

When cryptanalysis meets side-channel

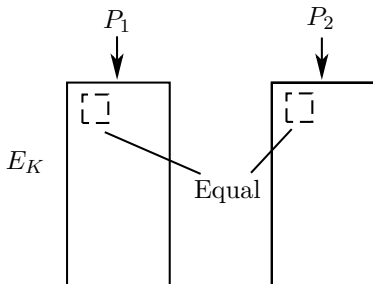
Alex Biryukov and Dmitry Khovratovich

University of Luxembourg

27.03.2007

Side-channel collision attacks

Detect the equality of intermediate variables — the *collision*:



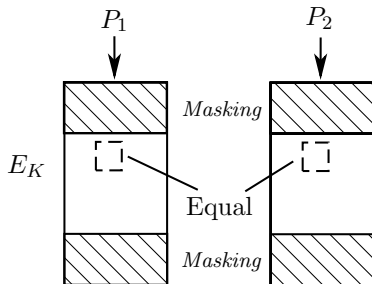
A collision after the first round of AES may imply:

$$S(a + k_1) + S(a + k_2) = S(b + k_1) + S(b + k_2),$$

which gives us information on k_1, k_2 (Schramm et al., 2004).

Side-channel collision attacks

Usually a few first and last rounds are masked:

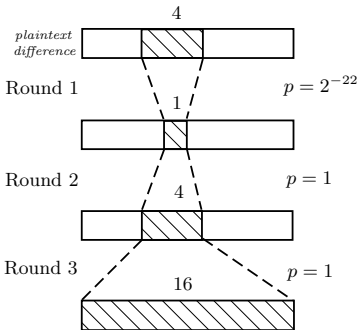


Handschuh and Preneel used a differential to obtain information on the subkey of an unmasked round of DES.

We propose to use powerful distinguishers that give information on **masked** subkeys.

Impossible collision attack on AES (3 masked rounds)

We use 3-round 2^{-22} differential:



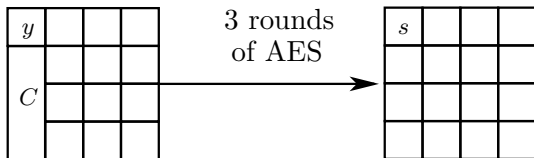
Our idea is to detect the **absence** of collisions.
A right pair reveals information about the first subkey.

We need 2^{19} measurements and about 2^{27} time.

However, we have to detect the absence of collisions accurately.

Multiset collision attack (4 masked rounds)

We guess 32 bits of the key and use 3-round Hilbert-Minier distinguisher



A right set has 256 collisions.

However, the overall complexity rises to 2^{27} measurements and 2^{51} offline steps.

Conclusions

Detecting the absence of collisions leaks information about the key.

A powerful r -round distinguisher can break through $r + 1$ masked rounds.

Two tools to construct such distinguishers.

Perhaps one should mask all 10 rounds of AES-128.