A Statistical Model for Higher Order DPA on Masked Devices

A. Adam Ding[1], Liwei Zhang[1], Yunsi Fei[2], Pei Luo[2]
[1]: Department of Mathematics, Northeastern University
[2]:Department of Electrical and Computer Engineering
Northeastern University

Acknowledgment: National Science Foundation CNS-1314655, CNS-1337854

Northeastern University

Outline

- Algorithmic confusion analysis for power analysis attack
  - Confusion coefficient for DPA, CPA – $\kappa\,(k_i, k_j)$
  - Model for DPA/CPA, success rate
- Success rate for higher order centered product combination attack (higher order CPA) on masking countermeasures
- Equivalence between the maximum-likelihood (ML) attack and the centered product combination attack

Preliminaries ([CHES 2012]): Algorithmic Confusion Analysis for mono-bit DPA

- Confusion coefficient: an algorithmic metric to reveal key distinguishability
- Confusion coefficient between two keys (k_i, k_j):

$$\kappa = \kappa(k_i, k_j) = Pr[(V \mid k_i) \neq (V \mid k_j)] = \frac{N_{(V|k_i) \neq (V|k_j)}}{N_t}$$

- Three-way confusion coefficient:

$$\tilde{\kappa} = \tilde{\kappa}(k_h, k_i, k_j) = Pr[(V \mid k_i) = (V \mid k_j), (V \mid k_h) \neq (V \mid k_i)]$$

- Confusion Lemma :

$$\tilde{\kappa}(k_h, k_i, k_j) = \frac{1}{2}[\kappa(k_h, k_i) + \kappa(k_h, k_j) - \kappa(k_i, k_j)]$$

Statistical Model for DPA ([CHES 2012])

- Power consumption leakage model with additive Gaussian noises: $\boldsymbol{l}_m = \varepsilon \boldsymbol{v}_m + c + \sigma r_m \quad m = 1, \cdots, n$
  - l_m (leakage), $v_m = \psi(x_m, k)$ is the select function, and r_m is the random noise, following a Gaussian distribution N(0, 1)
- Signal-to-noise ratio of the side channel: $SNR \quad \delta = \varepsilon / \sigma$
- For DPA model, the distance of means (DoM) attack

$$SR = \Phi_{N_k - 1}(\sqrt{n}\boldsymbol{\Sigma}^{-1/2}\boldsymbol{\mu})$$

where μ and $\sum$ are expressed by SNR and confusion coefficients.

Extension to CPA

$$\boldsymbol{l}_m = \varepsilon \mathbf{v}_m + c + \sigma r_m \qquad m = 1, \cdots, n$$

- v_m is Hamming distance/weight of multiple bits.
- Two-way confusion coefficient:

$$\kappa = \kappa(k_i, k_j) = E[(V|k_i - V|k_j)^2]$$

- Three-way confusion coefficient:

$$\tilde{\kappa} = \tilde{\kappa}(k_h, k_i, k_j) = E[(V|k_h - V|k_i)(V|k_h - V|k_j)]$$

$$\tilde{\kappa}^* = \tilde{\kappa}^*(k_h, k_i, k_j) = E[(V|k_h - V|k_i)(V|k_h - V|k_j)(V|k_h - E(V|k_h))^2]$$

- Confusion lemma still holds for:

$$\tilde{\kappa}(k_h, k_i, k_j) = \frac{1}{2}[\kappa(k_h, k_i) + \kappa(k_h, k_j) - \kappa(k_i, k_j)]$$

Success Rates for 1st Order CPA

- Under the CPA model:

$$\boldsymbol{\mu} = \frac{1}{2}\left(\frac{\varepsilon}{\sigma}\right)^2 \boldsymbol{\kappa} \qquad \boldsymbol{\Sigma} = \left(\frac{\varepsilon}{\sigma}\right)^2 \boldsymbol{K} + \frac{1}{4}\left(\frac{\varepsilon}{\sigma}\right)^4 (\boldsymbol{K}^* - \boldsymbol{\kappa}\boldsymbol{\kappa}^T)$$

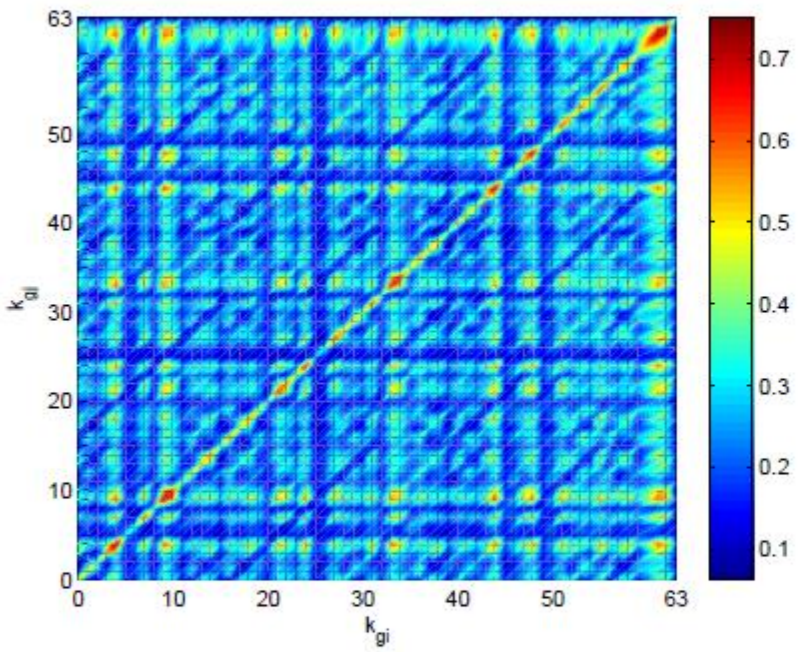
  - **κ** is called the "confusion vector", consisting of N_k*-1* two-way confusion coefficients $\kappa(k_c,k_g)$
  - **K** and **K*** are "confusion matrices", $(N_k\text{-}1)x(N_k\text{-}1)$, consisting of three-way confusion coefficients $\tilde{\kappa}(k_c, k_{g_i}, k_{g_j})$ and $\tilde{\kappa}^*(k_c, k_{g_i}, k_{g_j})$
- The success rate of the CPA (unmasked):

$$SR = \Phi_{N_k-1}\left\{ \sqrt{n}\,\frac{\varepsilon}{2\sigma}\left[\boldsymbol{K} + \left(\frac{\varepsilon}{2\sigma}\right)^2 (\boldsymbol{K}^* - \boldsymbol{\kappa}\boldsymbol{\kappa}^T)\right]^{-1/2} \boldsymbol{\kappa} \right\}$$

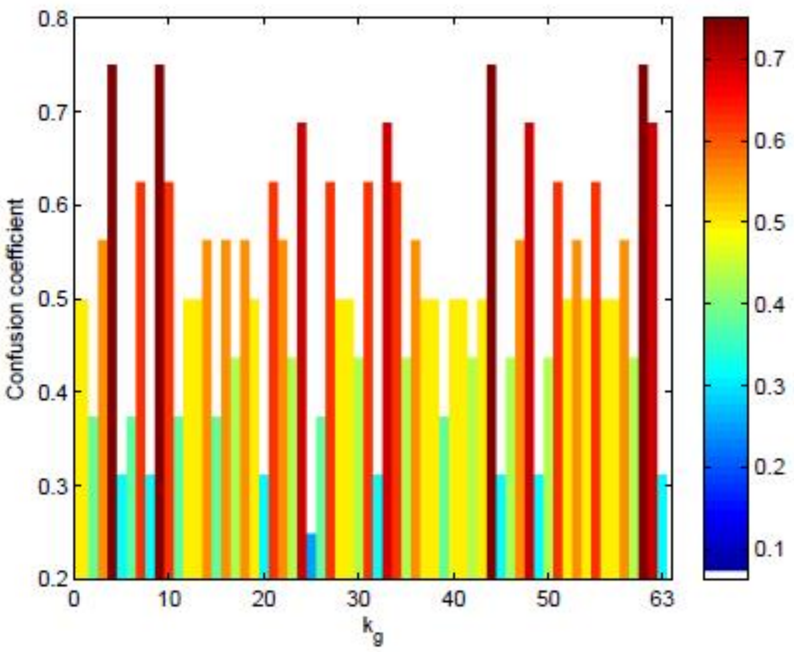
- http://eprint.iacr.org/ Report 2014/152

Experimental Results for DES

- Confusion matrix **K** of DPA on the first bit of the first SBox



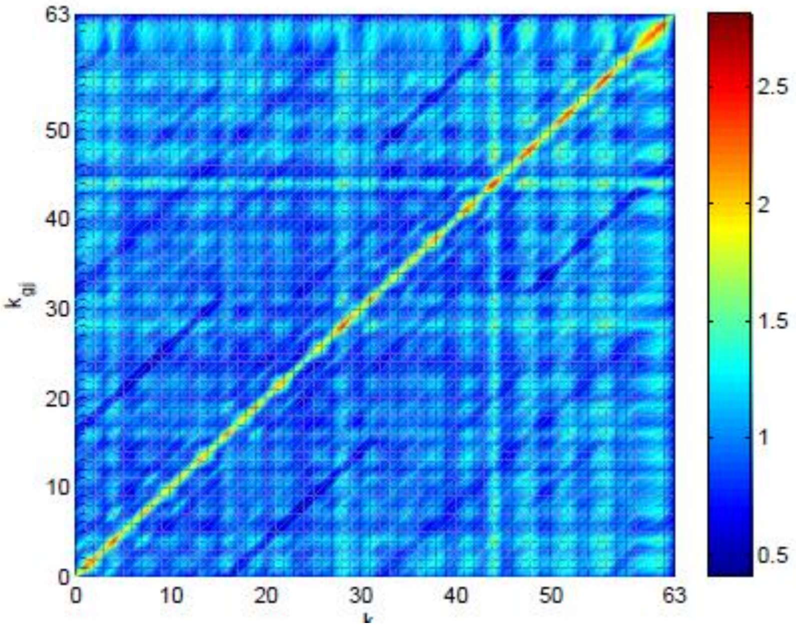
Confusion matrix **K** of DPA



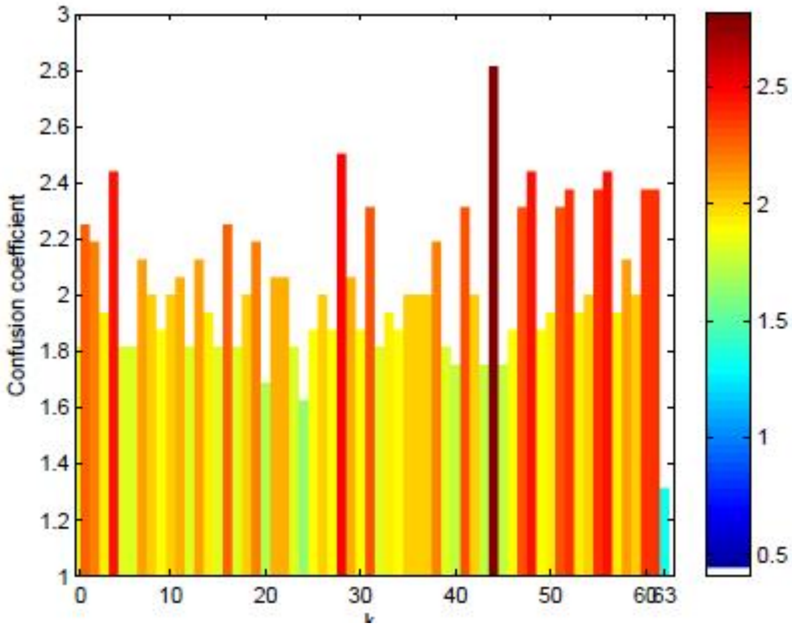
Diagonal of **K** – confusion vector **κ** of DPA

Results for DES (II)

- Confusion matrix **K** of CPA on the first DES SBox



Confusion matrix **K** of CPA



Diagonal of **K** – confusion vector $\boldsymbol{\kappa}$ of CPA

DPA vs. CPA

- DPA is a special case of CPA
- Under DPA model, **K** = **K***
- When the SNR is small, all the success rate (for ML attack, DPA, and CPA) become:

$$SR = \Phi_{N_k - 1}\{\sqrt{n}\,\frac{\varepsilon}{2\sigma}\,\boldsymbol{K}^{-1/2}\boldsymbol{\kappa}\}$$

2nd Order CPA on Masked Devices

- Using two leakage times points: one leaks mask M and the other leaks $Z(x, k) \oplus$ M.
  - Time point t_0: $L(t_0) = L_0 = \varepsilon_0 V_0 + c_0 + \sigma_0 r_0$
  - Time point t_1: $L(t_1) = L_1 = \varepsilon_1 V_1 + c_1 + \sigma_1 r_1$

  with $V_1 = HW(M)$ and $V_0 = HW(Z \oplus M)$,
- 2nd Order CPA: maximum correlation between the centered product of $L(t_0)L(t_1)$ and HW(Z).

Success Rates (SR) for 2nd Order CPA

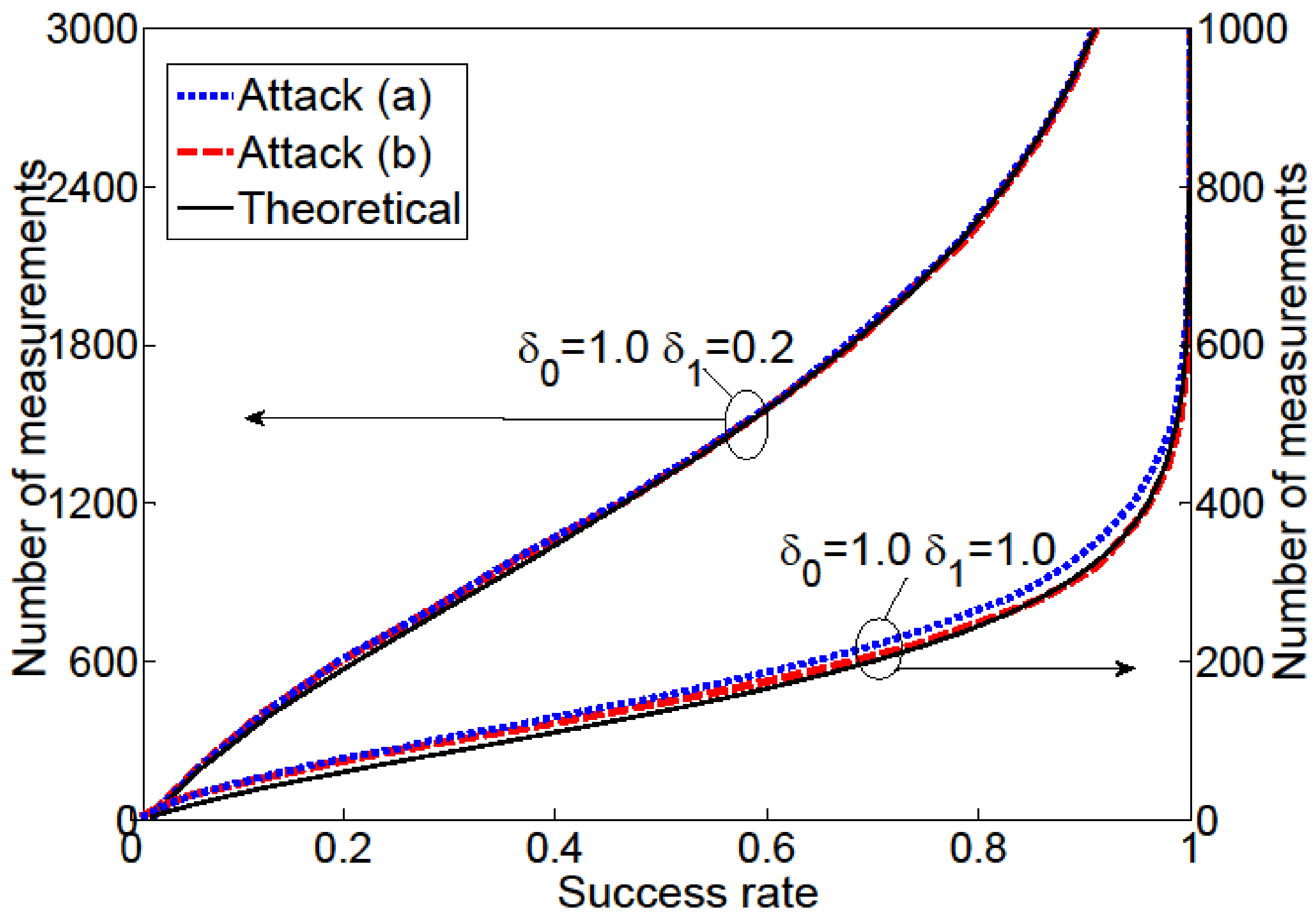
- Under the Hamming Weight/Distance model:

$$\boldsymbol{\mu} = \frac{1}{4}\delta_0^2\delta_1^2\boldsymbol{\kappa}$$

$$\boldsymbol{\Sigma} = \delta_0^2\delta_1^2(1+\frac{b}{4}\delta_0^2)(1+\frac{b}{4}\delta_1^2)\mathbf{K} + \frac{1}{16}\delta_0^4\delta_1^4(2\mathbf{K}^* - \frac{b}{2}\mathbf{K} - \boldsymbol{\kappa}\boldsymbol{\kappa}^T)$$

  - **κ , K** and **K*** are exactly the same as in the unmasked case.
- The formula does not assume Gaussian noise.
- Including second term, SR formula fits simulated SR for moderate SNR≈1

Success Rates for 2nd Order Attack



Black is the theoretical, Red is the simulated SR for CPA, blue for ML

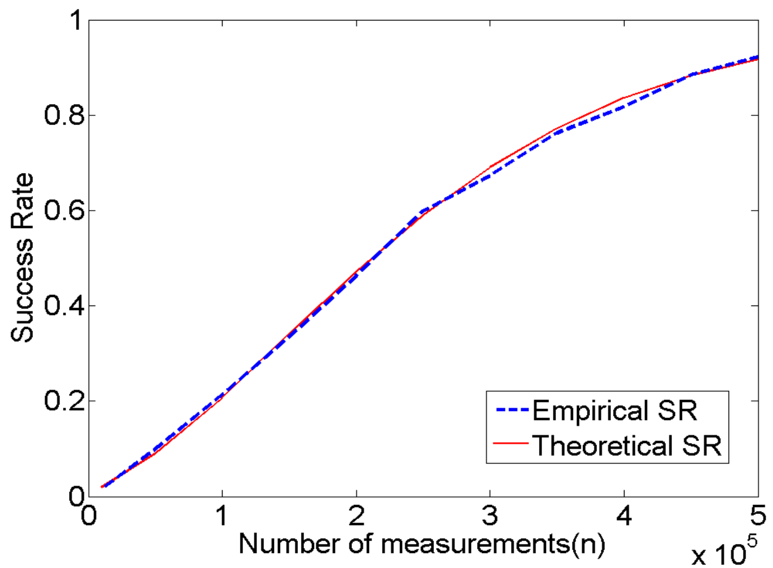
Use SR formula for 2nd Order CPA

- Quantify masking effect explicitly (small SNR):
  - 2nd Order CPA (leading term, for small SNR):

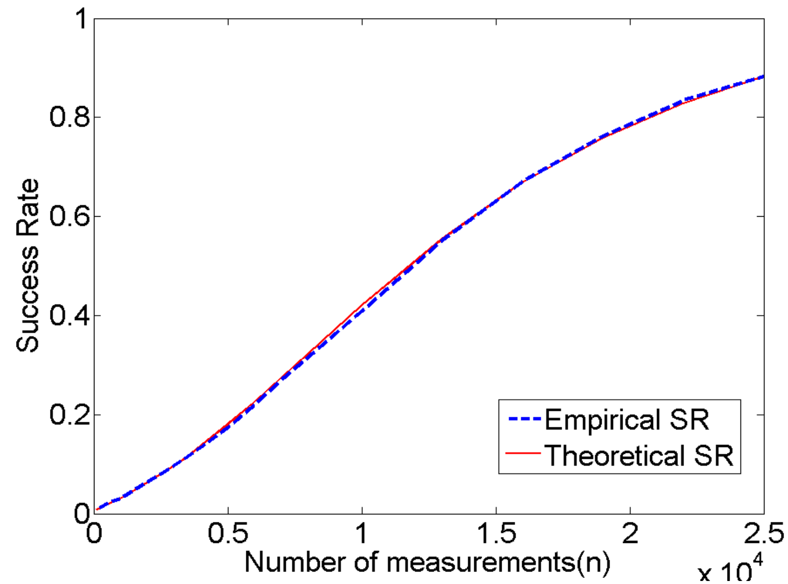
$$SR = \Phi_{N_k - 1}\{\sqrt{n}\,\frac{\delta_0 \delta_1}{4}\,\mathbf{K}^{-1/2}\boldsymbol{\kappa}\}$$

  - Versus unmasked CPA: $SR = \Phi_{N_k - 1}\{\sqrt{n}\,\frac{\delta}{2}\,\mathbf{K}^{-1/2}\boldsymbol{\kappa}\}$
- Masking increasing required sample size by $(2/\delta)^2$
- Faster evaluation: find SNR δ then plug-in.
- In next slide, find SNR from 10,000 traces, compare SR to empirical SR from 1.4M traces

Success Rates for 2^{nd} Order Attack



Empirical versus theoretical success rates on measurement data of a masked AES FPGA implementation



Empirical versus theoretical success rates on simulated data with Lapalace noise instead of Gaussian noise.

Higher Order CPA Success Rate

- J masks, process $Z \bigoplus_{j=1}^{J} M_j$
- J+1 order attack, at time points t_j

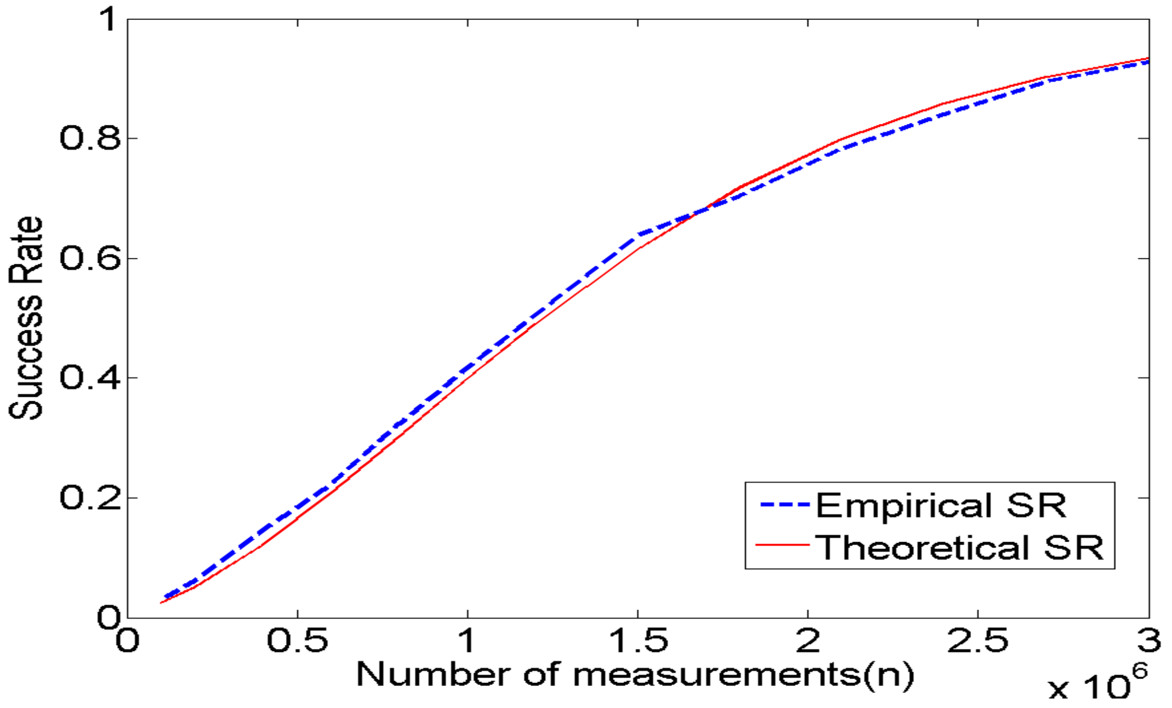
$j = 0,1,\ldots,J$ leaks $V_0 = V_0(Z \bigoplus_{j=1}^{J} M_j)$ and

$V_1 = V_1(M_1),\ldots,V_J = V_J(M_J)$

- Success Rate:

$$SR = \Phi_{N_k-1}(\sqrt{n}\Sigma^{-1/2}\mu) = \Phi_{N_k-1}\left(\frac{\sqrt{n}\prod_{j=0}^{J}\delta_j}{2^{J+1}}\vec{K}^{-1/2}\vec{\kappa}\right).$$

Success Rates for 3rd Order Attack



Empirical versus theoretical success rates on simulated data, SNR=0.2

2nd Order Maximum Likelihood ML-Attack

- The ML-attack statistic T:

$$T_{k_g} = \frac{1}{n}\sum_{i=1}^{n} \log f(\vec{l}_i \mid k_g)$$

$$= \frac{1}{n}\sum_{i=1}^{n} \log[\frac{1}{|\mathcal{M}|}\sum_{m \in \mathcal{M}} f_0(l_{i,0} \mid k_g, m) f_1(l_{i,1} \mid m)]$$

- The likelihood iterates over all possible mask values in $\mathcal{M}$
- The iteration is of order $|\mathcal{M}|$, and would increase exponentially with the order of masks.
- For Gaussian noises, this is a mixture Gaussian density.

2nd Order Attack Model

$$L_0 = \varepsilon_0 V_0 + c_0 + \sigma_0 r_0 \qquad L_1 = \varepsilon_1 V_1 + c_1 + \sigma_1 r_1$$

$$l_0^* = (L_0 - c_0)/\sigma_0 = \delta_0 V_0 + r_0 \qquad l_1^* = \delta_1 V_1 + r_1$$

- When SNRs $\delta_0 \to 0$, $\delta_1 \to 0$, the ML-attack statistic T_{k_g} has key-independent limit

$$\frac{1}{n}\sum_{i=1}^{n} \log[\frac{1}{|\mathcal{M}|}\sum_{m \in \mathcal{M}} f_r(l_{i,0}^* - \delta_0 V_0(k_g, m)) f_r(l_{i,1}^* - \delta_1 V_1(m))]$$

$$\to \frac{1}{n}\sum_{i=1}^{n} \log[f_r(r_{i,0}) f_r(r_{i,1})]$$

2nd Order Attack Approximation

- When SNRs $\delta_0 \to 0$, $\delta_1 \to 0$, do a Taylor expansion within the $E_m = \frac{1}{|\mathcal{M}|} \sum_{m \in \mathcal{M}}$ operation, and on the log[.]
- The first term after E_m operation is key independent. The key selection happens on the second term, which is equivalent to the centered product combination attack (2O CPA) statistic

$$\frac{1}{n}\sum_{i=1}^{n}[(l_{i,0} - El_{i,0})(l_{i,1} - El_{i,1})g(Z_i^g)]$$ with

$g(Z_i^g) = E_m[V_0(k_g, m)V_1(m)]$, for Hamming Weights model, $g(Z_i^g) \propto H(Z_i^g)$

For Higher Order Masking

- The centered product combination attack is the strongest possible attack for noisy (small SNRs) situation, Gaussian noise.
- Generally, the key selection happens on the second term of Taylor expansion: can find efficient attack asymptotic equivalent to ML-attack. (J+1)th for J order masking.
- Valid Taylor Approximation when the noise density has continuous third derivative.

Acknowledgments

- Project webpage: **http://tescase.coe.neu.edu**
- Funding
  - NSF SaTC TWC: Medium: A unified statistics-based framework for side-channel attack analysis and security evaluation of cryptosystems
  - NSF MRI: Development of a Testbed for Side-Channel Analysis and Security Evaluation -TeSCASE
- Collaborators
  - NU: Yunsi Fei, Dave Kaeli, Miriam Leeser
  - WPI: Thomas Eisenbarth
- Students
  - PhD students: Liwei Zhang, Pei Luo, Jian Lao, Zhen Hang Jiang
  - Undergraduate students: Neel Shah, Tushar Swamy, Ang Shen