8}$, $U_{4,14} = V_{3,8} \oplus K_{4,14}$ a $U_{3,16} = V_{3,6} \oplus K_{4,16}$.

LK IV

- Na základě předchozího můžeme psát:

$$U_{4,6} \oplus U_{4,8} \oplus U_{4,14} \oplus U_{4,16} \oplus P_5 \oplus P_7 \oplus P_8 \oplus \sum_K = 0 \quad \text{,kde}$$

$$\sum_K = K_{1,5} \oplus K_{1,7} \oplus K_{1,8} \oplus K_{2,6} \oplus K_{3,6} \oplus K_{3,14} \oplus K_{4,6} \oplus K_{4,8} \oplus K_{4,14} \oplus K_{4,16}$$

- $\sum_K$ má fixní hodnotu a to buď 0 nebo 1 v závislosti na klíči šifry.
- Použitím Piling-Up věty pro předchozí výraz dostáváme pravděpodobnost: $1/2 + 2^3(3/4 - 1/2)(1/4 - 1/2)^3 = 15/32$ a $LPB = -1/32$.
- Pokud je $\sum_K$ je fixní, potom platí:

$$U_{4,6} \oplus U_{4,8} \oplus U_{4,14} \oplus U_{4,6} \oplus P_5 \oplus P_7 \oplus P_8 = 0 \qquad (5)$$

  s pravděpodobností $15/32$ pro $\sum_K = 0$ nebo $(1 - 15/32) = 17/32$ pro $\sum_K = 1$.
- Nyní máme lineární aproximaci 3 rund šifry SPN s velikosti $LPB = 1/32$.

LK - extrakce bitů klíče I

- Jakmile je lineární aproximace pro $R-1$ rund R rundovní šifry SPN s dostatečně velkým LPB nalezena, je možné provést útok na šifru SPN s cílem získaní bitů posledního podklíče.
- Lineární výraz (5) obsahuje vstupy do S-boxů S_{42} a S_{44} v poslední rundě. Pro každou dvojici OT a jemu příslušnému ŠT budeme zkoušet všech 256 hodnot vybrané části podklíče $[K_{5,5} \ldots K_{5,8}, K_{5,13} \ldots K_{5,16}]$.
- Pro každou hodnotu podklíče, která je zpětně substituovaná S-boxy S_{42} a S_{44} na hodnoty $[U_{4,5} \ldots U_{4,8}, U_{4,13} \ldots U_{4,16}]$ dosazené do (5) s hodnotami bitů příslušného OT P_5, P_7 a P_8 vyhodnotíme daný lineární výraz.
- V případě, že výraz (5) je pro daný případ pravdivý inkrementujeme čítač příslušný dané hodnotě podklíče.
- Hodnota čítače bude největší v absolutní hodnotě minus počet vzorků OT/ŠT pro předpokládanou hodnotu podklíče.

LK - extrakce bitů klíče II

- Odchylka bude kladná nebo záporná v závislostí na hodnotách bitů podklíče zahrnutých v $\sum_K$. Když $\sum_K = 0$ bude pravděpodobnost lineární aproximace (5) menší než $1/2$ a v případě $\sum_K = 1$ bude pravděpodobnost větší než $1/2$.
- Následující tabulka představuje část výsledku z experimentu prováděného s 10000 páry OT/ŠT (kompletní tabulka má 256 položek). Hledaná část podklíče $[K_{5,5} \ldots K_{5,8}, K_{5,13} \ldots K_{5,16}] = [0010\ 0100]$.
- Výpočet $|bias| = |LPB|$je:

$$|bias| = |count - 5000|/10000$$

- Jak je z tabulky patrné, největší $|bias|$ je pro hodnotu částí podklíče $[2, 4]$.

Lineární aproximační tabulka

partial subkey $[K_{5,5}...K_{5,8}, K_{5,13}...K_{5,16}]$	| bias |	*partial subkey* $[K_{5,5}...K_{5,8}, K_{5,13}...K_{5,16}]$	| bias |
1 C	0.0031	2 A	0.0044
1 D	0.0078	2 B	0.0186
1 E	0.0071	2 C	0.0094
1 F	0.0170	2 D	0.0053
2 0	0.0025	2 E	0.0062
2 1	0.0220	2 F	0.0133
2 2	0.0211	3 0	0.0027
2 3	0.0064	3 1	0.0050
2 4	**0.0336**	3 2	0.0075
2 5	0.0106	3 3	0.0162
2 6	0.0096	3 4	0.0218
2 7	0.0074	3 5	0.0052
2 8	0.0224	3 6	0.0056
2 9	0.0054	3 7	0.0048

LK - Vyhodnocení

- Experimentálně určený $|bias|$ má hodnotu $0,0336$ a je velmi blízký teoreticky vypočítané hodnotě $1/32 = 0,03125$.
- Odchylka experimentální hodnoty a teoretické je také způsobená menším počtem testovaných dvojic OT/ŠT a také neúplnou vzájemnou nezávislosti vzorků.