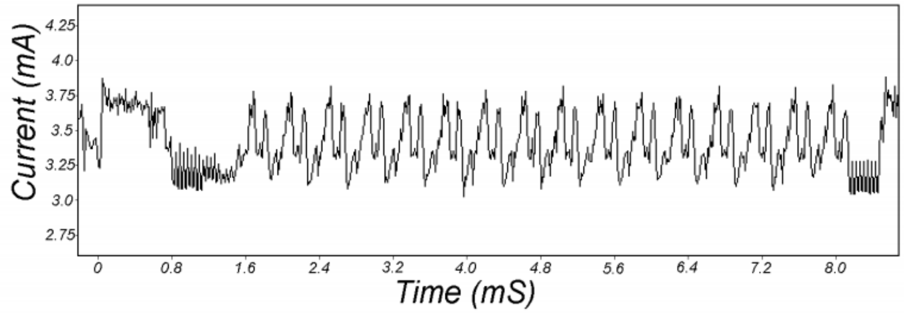
Block ciphers

More attacks on block ciphers

Attacks on the implementation

1. Side channel attacks:
   – Measure **time** to do enc/dec,   measure **power** for enc/dec

smartcard



[Kocher, Jaffe, Jun, 1998]

2. Fault attacks:
   – Computing errors in the last round expose the secret key k

⇒ do not even implement crypto primitives yourself …

Linear and differential attacks [BS'89,M'93]

Given *many* inp/out pairs, can recover key in time less than 2^{56} .

Linear cryptanalysis (overview) : let $c = DES(k, m)$

Suppose for random k,m :

$$\Pr\Big[\ \underbrace{m[i_1]\oplus\cdots\oplus m[i_r]}_{\text{subset of msg bits}}\ \bigoplus\ \underbrace{c[j_j]\oplus\cdots\oplus c[j_v]}_{\text{subset of ciphertext bits}} = \underbrace{k[l_1]\oplus\cdots\oplus k[l_u]}_{\text{subset of key bits}}\ \Big] = \tfrac{1}{2} + \varepsilon$$

For some ε. For DES, this exists with $\varepsilon = 1/2^{21} \approx 0.0000000477$

Linear attacks

$$\Pr\Big[\; m[i_1]\oplus\cdots\oplus m[i_r] \;\bigoplus\; c[j_j]\oplus\cdots\oplus c[j_v] \;=\; k[l_1]\oplus\cdots\oplus k[l_u] \;\Big] = \tfrac{1}{2} + \varepsilon$$

Thm: given $1/\varepsilon^2$ random $\big(m,\ c=\mathrm{DES}(k, m)\big)$ pairs then

$$k[l_1,\ldots,l_u] \;=\; \mathrm{MAJ}\Big[\; m[i_1,\ldots,i_r] \;\bigoplus\; c[j_j,\ldots,j_v] \;\Big]$$

with prob. $\geq 97.7\%$

$\Rightarrow$ with $1/\varepsilon^2$ inp/out pairs can find $k[l_1,\ldots,l_u]$ in time $\approx 1/\varepsilon^2$.

Linear attacks

For DES, $\varepsilon = 1/2^{21} \Rightarrow$

with 2^{42} inp/out pairs can find $k[l_1,\ldots,l_u]$ in time 2^{42}

Roughly speaking: can find 14 key "bits" this way in time 2^{42}

Brute force remaining $56-14=42$ bits in time 2^{42}

Total attack time $\approx 2^{43}$ ($\ll 2^{56}$) with 2^{42} random inp/out pairs

Lesson

A tiny bit of linearly in S_5 lead to a 2^{42} time attack.

$\Rightarrow$ don't design ciphers yourself !!

Quantum attacks

Generic search problem:

Let $f: X \longrightarrow \{0,1\}$ be a function.

Goal: find $x \in X$ s.t. $f(x)=1$.

Classical computer: best generic algorithm time = $O(|X|)$

Quantum computer [Grover '96] : time = $O(|X|^{1/2})$

Can quantum algorithms be built: unknown

Quantum exhaustive search

Given m, c=E(k,m) define

$$f(k) = \begin{cases} 1 & \text{if } E(k,m) = c \\ 0 & \text{otherwise} \end{cases}$$

Grover $\Rightarrow$ quantum computer can find k in time $O(\,|K|^{1/2}\,)$

DES: time $\approx 2^{28}$, AES-128: time $\approx 2^{64}$

quantum computer $\Rightarrow$ 256-bits key ciphers (e.g. AES-256)

End of Segment