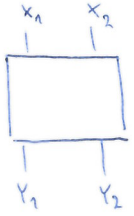
Lineární kryptoanalýza, aproximace S-Boxů, lineární aproximační funkce, extrakce bitů klíče.

⇒ Hledáme lineární aproximaci jednotlivých součástí šifry
- typicky aproximujeme SBoxy ⇒ používá se u blokové šifry

⇒ K účelům potřebujeme znát OT a ST, ale nemusíme si je psát
⇒ obecný tvar $X_1 \oplus \dots X_n \oplus \dots Y_1 \oplus \dots Y_n = 0$

⇒ v ideálním případě by výstup SBoxu měl být lin. nezávislý na vstupu
⇒ $P(A = B) = 1/2$ pro 1 bit

⇒ spočítáme odchylku od $1/2$ na obě strany = LINEAR PROBABILITY BIAS
⇒ čím větší LPB je, tím lépe se nám bude aproximovat



A my chceme závislost

$P(x_1 = 0) = p_1$ $P(x_2 = 0) = p_2$
$P(x_1 = 1) = 1 - p_1$ $P(x_2 = 1) = 1 - p_2$

Řekněme x_1 a x_2 jsou nezávislé ⇒ $P(x_1 = 0, x_2 = 0) = p_1 p_2$
$P(x_1 = 0, x_2 = 1) = p_1 (1 - p_2)$
⋮

⇒ $P(x_1 \oplus x_2 = 0) = p_1 p_2 + (1 - p_1)(1 - p_2)$ ⇒ odchylka od $1/2$ značíme ε_1 a ε_2
$P(x_1 \oplus x_2 = 0) = 1/2 + 2\varepsilon_1 \varepsilon_2$

PILING UP PRINCIP: zobecnění se dokazuje ⇒

$$P(x_1 \oplus x_2 \oplus \dots \oplus x_n) = 1/2 + 2^{n-1} \cdot \prod \varepsilon_i$$

Postup ⇒ Vybereme (vhodnou) rovnici, která aproximuje SBox
Vybereme si vhodnou ⇒ všechna a spočítáme LPB našeho vzorku ⇒ STATISTICKY
Takto uděláme všech SBoxy
Postupně vyjadřujeme bity mimo SBoxů, to nám umožní Piling UP Princip
Uděláme aproximaci pro $R - 1$ a celkem R runt.

Pro každou dvojici OT - ST uhodneme všech 256 možností klíče jiné poslední runtu ⇒ TZN poslední SBoxy musíme projít od spodu (inverze)
Pokud hodnoty odpovídají, inkrementujeme čítač a hotovo.

⇒ Takto dostaneme jen úzkou množinu počet bitů klíče :(
MUSÍME TO OPAKOVAT

Diferenciální kryptoanalýza, analýza SBoxů, diferenciální apot. funkce, extrakce bitů klíče. Algebraická kryptoanalýza.

⇒ DIFF. KRYPTOANALÝZA

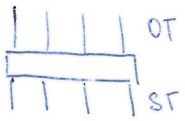
⇒ Využijeme pravděpodobnost výskytu dvojic rozdílů mezi 2 otevř. a výstupy

$$OT_1 + \Delta_0 = OT_2 \Rightarrow ST_1 + \Delta_S = ST_2$$

⇒ Ideálně je pravd. výskytu rozdílu $1/2^n$ ... n je poč. bitů X

⇒ Využijeme analýzu odchylek k prolomení.

⇒ ANALÝZA SBOXu



⇒ zajímají nás jaké Δ ST jsou k jakému Δ OT a nejsou pravděpodobnost

Zavedeme diferenční páry

X	Y	$\Delta X = 1011$ / $\Delta Y = ?$
0000	1110	0010
⋮	⋮	
1011	1100	0010
⋮	⋮	

Δ 1011

⇒ Např. pro $\Delta X = 1011$ nejsou pravděpodobnosti pro ΔY nejsou

⇒ my maximalizujeme odchylku od $1/2$

⇒ páry by měly být ideálně jedna

⇒ diference rozšíření na klíči ⇒ ten se využívá XORem

⇒ na základě charakteristik SBoxů určíme určitou šifru tak, že nejsou SBoxy

⇒ tuto použijeme diferenční páry s teoretickou odchylkou

⇒ stačí hrubá síla pravděpodobností SBoxů

⇒ Určíme pro R-1 runt a extrahujeme klíč. (bity)

⇒ pro $\forall$ klíč ⇒ zkusíme si zda se trefíme ⇒ stačí zkusit jen určité bity

⇒ pro $\forall$ dvojici OT a $\forall$ dvojici ST

⇒ tj. spočteme počet ... a jak je experimentálně ověříme ⇒ děláme čísla

ALGEBRAICKÁ KRYPTOANALÝZA

- řešíme soustavu polyn. rovnic nad tělesem
- založena AS ale i SYM krypto.

a) se spec. vl. se odvodí soustava

b) řeší se => NP Complete ?

- CHCEME - co nejméně rovnic, co nejm. stupně

ŘEŠENÍ - a) gaussova eliminace (odvodí a řádky)
b) linearizace
c) XL algoritmus

LINEARIZACE: a) k součinu nahradí novou proměnnou
b) řešíme soustavu
c) dosadí a opět

=> ke soustavě, které jsou přiřazené ?

Druhy postranních kanálů, časovací útoky. Útoky hrubou silou. Útok na formátování a doplnění zpráv.

Využíváme nedokonalostí v implementaci – porušuje předpoklady šifry

a) Časový – závislost na datech
b) Chybový – chyba závisí na datech
c) Odběrový postr. kanál – SPA, DPA
d) Elektromagnetický
e) Sociální kanál

ČASOVACÍ – login závisí na username ⇒ enumeraci
- kontrola session key – break v cyklu
- Square and Multiply – ciákulum – 2 many s odlišným časem

OBRANA: Maskování: aritmetické vlastnosti ⇒ např. mult. homomorfismus RSA

$$a^m \cdot b^m = (a \cdot b)^m \mod m$$

⇒ násobíme s maskou a tu pak odstraníme inverzí

$$ST = (x \cdot m^e)^d_m \Rightarrow m \cdot x^d \text{ ... jen } m^{-1} \text{ a hotovo}$$

DPA ... hypotéza závislosti spotřeby na vnitřní hodnotě a části klíče
... šifrujeme známé OT, změříme spotřebu
... sestavíme matici hypotéz ... ne + průběh a možný klíč
statisticky vyhodnotíme
⇒ např. korelace

⇒ a) Spotřeba závisí na Hammingově váze, Hammingově vzdálenosti ⇒ změna hodnoty

OBRANA: skrývání spotřeby

BRUTEFORCE: ukládáme ∀ klíč, nebo ∀ OT :(

=> chceme TIME × MEMORY TRADEOFF

$c = E_{k_1}(E_{k_2}(m))$

$D_{k_1}(c) = E_{k_2}(m)$ ...

Předpočítám a uložím

spočítám online a najdu kolizi

=> stejně to funguje i pro 3DES

RSA ... m .. 64 bitů ... ukládáme zprávu na 2 × 32 bitů

=> 18 % šance nálezu

=> $|M_1^e M_2^e|_n$ => bruteforce jedné hodnoty a druhou dopočítám z c a M_1^e

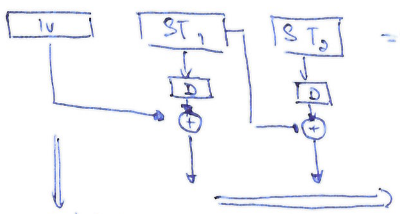
=> ochranou je padding

ÚTOKY NA FORMÁTOVÁNÍ A PADDING

↘ maskování, doplnění na délku, ochrana proti pozměnění, MAC

= Požadavky: Determinismus, Odstranění, Nejasnost útočníkovi

=> Padding oracle útok na CBC => zpráva odhalí chybu v paddingu × integritě



=> zná

Musíme znát padding schéma!

mění tak, že se změní odpověď

nevím co je tady, ale zjistím to tak, že se změní odpověď?

=> jde jen o to trefit délku paddingu

RSA ... útočník může modifikovat zprávu => přenásobit => hodnota se zvětší

... hodnota je menší jak modul => odmocnina => padding to ochrání?

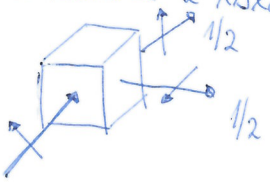
MI-PB 16

Kvantová kryptografie. Shorův algoritmus. Detekce odposlechu u BB84.

Bezpečnost garantována fyzikálními zákony

Kvantová distribuce klíče ⇒ detekce odposlechu?

- Nelze přesně měřit rychlost a hybnost a polohu
- Polarizační báze ↕ ↔ ⇒ pomocí hranolu a islandského ráječka



⇒ foton se nemůže rozdělit

BB84

1. → Bob odesílá data (fotony) v náhodné bázi × nebo +
2. → Alice přijímá v náhodné bázi + nebo ×
3. → Bob zveřejní použitou bázi ⇒ nechají si pouze společné hodnoty

⇒ Pokud Eva poslouchá, jak způsobí chyby.

→ Pokud zná bázi, tak v 50% případů udělá chyby ⇒ FYZIKA
Pokud nezná bázi, tak tipuje ⇒ 50%

⇒ ~ udělá 75% chyb ⇒ úspěšnost 25%

⇒ P detekce odposlechu = $1-\left(\frac{3}{4}\right)^n$

– obětujeme část bitů a otestujeme, zda sedí

Založeno na nemožnosti trvalý identický kopií

Qubit: objekt ∈ 2D Hilbertova prostor – fotony, elektrony, atomy

$|\psi\rangle = w_0|0\rangle + w_1|1\rangle$ ⇒ bázové vektory

w_0 a w_1 určují pravděpodobnost

$P[\text{Měření} = |k\rangle] = |w_k|^2,\ k \in \{0,1\}$

⇒ měřením superpozice stav zaniká

Heisenbergův princip: nelze přesně měřit v obou bázích zároveň

=> ke ∀ kvant. systému existuje přiřazený Hilbertův prostor => tj. má skalární součin $\langle\psi|\psi\rangle$

$\|\psi\| = \sqrt{\langle\psi|\psi\rangle}$

=> evoluci popisuje Schrödingerova rovnice $H|\psi(t)\rangle = -i\hbar \frac{\partial}{\partial t}(|\psi(t)\rangle)$

A^+ = transp. a komplex. sdružená A

$A^H = A^{-1}$ => unitární

$UU^+ = 1$ ... identita => zachovává skalární součin

Probabilistický registr: z 1 čísla je až 2^n možných výsledků, ale vidíme jen jeden

Kvantový registr: z 1 čísla je až 2^n -||- , výsledky mají amplitudy (i záporné) => některé se vyruší

Kvantová FT: vyvolává interferenci => zvýrazňuje frekvence

Shorův ALGO: FAKTORIZACE ~ $O(L^2 \log L \log\log L)$ .. L = bity čísla

$f_{y,n}(a) = y^a \bmod n$ ... n faktorizujeme

... y je nesoudělné s n

=> počet prvků grupy .. tj. řád prvku y

$f_{y,n}(a) = f_{y,n}(a+r)$ ... r je perioda

$y^r \equiv 1 \bmod n$ => $(y^{r/2} - 1)(y^{r/2} + 1) \equiv 0 \bmod n$ ... sudá mocnina

=> pro lichou bereme jiné y!

=> udělám $\gcd(y^{r/2} \pm 1, n)$! a musíme ověřit, že $y^{r/2} \not\equiv \pm 1 \bmod n$

→ zjištění periody => KVANTOVÝ POČÍTAČ + FT

a) registry R_1 a R_2 b) zvolíme y, q c) $R_1 = \{0 \dots q-1\}$ $R_2 = \{0 \dots 0\}$

d) paralelně vypočteme $f_{y,n}(a)$ a uložíme v R2

e) změříme pouze R2 => superpozice pro číslo k => zjistíme jaké R_1 vedlo na daný R_2

f) když dostaneme jednu z možností => tj. všechny exponenty, co vedou na periodu
– všechny hodnoty mají ale různý offset => nemůžeme odlišit

g) provedeme FT. ta odstraní offsety a já získám již zvýrazněnou periodu

MI-PB 17.

Bezpečnostní slabiny počítačových sítí a komunikačních protokolů, jejich zneužití

=> co znát: ISO/OSI

=> protokoly: ARP, IP, ICMP, TCP, UDP, DHCP, DNS, TLS/SSL, FTP, HTTP (ICMP, TCP, UDP: TRANP)

↳ leží nad IP

=> co je to firewall, NAT

=> princip fungování => na čem to může záviset => SRC, DST, PORT, Header, Flow, Content

=> fáze DHCP = Discovery, Offer, Request, Acknowledgement

=> PATŘÍ SEM:
- lidský faktor
- DHCP - unauth server / fals. client
- M.ITM - např. ARP
- 802.11 - deauth attack
- DNS / ICMP tunelling
- obecný určení těmto útokům

=> zmínit různé, co člověka napadne => DoS, DDoS, IP sequence prediction, Wifi útok, Bluetooth útok

=> napsillat Ping of Death,

Monitorování provozu v počítačových sítích včetně HW řešení pro ultra rychlé sítě

- intrusion detection systémy
- intrusion prevention systémy

- dnes ⇒ NEMEA ⇒ vytvoří FLOW a klasifikátor, který vyhledá
  - ⇒ v backendu se data zpracují a vystupem je ALERT
  - ⇒ machine learning, statistické metody ...

DŘÍVE: nfcat a nfsen (GUI pro nfdump)

⇒ vyhodnocují se rozličné parametry

⇒ typicky SLIDING WINDOW nebo LAST N-FLOWS