Collision-Correlation Attack against some 1st-order Boolean Masking Schemes in the Context of Secure Devices

Thomas Roche
joint work with Victor Lomné

ANSSI, France

COSADE'13, Paris, France
March 8, 2013

Overview

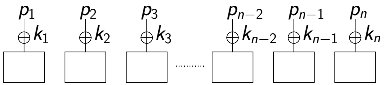
Linear Collision Attacks

Mechanisms of Collision Detection

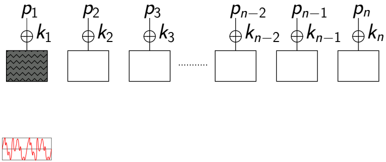
2O-CPA on Mask-Reuse Scheme Implementation

Experiments and Results

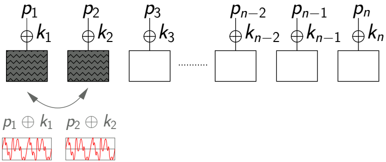
Linear Collision Attack [Bog07, GS12]



Linear Collision Attack [Bog07, GS12]

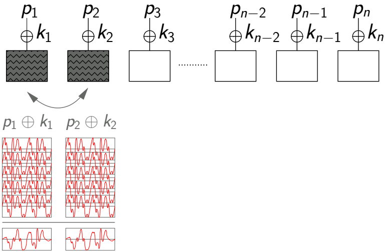


Linear Collision Attack [Bog07, GS12]



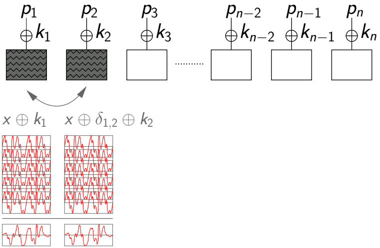
$$k_1 \oplus k_2 = p_1 \oplus p_2$$

Linear Collision Attack [Bog07, GS12]



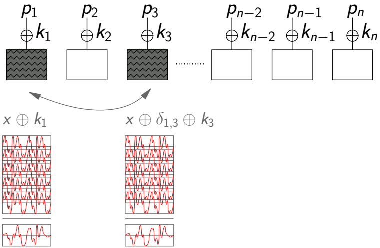
$$k_1 \oplus k_2 = p_1 \oplus p_2$$

Linear Collision Attack [Bog07, GS12]



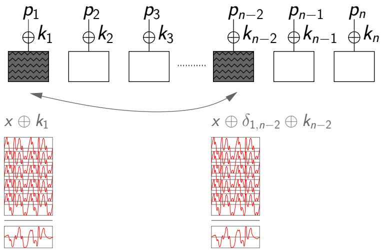
$$k_1 \oplus k_2 = \delta_{1,2}$$

Linear Collision Attack [Bog07, GS12]



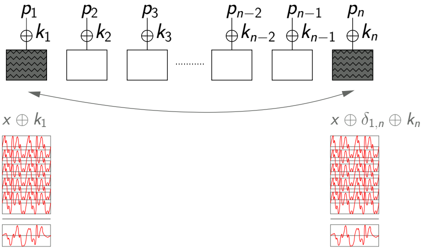
$$k_1 \oplus k_2 = \delta_{1,2}$$
$$k_1 \oplus k_3 = \delta_{1,3}$$

Linear Collision Attack [Bog07, GS12]



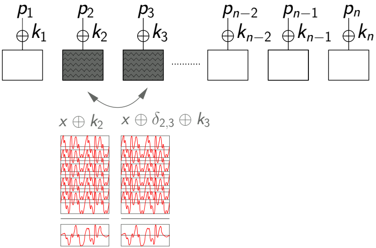
$$k_1 \oplus k_2 = \delta_{1,2}$$
$$k_1 \oplus k_3 = \delta_{1,3}$$
$$\vdots$$
$$k_1 \oplus k_{n-2} = \delta_{1,n-2}$$

Linear Collision Attack [Bog07, GS12]



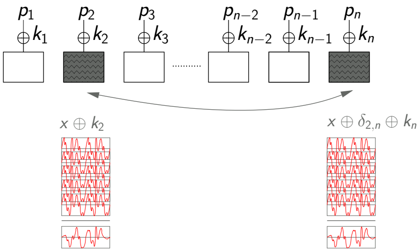
$$
\begin{aligned}
k_1 \oplus k_2 &= \delta_{1,2} \\
k_1 \oplus k_3 &= \delta_{1,3} \\
&\vdots \\
k_1 \oplus k_{n-2} &= \delta_{1,n-2} \\
k_1 \oplus k_{n-1} &= \delta_{1,n-1} \\
k_1 \oplus k_n &= \delta_{1,n}
\end{aligned}
$$

Linear Collision Attack [Bog07, GS12]



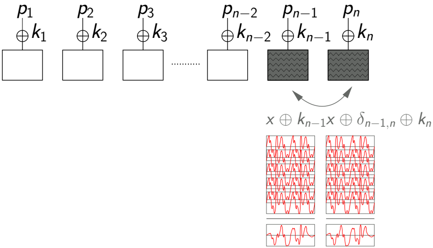
$$k_1 \oplus k_2 = \delta_{1,2}$$
$$k_1 \oplus k_3 = \delta_{1,3}$$
$$\vdots$$
$$k_1 \oplus k_{n-2} = \delta_{1,n-2}$$
$$k_1 \oplus k_{n-1} = \delta_{1,n-1}$$
$$k_1 \oplus k_n = \delta_{1,n}$$
$$k_2 \oplus k_3 = \delta_{2,3}$$

Linear Collision Attack [Bog07, GS12]



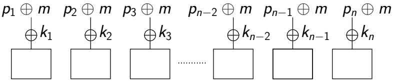
$$
\begin{aligned}
k_1 \oplus k_2 &= \delta_{1,2} \\
k_1 \oplus k_3 &= \delta_{1,3} \\
&\vdots \\
k_1 \oplus k_{n-2} &= \delta_{1,n-2} \\
k_1 \oplus k_{n-1} &= \delta_{1,n-1} \\
k_1 \oplus k_n &= \delta_{1,n} \\
k_2 \oplus k_3 &= \delta_{2,3} \\
&\vdots \\
k_2 \oplus k_n &= \delta_{2,n}
\end{aligned}
$$

Linear Collision Attack [Bog07, GS12]

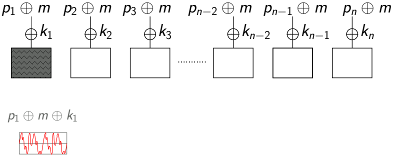


$$
\begin{cases}
k_1 \oplus k_2 = \delta_{1,2} \\
k_1 \oplus k_3 = \delta_{1,3} \\
\vdots \\
k_1 \oplus k_{n-2} = \delta_{1,n-2} \\
k_1 \oplus k_{n-1} = \delta_{1,n-1} \\
k_1 \oplus k_n = \delta_{1,n} \\
k_2 \oplus k_3 = \delta_{2,3} \\
\vdots \\
k_2 \oplus k_n = \delta_{2,n} \\
\vdots \\
k_{n-1} \oplus k_n = \delta_{n-1,n}
\end{cases}
$$

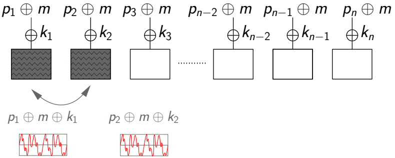
Linear Collision Attack on Masked Implementations [MME10, CFGRV11]



Linear Collision Attack on Masked Implementations [MME10, CFGRV11]

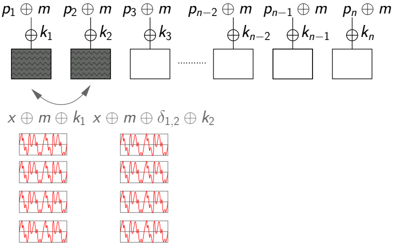


Linear Collision Attack on Masked Implementations [MME10, CFGRV11]



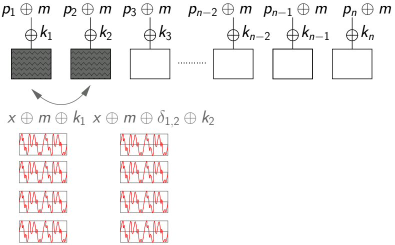
$$k_1 \oplus k_2 = p_1 \oplus p_2$$

Linear Collision Attack on Masked Implementations [MME10, CFGRV11]



$$k_1 \oplus k_2 = \delta_{1,2}$$

Linear Collision Attack on Masked Implementations [MME10, CFGRV11]



$$\begin{cases} k_1 \oplus k_2 = \delta_{1,2} \\ k_1 \oplus k_3 = \delta_{1,3} \\ \vdots \\ k_1 \oplus k_{n-2} = \delta_{1,n-2} \\ k_1 \oplus k_{n-1} = \delta_{1,n-1} \\ k_1 \oplus k_n = \delta_{1,n} \\ k_2 \oplus k_3 = \delta_{2,3} \\ \vdots \\ k_2 \oplus k_n = \delta_{2,n} \\ \vdots \\ k_{n-1} \oplus k_n = \delta_{n-1,n} \end{cases}$$

Complexity Comparison After N Encryptions

- Unprotected Case

$$\Pr[\exists(i,j) \text{ s.t. } x_a^i \oplus x_b^j = k_a \oplus k_b] = \left(1 - (1 - \frac{1}{2^m})^{N^2}\right)$$

[AES] full rank system $\sim$ 7 messages [Bog07]

- Mask-Reuse Case

$$\Pr[\exists i \text{ s.t. } x_a^i \oplus x_b^i = k_a \oplus k_b] = \left(1 - (1 - \frac{1}{2^m})^{N}\right)$$

[AES] full rank system $\sim$ 59 messages [CFGRV11]

Same complexity of collision detection, depends on σ (noise std.)

dth-Order CPA: exponential complexity $O(\bar{\sigma}^d)$

Complexity Comparison After N Encryptions

- Unprotected Case

$$\Pr[\exists(i,j) \text{ s.t. } x_a^i \oplus x_b^j = k_a \oplus k_b] = \left(1 - (1 - \frac{1}{2^m})^{N^2}\right)$$

[AES] full rank system $\sim$ 7 messages [Bog07]

- Mask-Reuse Case

$$\Pr[\exists i \text{ s.t. } x_a^i \oplus x_b^i = k_a \oplus k_b] = \left(1 - (1 - \frac{1}{2^m})^{N}\right)$$

[AES] full rank system $\sim$ 59 messages [CFGRV11]

Same complexity of collision detection, depends on σ (noise std.)

dth-Order CPA: exponential complexity $O(\bar{\sigma}^d)$

Threshold Approach [Bog07, Bog08, CFGRV11] 1/2

Decide the presence (*resp.* absence) of collision from a set of traces pairs $((\ell_a^{i_k})_k, (\ell_b^{j_k})_k)$ such that $p_a^{i_k} \oplus p_b^{j_k} = \delta$.

- $\dfrac{1}{\bar{N}_\delta} \sum_x \mathrm{ED}(\bar{\ell}_{x,a}, \bar{\ell}_{x \oplus \delta, b}) < T$
- $\rho((\ell_a^{i_k})_k, (\ell_b^{i_k})_k) > T$

$\hookrightarrow$ Collision-based attack more efficient than CPA/2O-CPA

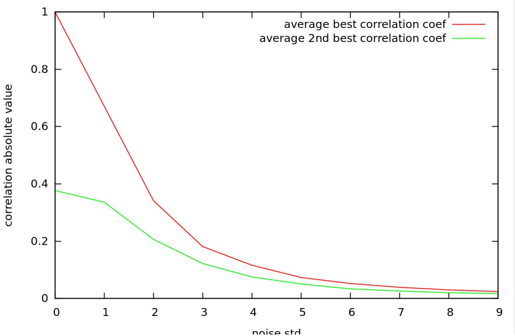
Threshold Approach [Bog07, Bog08, CFGRV11] 1/2

Decide the presence (*resp.* absence) of collision from a set of traces pairs $((\ell_a^{i_k})_k, (\ell_b^{j_k})_k)$ such that $p_a^{i_k} \oplus p_b^{j_k} = \delta$.

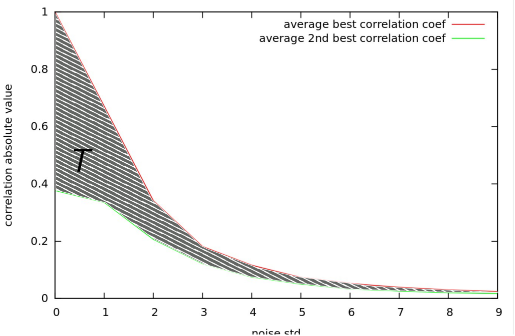
- $\dfrac{1}{\bar{N}_\delta} \sum_x \mathrm{ED}(\bar{\ell}_{x,a}, \bar{\ell}_{x\oplus\delta,b}) < T$
- $\rho((\ell_a^{i_k})_k, (\ell_b^{i_k})_k) > T$

$\hookrightarrow$ Collision-based attack more efficient than CPA/2O-CPA

Threshold Approach [Bog07, Bog08, CFGRV11] 2/2

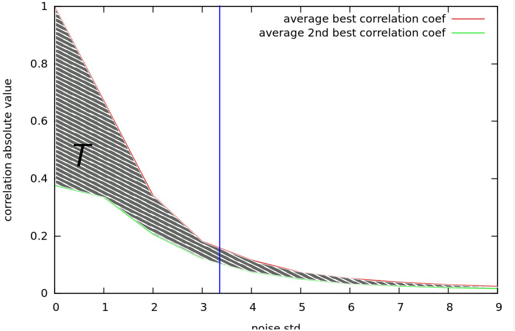


Threshold Approach [Bog07, Bog08, CFGRV11] 2/2



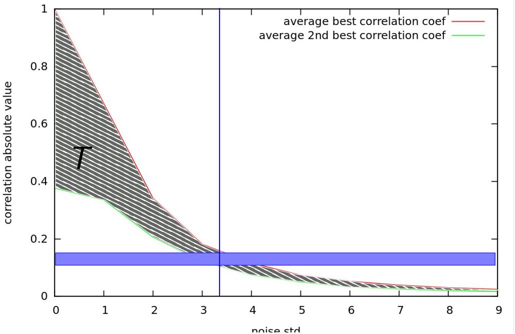
Threshold Approach [Bog07, Bog08, CFGRV11] 2/2

$S(p_2 \oplus k_2)$

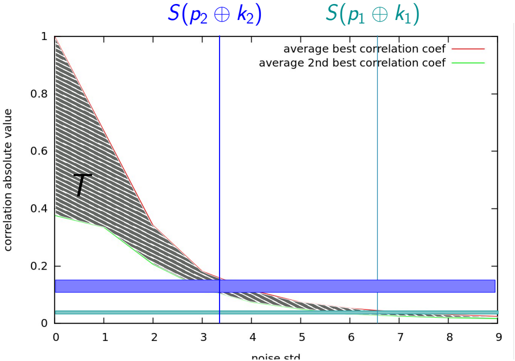


Threshold Approach [Bog07, Bog08, CFGRV11] 2/2

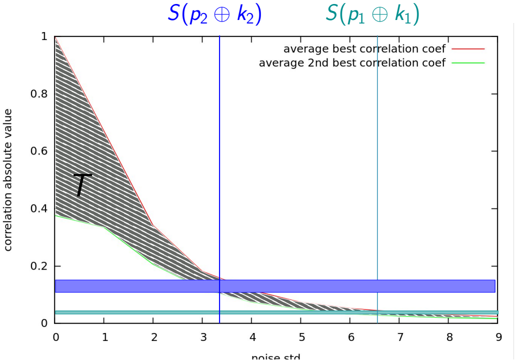
$S(p_2 \oplus k_2)$



Threshold Approach [Bog07, Bog08, CFGRV11] 2/2



Threshold Approach [Bog07, Bog08, CFGRV11] 2/2



Limits of the approach

- T unknown and hard to guess when σ "high"
- different Ts for each pair of IVs

Unified Approach [GS12] 1/3

Decide the presence of collision from all the traces pairs $((\ell_a^{i_k})_k, (\ell_b^{j_k})_k)_\delta$ such that $p_a^{i_k} \oplus p_b^{j_k} = \delta$.

- $\min_\delta \frac{1}{\bar{N}_\delta} \sum_x \mathrm{ED}(\bar{\ell}_{x,a}, \bar{\ell}_{x \oplus \delta, b})$
- $\max_\delta \rho((\bar{\ell}_{x,a})_x, (\bar{\ell}_{x \oplus \delta, b})_x)$

$\hookrightarrow$ increase in message complexity

distinguishing values must be compared with something.

Unified Approach [GS12] 2/3

$$
\begin{aligned}
k_1 \oplus k_2 &= \delta_{1,2} \\
&\vdots \\
k_1 \oplus k_n &= \delta_{1,n} \\
k_2 \oplus k_3 &= \delta_{2,3} \\
&\vdots \\
k_{n-1} \oplus k_n &= \delta_{n-1,n}
\end{aligned}
$$

Unified Approach [GS12] 2/3

$$
\begin{array}{rcl}
k_1 \oplus k_2 & = & \delta_{1,2}, p_{1,2} \\
 & \vdots & \\
k_1 \oplus k_n & = & \delta_{1,n}, p_{1,n} \\
k_2 \oplus k_3 & = & \delta_{2,3}, p_{2,3} \\
 & \vdots & \\
k_{n-1} \oplus k_n & = & \delta_{n-1,n}, p_{n-1,n}
\end{array}
$$

Unified Approach [GS12] 2/3

$$
\begin{array}{lcll}
k_1 \oplus k_2 & = & 0, p_{1,2}(0); & \cdots ; \quad 2^m - 1, p_{1,2}(2^m - 1) \\
 & \vdots & & \\
k_1 \oplus k_n & = & 0, p_{1,n}(0); & \cdots ; \quad 2^m - 1, p_{1,n}(2^m - 1) \\
k_2 \oplus k_3 & = & 0, p_{2,3}(0); & \cdots ; \quad 2^m - 1, p_{2,3}(2^m - 1) \\
 & \vdots & & \\
k_{n-1} \oplus k_n & = & 0, p_{n-1,n}(0); & \cdots ; \quad 2^m - 1, p_{n-1,n}(2^m - 1)
\end{array}
$$

Unified Approach [GS12] 2/3

$$
\begin{array}{lcllll}
k_1 \oplus k_2 & = & 0, p_{1,2}(0); & \cdots; & 2^m - 1, p_{1,2}(2^m - 1) \\
 & \vdots & & & \\
k_1 \oplus k_n & = & 0, p_{1,n}(0); & \cdots; & 2^m - 1, p_{1,n}(2^m - 1) \\
k_2 \oplus k_3 & = & 0, p_{2,3}(0); & \cdots; & 2^m - 1, p_{2,3}(2^m - 1) \\
 & \vdots & & & \\
k_{n-1} \oplus k_n & = & 0, p_{n-1,n}(0); & \cdots; & 2^m - 1, p_{n-1,n}(2^m - 1)
\end{array}
$$

While $\underset{\delta_{1,2},\cdots,\delta_{n-1,n}}{\operatorname{argmax}} (p_{i,j}(\delta_{i,j}))$ is not a codeword

For $1 \leq a < b \leq n, \delta \in \mathrm{GF}(2^m)$

Do $p_{a,b}(\delta) \leftarrow p_{a,b}(\delta) \cdot \prod_{c \notin \{a,b\}} \sum_{\beta \in \mathrm{GF}(256)} p_{a,c}(\beta) \times p_{b,c}(\beta \oplus \delta)$

Unified Approach [GS12] 2/3

$$\begin{array}{lcllll}
k_1 \oplus k_2 & = & 0, p_{1,2}(0); & \cdots; & 2^m - 1, p_{1,2}(2^m - 1) \\
 & \vdots & & & \\
k_1 \oplus k_n & = & 0, p_{1,n}(0); & \cdots; & 2^m - 1, p_{1,n}(2^m - 1) \\
k_2 \oplus k_3 & = & 0, p_{2,3}(0); & \cdots; & 2^m - 1, p_{2,3}(2^m - 1) \\
 & \vdots & & & \\
k_{n-1} \oplus k_n & = & 0, p_{n-1,n}(0); & \cdots; & 2^m - 1, p_{n-1,n}(2^m - 1)
\end{array}$$

$\texttt{While} \underset{\delta_{1,2},\cdots,\delta_{n-1,n}}{\operatorname{argmax}} (p_{i,j}(\delta_{i,j}))$ is not a codeword

  $\texttt{For } 1 \leq a < b \leq n, \delta \in \mathrm{GF}(2^m)$

    $\texttt{Do } p_{a,b}(\delta) \leftarrow p_{a,b}(\delta) \cdot \prod_{c \notin \{a,b\}} \sum_{\beta \in \mathrm{GF}(256)} p_{a,c}(\beta) \times p_{b,c}(\beta \oplus \delta)$

Unified Approach [GS12] 2/3

$$
\begin{array}{lcllcl}
k_1 \oplus k_2 & = & 0, p_{1,2}(0); & \cdots; & 2^m-1, p_{1,2}(2^m-1) \\
 & \vdots & & & \\
k_1 \oplus k_n & = & 0, p_{1,n}(0); & \cdots; & 2^m-1, p_{1,n}(2^m-1) \\
k_2 \oplus k_3 & = & 0, p_{2,3}(0); & \cdots; & 2^m-1, p_{2,3}(2^m-1) \\
 & \vdots & & & \\
k_{n-1} \oplus k_n & = & 0, p_{n-1,n}(0); & \cdots; & 2^m-1, p_{n-1,n}(2^m-1)
\end{array}
$$

$\texttt{While} \underset{\delta_{1,2},\cdots,\delta_{n-1,n}}{\operatorname{argmax}} (p_{i,j}(\delta_{i,j}))$ is far from a codeword

$\quad \texttt{For } 1 \leq a < b \leq n, \delta \in \mathrm{GF}(2^m)$

$$\texttt{Do } p_{a,b}(\delta) \leftarrow p_{a,b}(\delta) \cdot \prod_{c \notin \{a,b\}} \sum_{\beta \in \mathrm{GF}(256)} p_{a,c}(\beta) \times p_{b,c}(\beta \oplus \delta)$$

Unified Approach [GS12] 3/3

$\hookrightarrow$ CPA (stochastic) more efficient than Collision-based attack
when the leakage function is not too far from the model basis

$\hookrightarrow$ extension to second order?
mask-reuse implementations

2nd-Order Correlation Power Analysis on Mask-Reuse Implementation

Classical Approach

$$\rho_{\hat{k}}\left((f_{\mathrm{opt}(\hat{z}_a^i)})_i, \mathcal{C}(\ell_m^i, \ell_{z_a^i \oplus m}^i)_i\right)$$

2nd-Order Correlation Power Analysis on Mask-Reuse Implementation

Classical Approach

$$\rho_{\hat{k}}\left((f_{\mathrm{opt}(\hat{z}_a^i)})_i, \mathcal{C}(\ell_m^i, \ell_{z_a^i \oplus m}^i)_i\right)$$

Adapted Approach

$$\rho_{\hat{k}_a, \hat{k}_b}\left((f_{\mathrm{opt}(\hat{z}_a^i, \hat{z}_b^i)})_i, \mathcal{C}(\ell_{z_a^i \oplus m}^i, \ell_{z_b^i \oplus m}^i)_i\right)$$

2nd-Order Correlation Power Analysis on Mask-Reuse Implementation

Classical Approach

$$\rho_{\hat{k}}\left(\left(f_{\mathrm{opt}(\hat{z}_a^i)}\right)_i, \mathcal{C}\left(\ell^i_m, \ell^i_{z_a^i \oplus m}\right)_i\right)$$

Adapted Approach

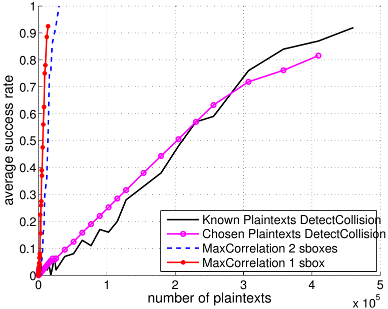
$$\rho_{\hat{k}_a, \hat{k}_b}\left(\left(f_{\mathrm{opt}(\hat{z}_a^i, \hat{z}_b^i)}\right)_i, \mathcal{C}\left(\ell^i_{z_a^i \oplus m}, \ell^i_{z_b^i \oplus m}\right)_i\right)$$

$$\left\{\begin{array}{lcl} k_1, k_2 & = & \alpha_{1,2} \\ k_1, k_3 & = & \alpha_{1,3} \\ & \vdots & \\ k_1, k_{n-1} & = & \alpha_{1,n-1} \\ k_1, k_n & = & \alpha_{1,n} \\ k_2, k_3 & = & \alpha_{2,3} \\ & \vdots & \\ k_{n-1}, k_n & = & \alpha_{n-1,n} \end{array}\right.$$

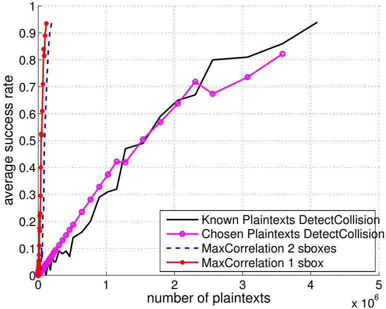
Simulations on two bytes

Simulations Hamming Weight + Gaussian Noise

$\sigma = 4$



$\sigma = 7$



Experiments on AES Mask-Reuse Implementation

Description

- component: 8-bit MCU
- side-channel: electromagnetic radiations
- sampling rate: 10G samples per seconds

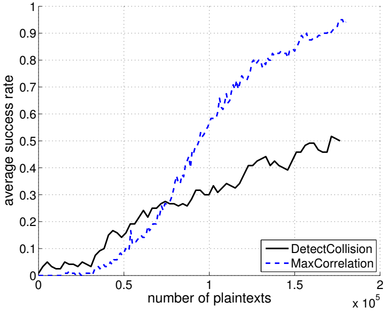
Noise Standard Deviation

	S-box 1	S-box 2	S-box 3	S-box 4
σ	6.0	3.7	3.4	3.3

Focusing on two bytes

Attacks on the MCU

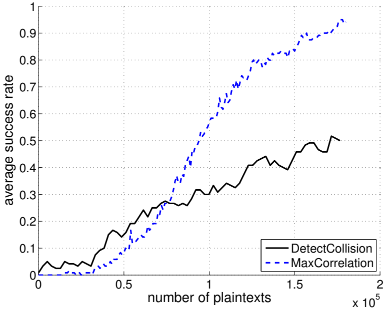
Results on real traces



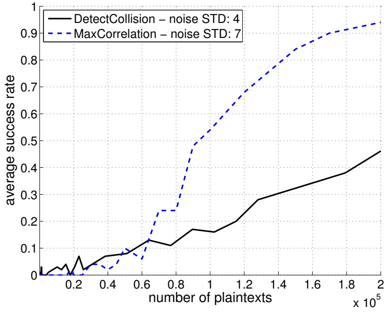
Focusing on two bytes

Attacks on the MCU

Results on real traces



Simulations Co-co: $\sigma = 4$ Simulations 2O-CPA: $\sigma = 7$



Attacks on the whole 16-byte key

	Raw Attack	Hard Decoding	Soft Decoding
Co-co	> 200000	123000	50000
2O-CPA	160000	73000	X

To sum up (on our MCU)

- The use of decoding techniques helps a lot the attack efficiency.
- Collision-Correlation attack was less efficient that 2O-CPA (on our component).