Two New Techniques of Side-Channel Cryptanalysis

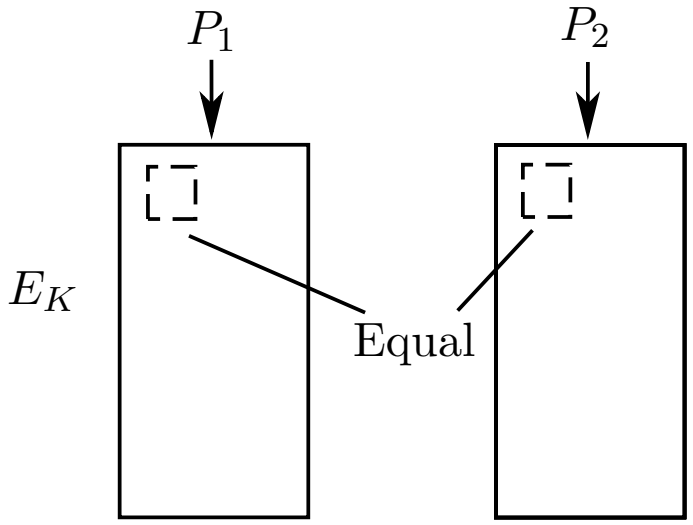
Alex Biryukov and Dmitry Khovratovich

University of Luxembourg

12.09.2007

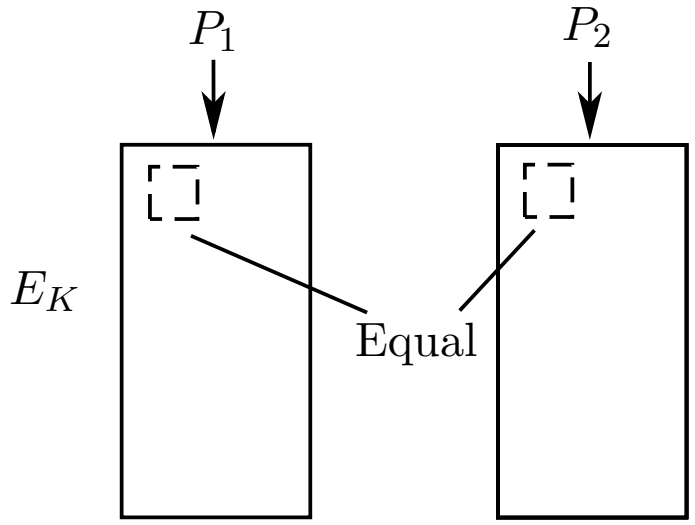
Side-channel collision attacks

Detect the equality of intermediate variables — the *collision* — measuring the power consumption:



Side-channel collision attacks

Detect the equality of intermediate variables — the *collision* — measuring the power consumption:



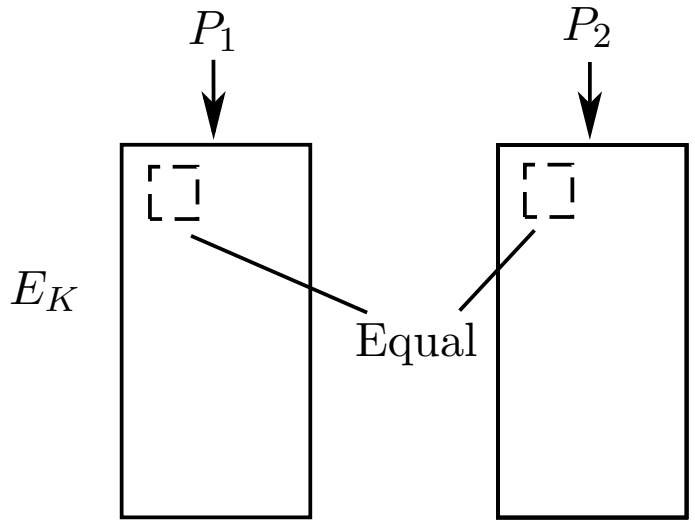
A collision after the first round of AES may imply:

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

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

Side-channel collision attacks

Detect the equality of intermediate variables — the *collision* — measuring the power consumption:



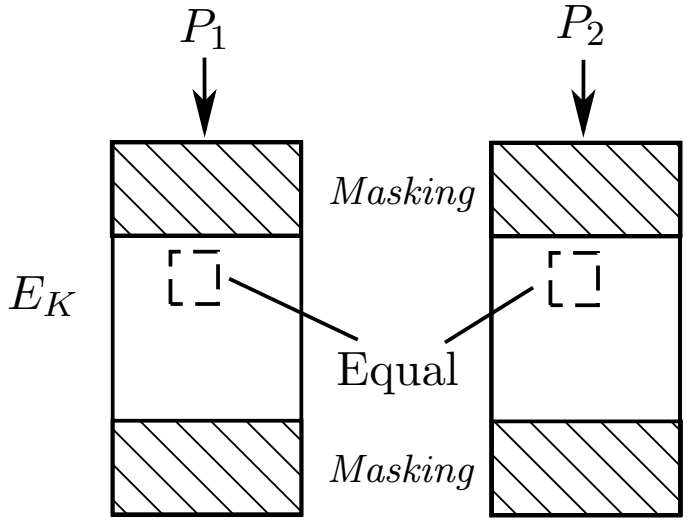
A collision after the first round of AES may imply:

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

which gives us information on k_1, k_2 (Schramm et al., 2004).
See also a recent attack on Alpha-MAC [BBKK07].

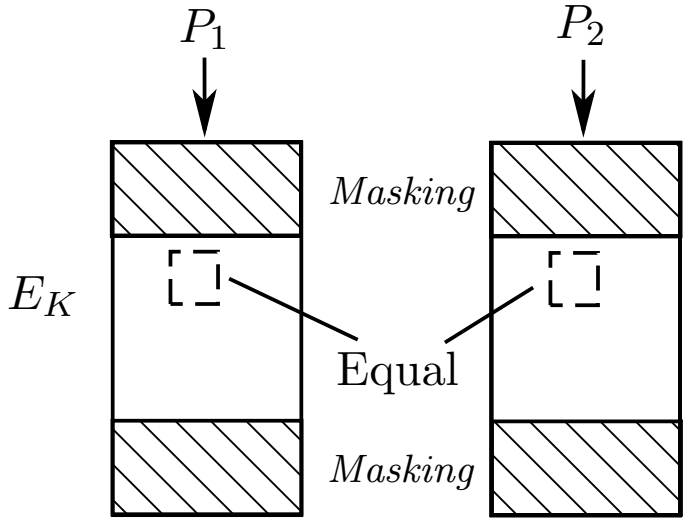
Countermeasures

A typical countermeasure is masking. The idea is to make the dependency between intermediate variables and a plaintext weaker:



Countermeasures

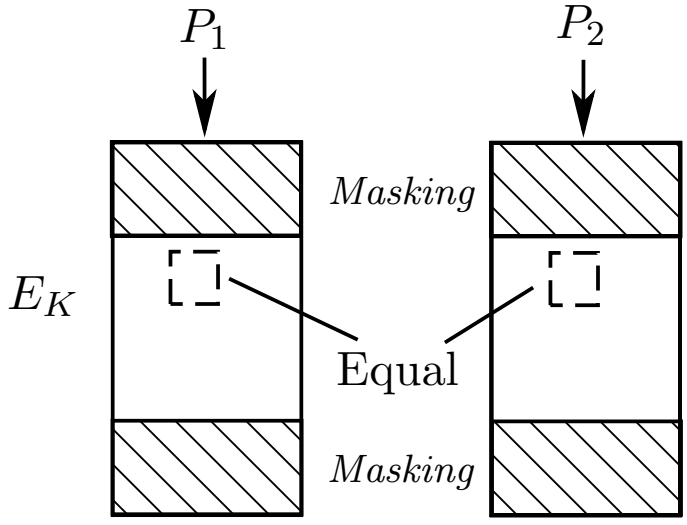
A typical countermeasure is masking. The idea is to make the dependency between intermediate variables and a plaintext weaker:



Some properties may be exploited to pass through masked rounds. Handschuh and Preneel used a differential to obtain information on the subkey of an unmasked round of DES [HP06].

Countermeasures

A typical countermeasure is masking. The idea is to make the dependency between intermediate variables and a plaintext weaker:



Some properties may be exploited to pass through masked rounds. Handschuh and Preneel used a differential to obtain information on the subkey of an unmasked round of DES [HP06].

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

What we do

Attack AES with 2, 3, and 4 masked rounds.

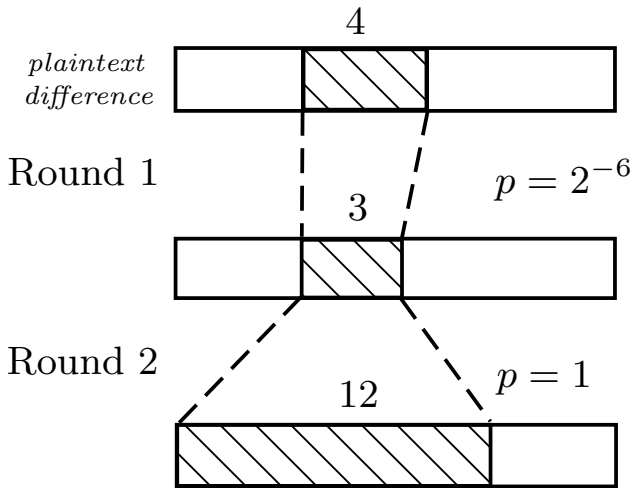
What we do

Attack AES with 2, 3, and 4 masked rounds.

Use the AES differential/square properties to reveal the secret key using the collision technique.

Simple collision attack on AES (2 masked rounds)

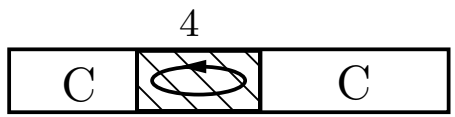
We use 2-round 2^{-6} differential:



and search for 4 collisions before the 3rd round.

Simple collision attack on AES (2 masked rounds)

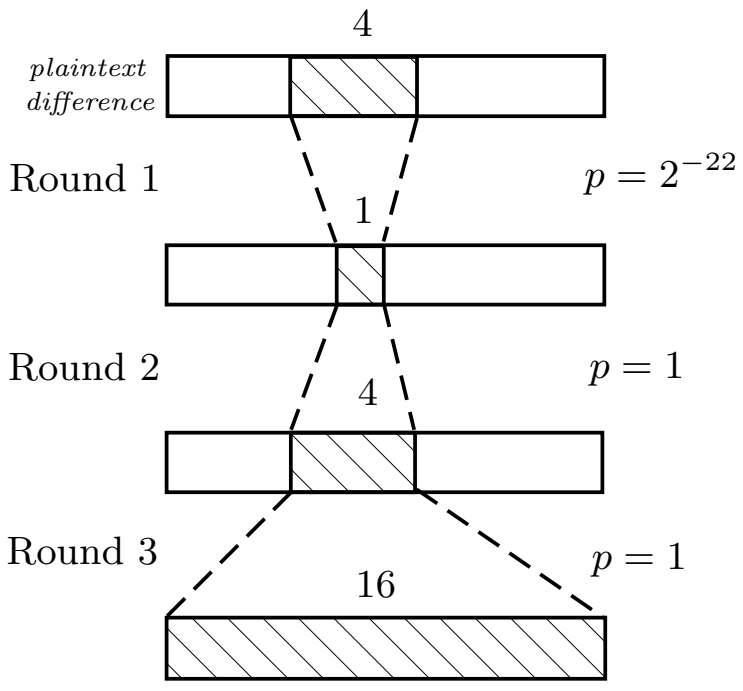
We use structures to reduce the number of measurements:



24 texts $\Rightarrow \sim 2^8$ pairs $\Rightarrow$ 4 right pairs $\Rightarrow$ 32 bits of key.
Overall: 72 measurements $+ \sim 2^{32}$ offline operations (key testing).

Impossible collision attack (3 masked rounds)

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

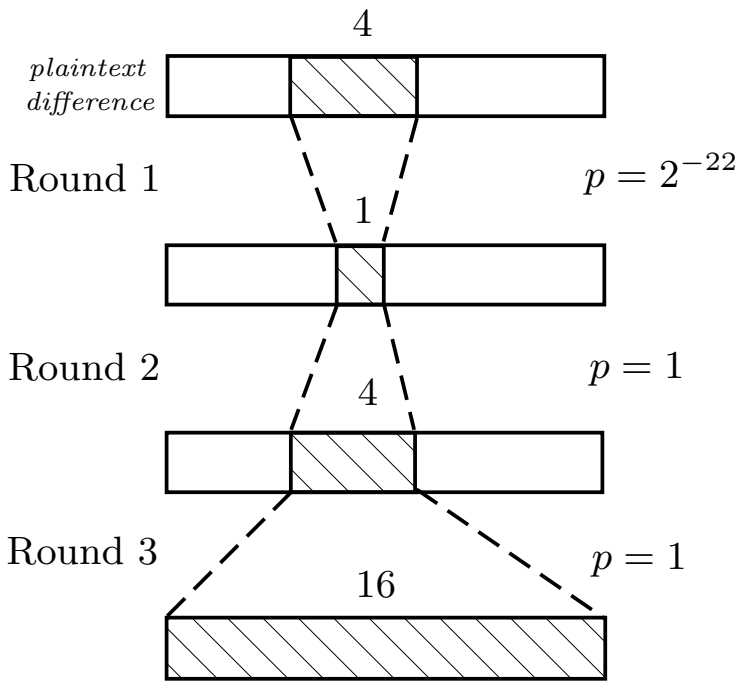


Our idea is to detect the **absence** of collisions.

A right pair reveals information about the first subkey.

Impossible collision attack (3 masked rounds)

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

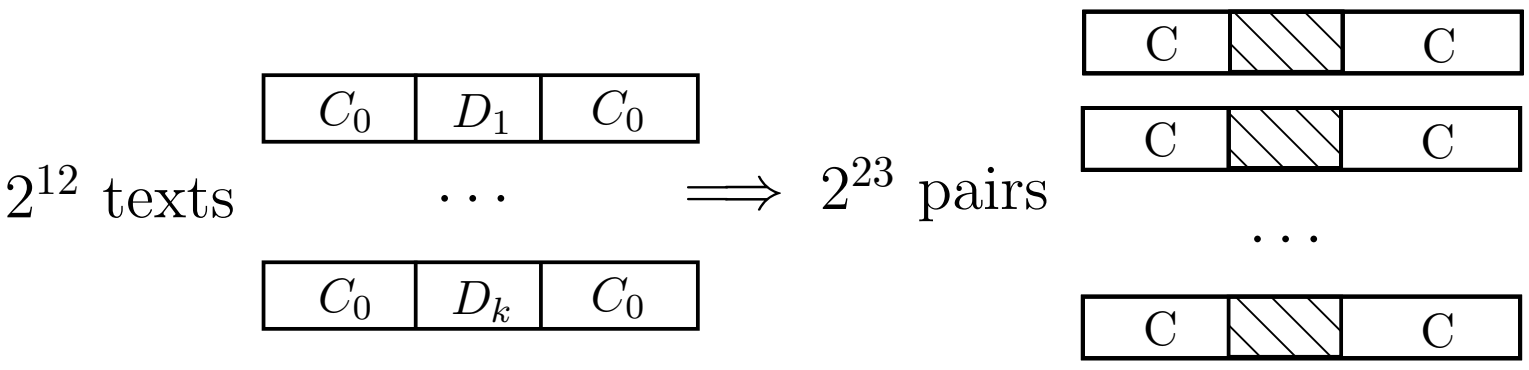


Our idea is to detect the **absence** of collisions.
A right pair reveals information about the first subkey.

The probability of a right pair is 2^{-22}. We test 2^{23} pairs to get 2 right ones.

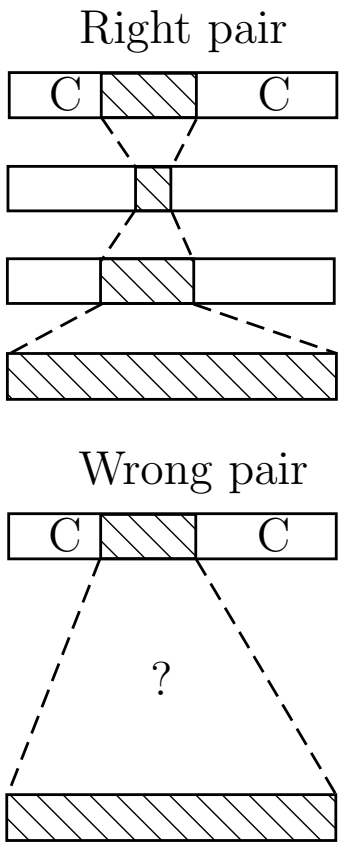
Impossible collision attack (3 masked rounds)

We test 2^{23} pairs (with a fixed C).



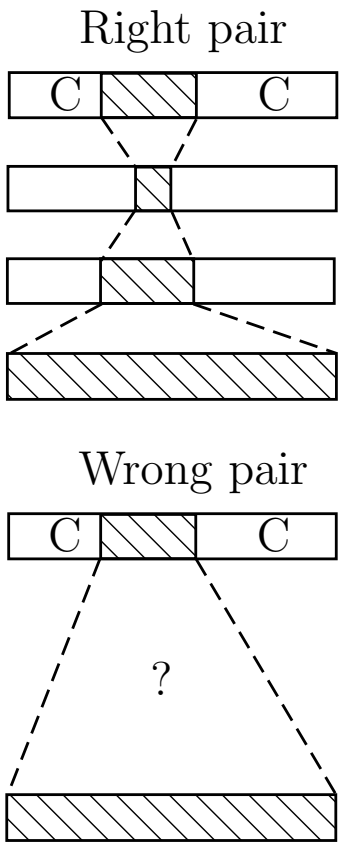
Impossible collision attack (3 masked rounds)

The probability of the wrong pair to survive is $\sim 15/16$. We need to filter them.



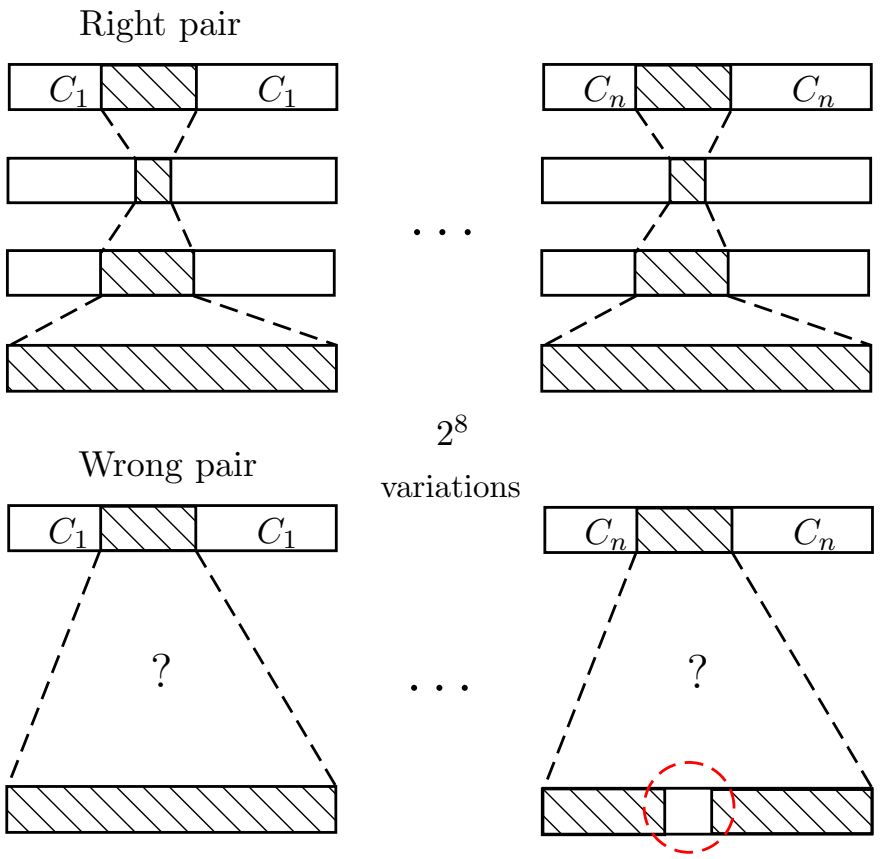
Impossible collision attack (3 masked rounds)

The probability of the wrong pair to survive is $\sim 15/16$. We need to filter them.

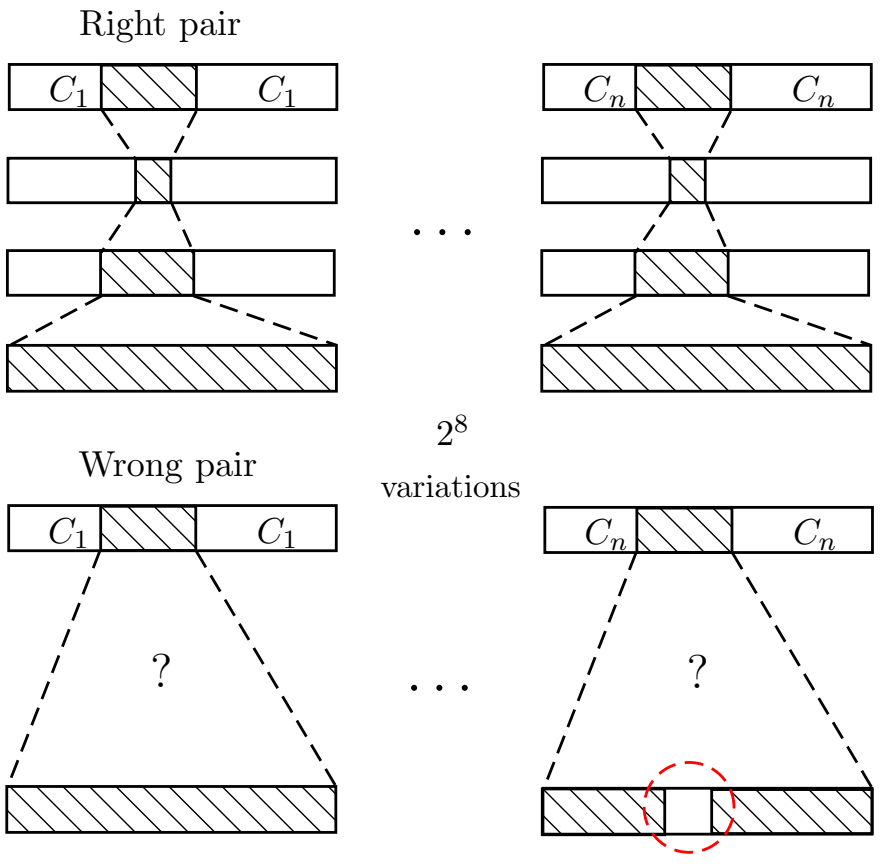


If we modify constants a right pair survives while a wrong one may not with $p = \frac{1}{16}$.

Impossible collision attack (3 masked rounds)



Impossible collision attack (3 masked rounds)



We need 2^{20} measurements and about 2^{27} time.

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

Errors in the impossible collision attack

The probability of the differential (p) was 2^{-22} so we test about $1/p = 2^{22}$ pairs.

Errors in the impossible collision attack

The probability of the differential (p) was 2^{-22} so we test about $1/p = 2^{22}$ pairs.
Let errors be: $\mathbb{P}$(right pair survives) $= \alpha$,
$\mathbb{P}$(wrong pair survives) $= \beta$.

Errors in the impossible collision attack

The probability of the differential (p) was 2^{-22} so we test about $1/p = 2^{22}$ pairs.
Let errors be: $\mathbb{P}$(right pair survives) $= \alpha$,
$\mathbb{P}$(wrong pair survives) $= \beta$.
Then the following condition on the number M of the tested pairs should hold:

$$M > \left(\frac{1}{p}\right)^{\log_{\beta/\alpha} \beta},$$

Errors in the impossible collision attack

The probability of the differential (p) was 2^{-22} so we test about $1/p = 2^{22}$ pairs.
Let errors be: $\mathbb{P}$(right pair survives) $= \alpha$,
$\mathbb{P}$(wrong pair survives) $= \beta$.
Then the following condition on the number M of the tested pairs should hold:

$$M > \left(\frac{1}{p}\right)^{\log_{\beta/\alpha} \beta},$$

which implies $\beta < \alpha$.

How to satisfy the last one?

Errors in the impossible collision attack

$$\beta < \alpha$$

Introduce new notation:
α_B — the probability of a difference in a single byte to be recognized;
β_B — that of a collision in a single byte to be missed.

Errors in the impossible collision attack

$$\beta < \alpha$$

Introduce new notation:
α_B — the probability of a difference in a single byte to be recognized;
β_B — that of a collision in a single byte to be missed.
Then

$$\beta = \left(\frac{255}{256}\beta_B + \frac{\alpha_B}{256}\right)^{16}; \quad \alpha = \alpha_B^{16}.$$

Errors in the impossible collision attack

$$\beta < \alpha$$

Introduce new notation:
α_B — the probability of a difference in a single byte to be recognized;
β_B — that of a collision in a single byte to be missed.
Then

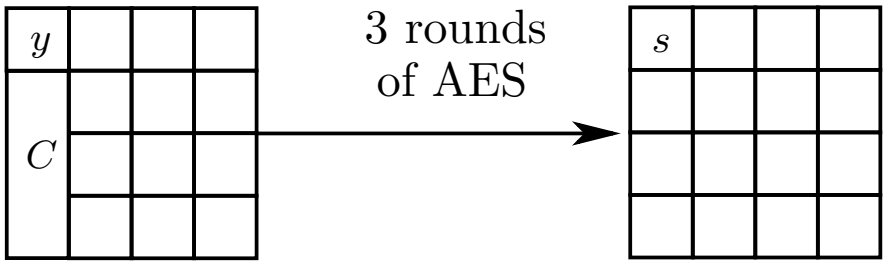
$$\beta = \left(\frac{255}{256}\beta_B + \frac{\alpha_B}{256}\right)^{16}; \quad \alpha = \alpha_B^{16}.$$

So the condition is

$$\beta_B < \alpha_B.$$

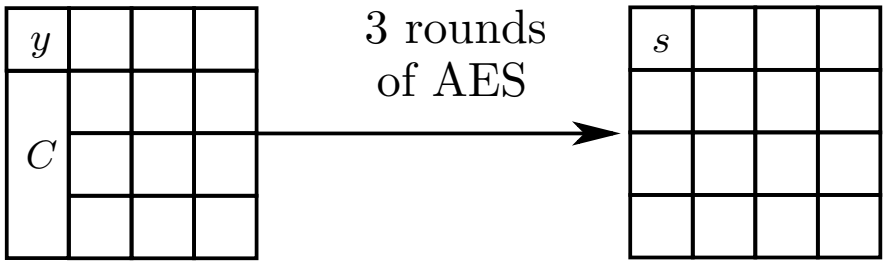
Multiset collisions. Distinguisher

3-round Gilbert-Minier distinguisher:



Multiset collisions. Distinguisher

3-round Gilbert-Minier distinguisher:

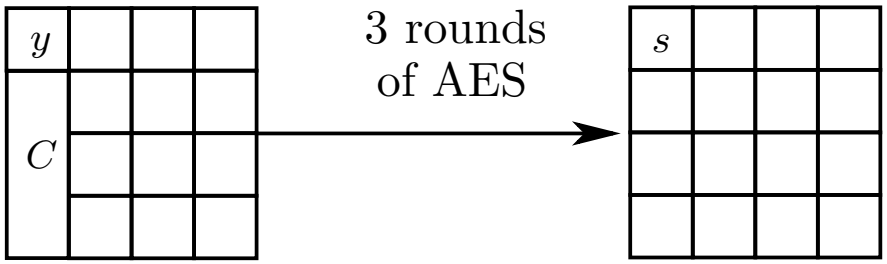


Among 2^{16} distinct C's always exist C', C'':

$$s^{C'}[y] \equiv s^{C''}[y] \text{ (256 collisions).}$$

Multiset collisions. Distinguisher

3-round Gilbert-Minier distinguisher:



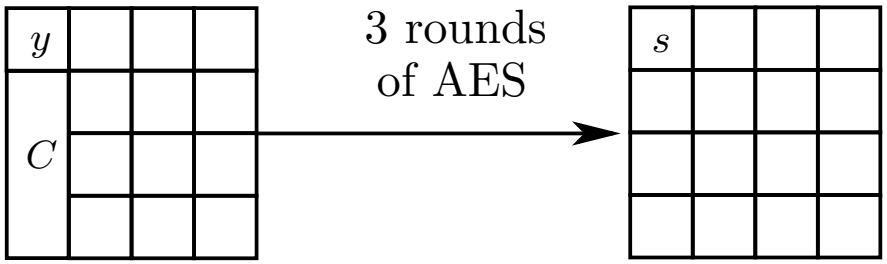
Among 2^{16} distinct C's always exist C', C'':

$$s^{C'}[y] \equiv s^{C''}[y] \text{ (256 collisions).}$$

Actually 6 trials are enough.

Multiset collisions. Distinguisher

3-round Gilbert-Minier distinguisher:



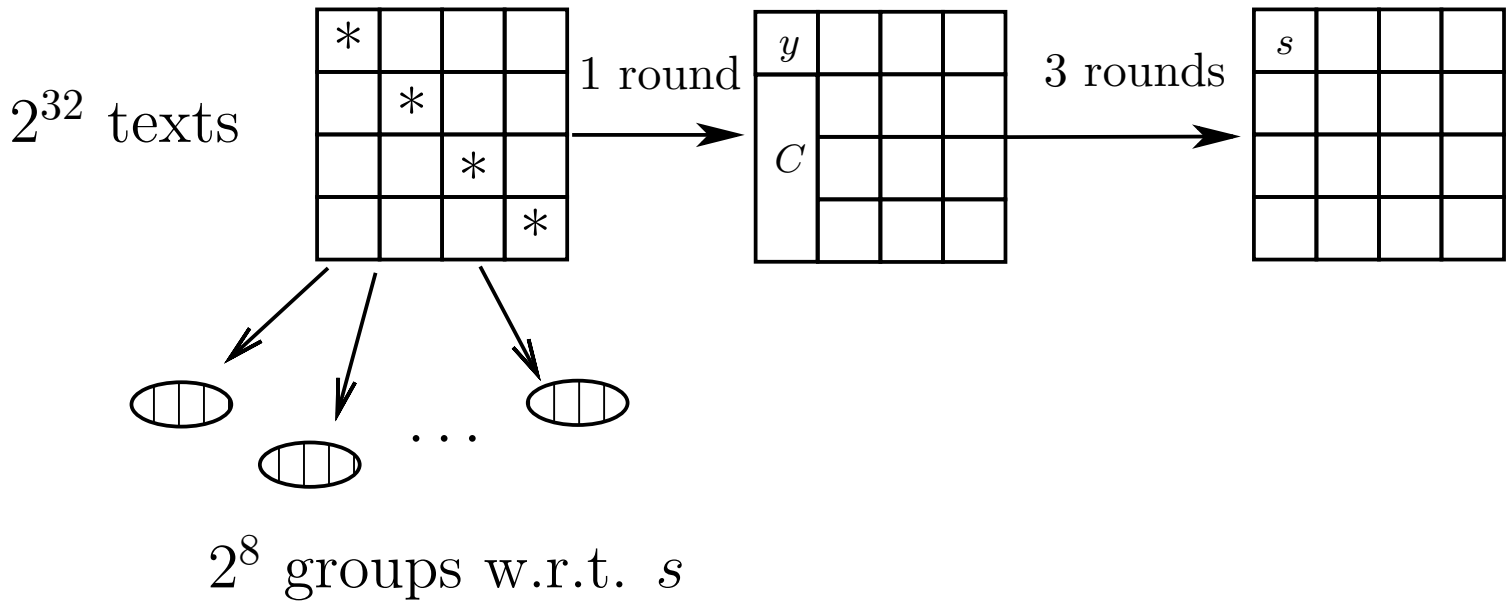
Among 2^{16} distinct C's always exist C', C'':

$$s^{C'}[y] \equiv s^{C''}[y] \text{ (256 collisions).}$$

Actually 6 trials are enough.
Overall $6 \cdot 2^{16} \approx 2^{18.5}$ plaintexts are needed to find such a C-pair.

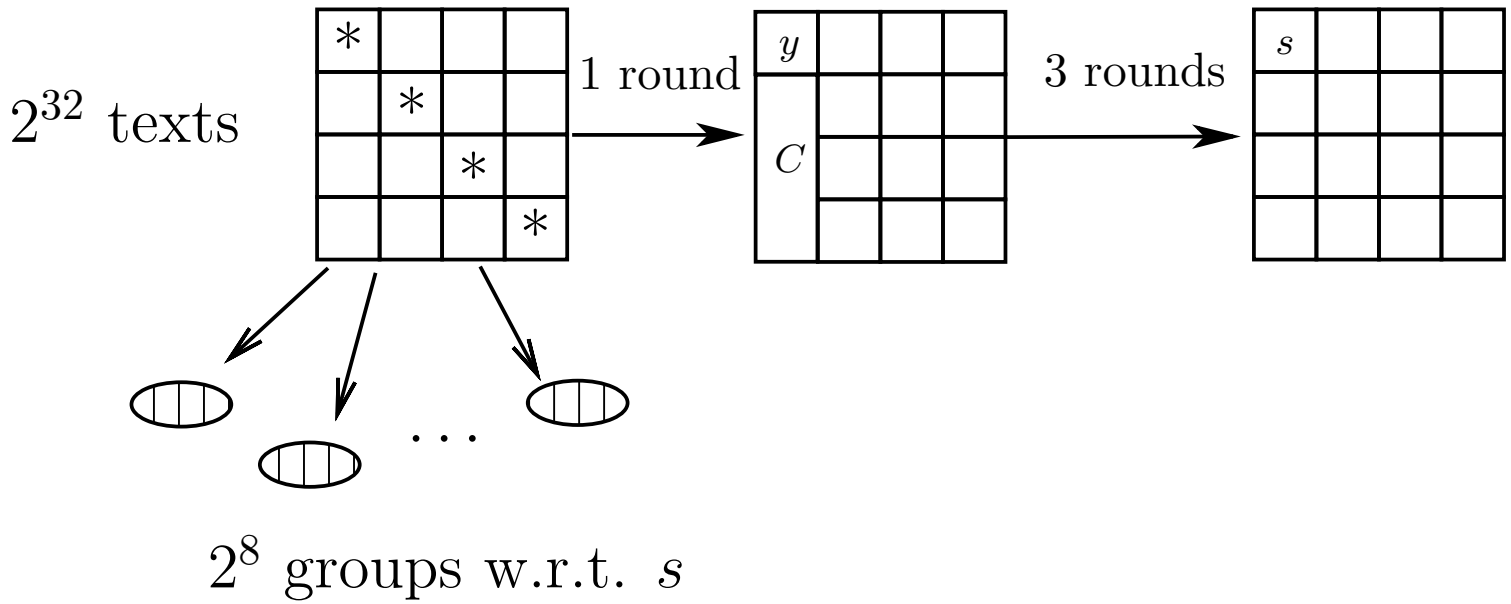
Multiset collision attack I (4 masked rounds)

Add a round in the beginning:



Multiset collision attack I (4 masked rounds)

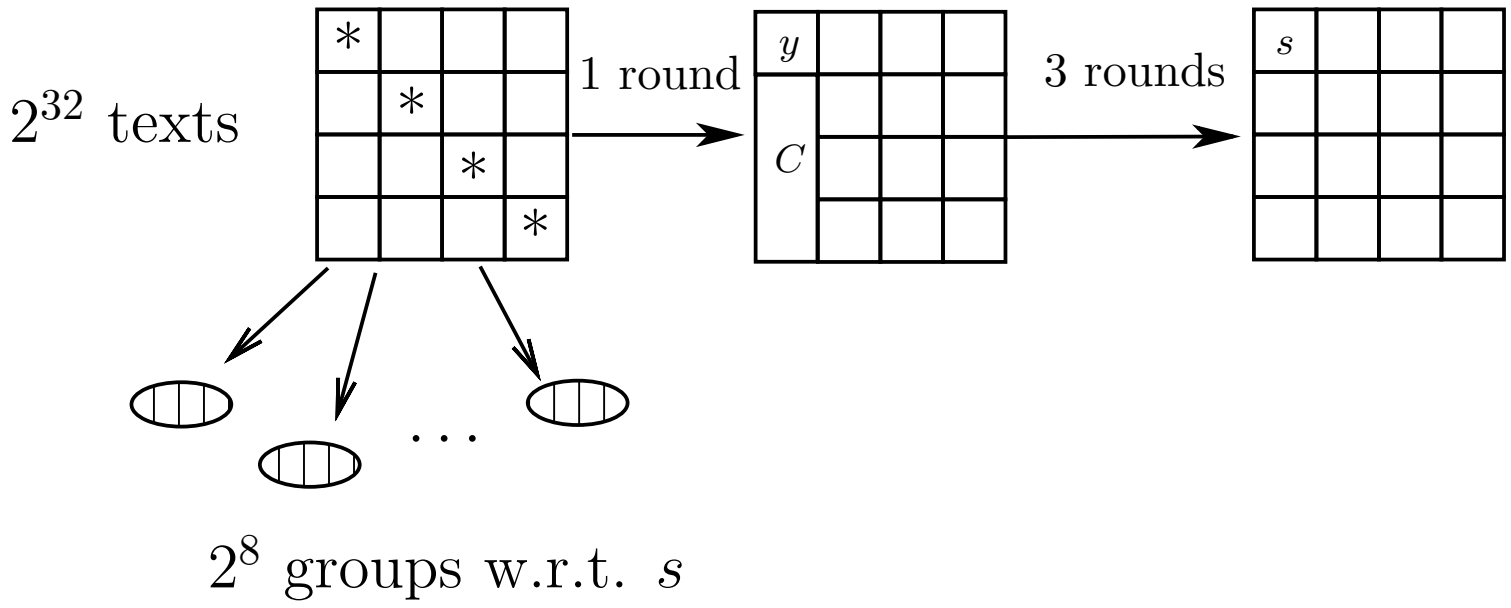
Add a round in the beginning:



For each key guess we construct 6-values vectors for the distinguisher.

Multiset collision attack I (4 masked rounds)

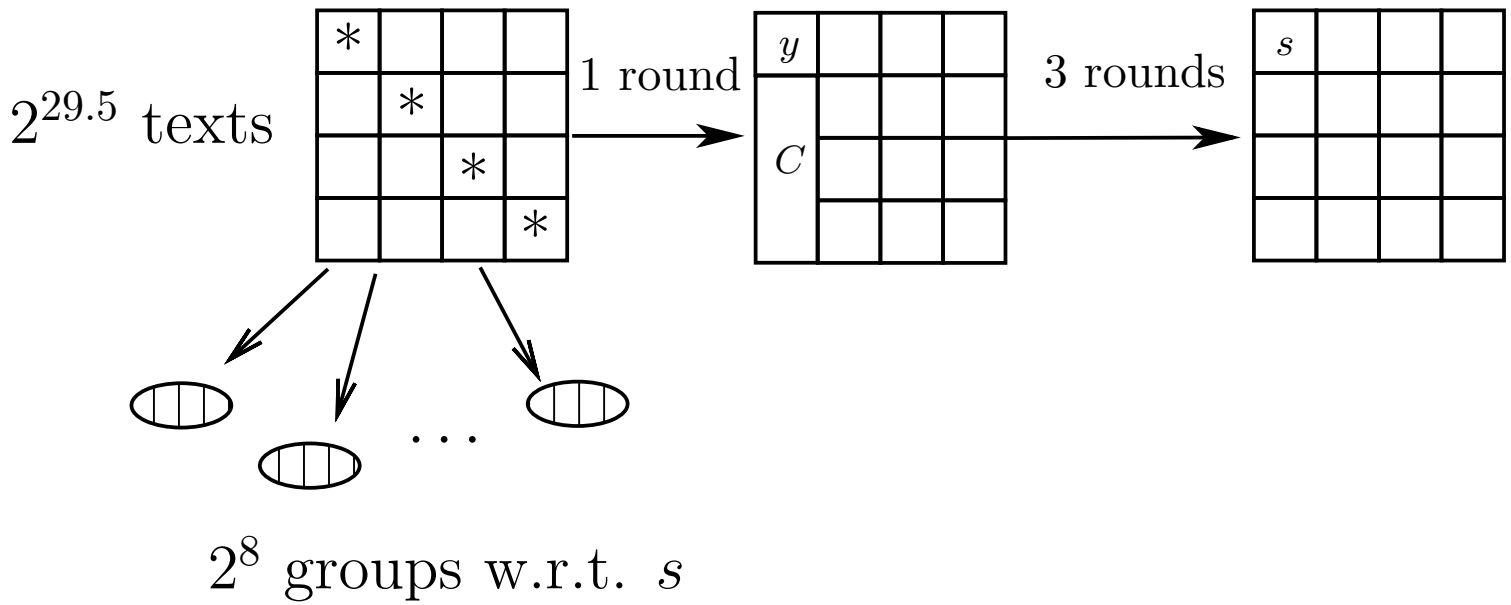
Add a round in the beginning:



For each key guess we construct 6-values vectors for the distinguisher.
The offline complexity is 2^{45} AES rounds.

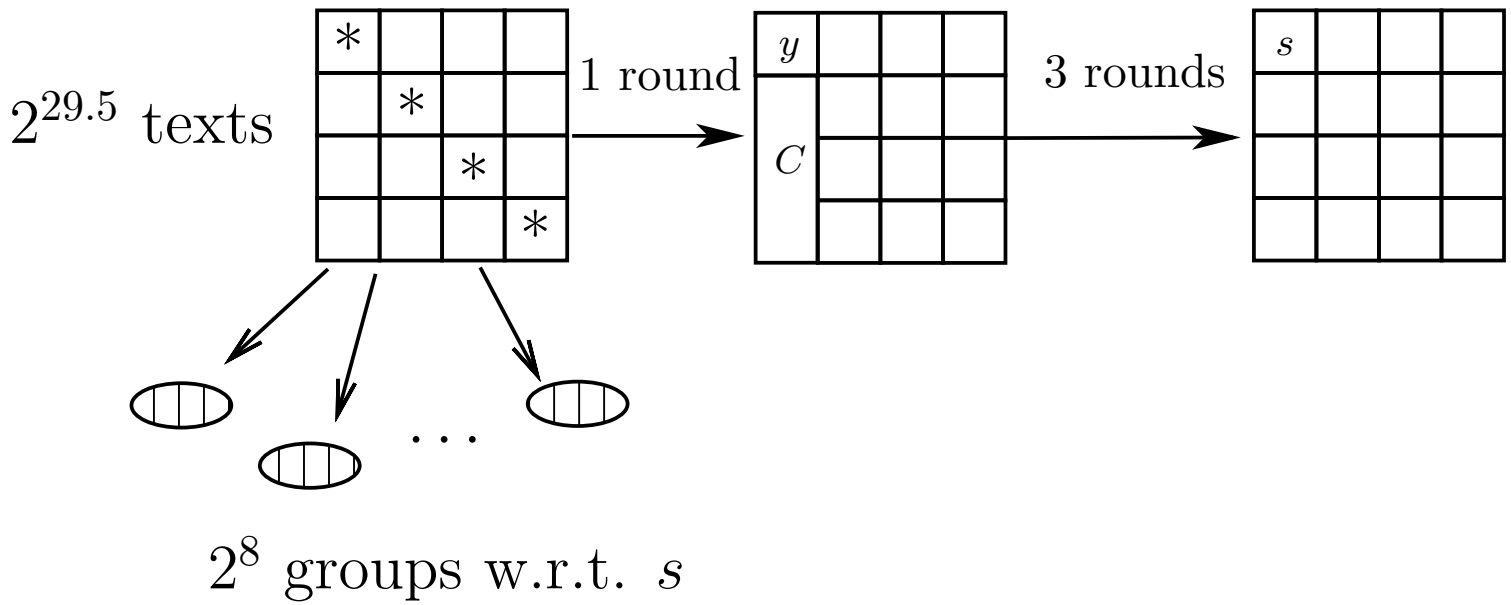
Multiset collision attack II (4 masked rounds)

Use fewer texts:



Multiset collision attack II (4 masked rounds)

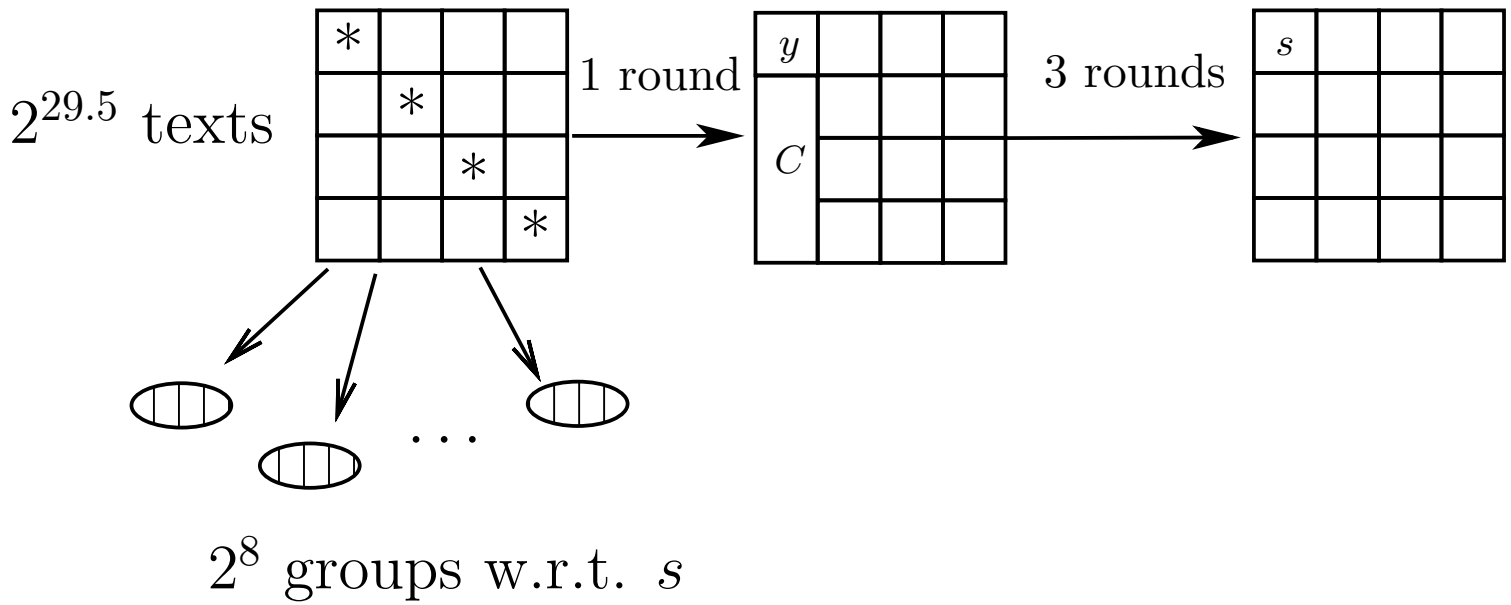
Use fewer texts:



However, it becomes more complicated to use the distinguisher (a specific matching problem arises).

Multiset collision attack II (4 masked rounds)

Use fewer texts:



However, it becomes more complicated to use the distinguisher (a specific matching problem arises).
The offline complexity is 2^{54} AES rounds.

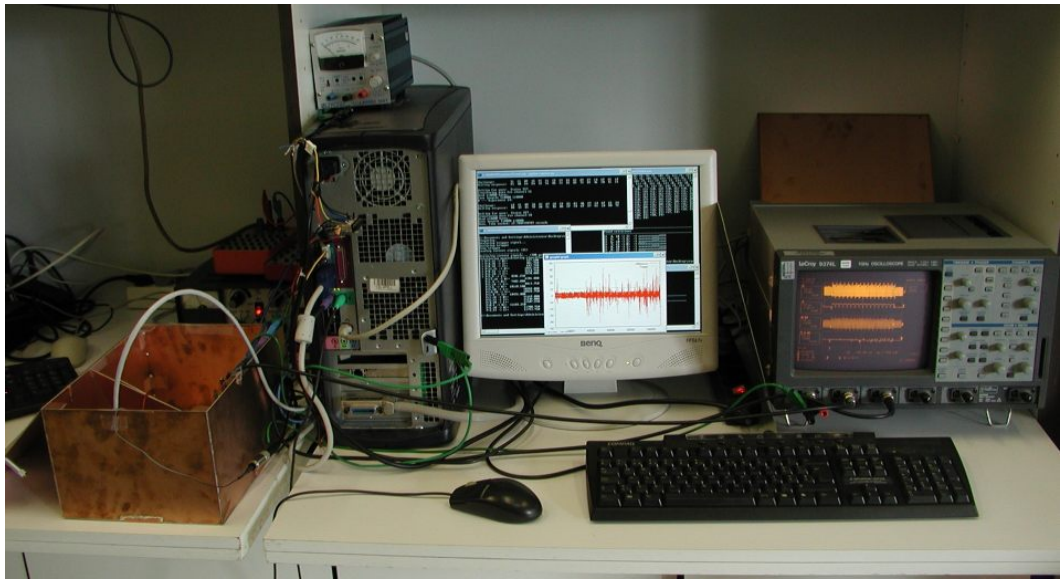
Summary of the results

Method	**Complexity**		**Masked rounds**	**Attack**
	Measur-ts	Off-line		
Simple	2^6–2^7	2^{32}	2	Full key recovery
Impossible	2^{21}	2^{29}	3	Full key recovery
MultiSet	$2^{18.5}$	2^{20}	3	Distinguisher
MultiSet	2^{32}	$2^{44.5}$	4	32 key bits recovery
MultiSet	2^{29}–2^{30}	2^{54}	4	32 key bits recovery

Setup

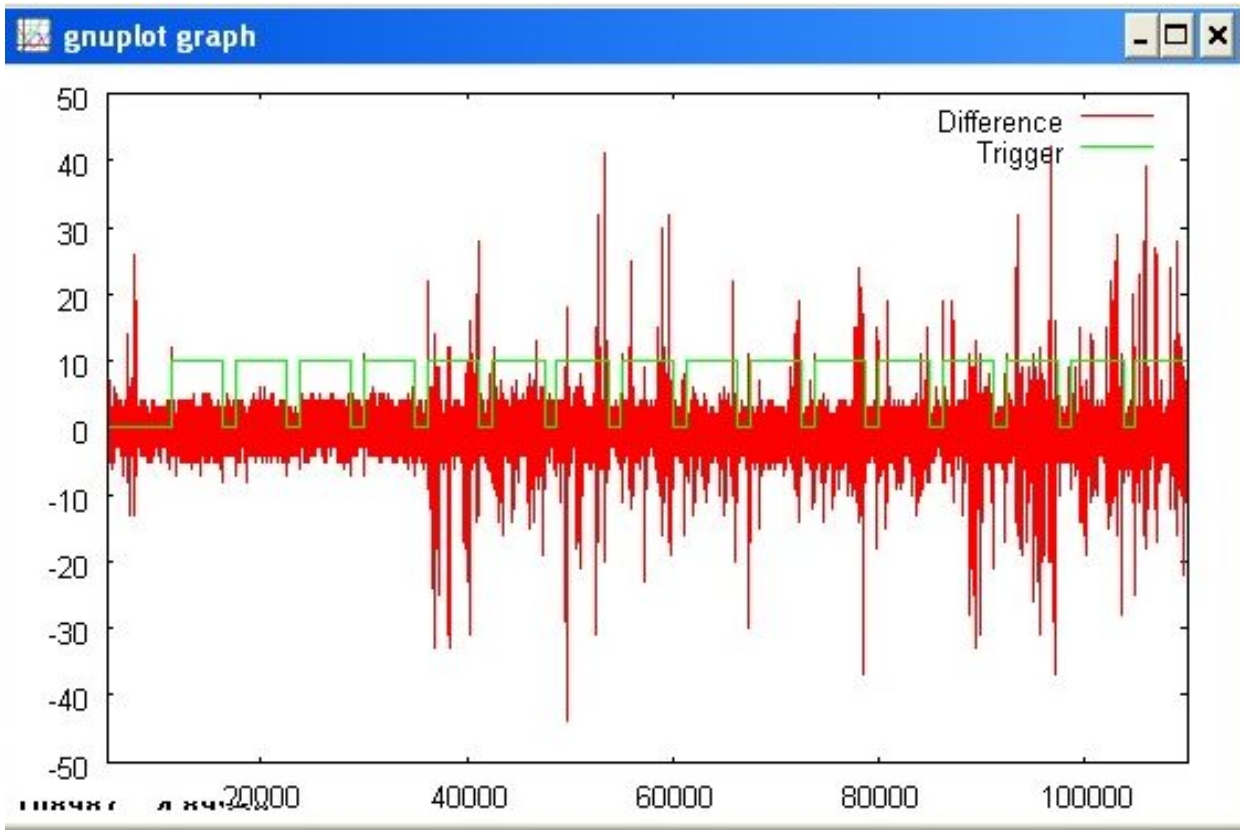
Implemented by André Stemper:

- AES-128 RISC microcontroller;
- Microchip PIC16F87 clocked at 4Mhz;
- LeCroy 9374L 1GHz digital oscilloscope;
- Measurement time: 0.35s per measurement (oscilloscope is the bottleneck).



Attacks inside

Simple collision attack:



The features of implementation

- Protection against EM-radiation (Faraday cage);
- Automatic threshold search in the simple collision attack (4 collisions help);
- Manual search for a threshold to detect a collision in the impossible collision attack;
- Use analog filters for the communication noise removal.

Conclusions

Simple collision attacks for AES with 2 masked rounds.

Detecting the absence of collisions gives information about the key.

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

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