Block Cipher

October 7, 2019

1 Attacks on the Implementation

1. Side Channel Attacks:
   - Measure **time** to do enc/dec, measure **power** for enc/dec
2. Fault Attacks:
   - Computing errors in the last round expose the secret key k.

2 Linear and Differential Attacks

Given *many* input/output pairs, we can recover the key with time less than 2^{56}.
Linear Cryptanalysis (overview): let $c = DES\left(k, m\right)$
Suppose for random k, m :

$$Pr\Big[m\left[i_1\right] \oplus \ldots \oplus m\left[i_r\right] \bigoplus c\left[j_j\right] \oplus \ldots \oplus c\left[j_v\right] = k\left[l_1\right] \oplus \ldots \oplus k\left[l_u\right]\Big] = \frac{1}{2} + \mathcal{E} \tag{1}$$

For some $\mathcal{E}$. For DES, this exists with $\mathcal{E} = \frac{1}{2^{21}} \approx 0.0000000477$.

First part is the subset of message bits, second part is the subset of cipher text bits, third part is the subset of key bits.

2.1 Linear Attacks

Theorem: given $\frac{1}{\mathcal{E}^2}$ random $\left(m, c = DES\left(k, m\right)\right)$ pairs then

$$k\left[l_{1,u}\right] = MAJ\left[m\left[i_1, \ldots, i_r\right] \oplus c\left[j_j, \ldots, j_v\right]\right] \text{with probability} \geq 97.7\%$$

$\implies$ with $\frac{1}{\mathcal{E}^2}$ input/output pairs we can find $k\left[l_1, \ldots, l_u\right]$ in time $\approx \frac{1}{\mathcal{E}^2}$.
For DES, $\mathcal{E} = \frac{1}{2^{21}} \implies$ with 2^{24} input/output pairs can find $k\left[I_1, \ldots, I_u\right]$ in time 2^{24}.
Roughly speaking: can find 14 key "bits" this way in time 2^{24}. Brute force remaining $56 - 14 = 42$ bits in time 2^{24}. Total attack time $\approx 2^{43}$ $\left(\ll_2^{56}\right)$ with 2^{24} random input/output pairs.
A tiny bit of linearity in S_5 lead to a 2^{42} time attack.

2.2 Quantum Attacks

Generic search problem: Let $f : X \to \{0, 1\}$ be a function. Goal: find $x \in X$

3 Exploiting the DRAM Rowhammer Bug to Gain Kernel Privileges

3.1 The DRAM subsystem