A Statistical Model for DPA with Novel Algorithmic Confusion Analysis

Yunsi Fei[1], Qiasi Luo[2], and A. Adam Ding[3]
1: Department of Electrical and Computer Engineering
Northeastern University
2: Marvell Technology Group Ltd., Santa Clara
3: Department of Mathematics, Northeastern University

Acknowledgment: NSF CNS-0845871

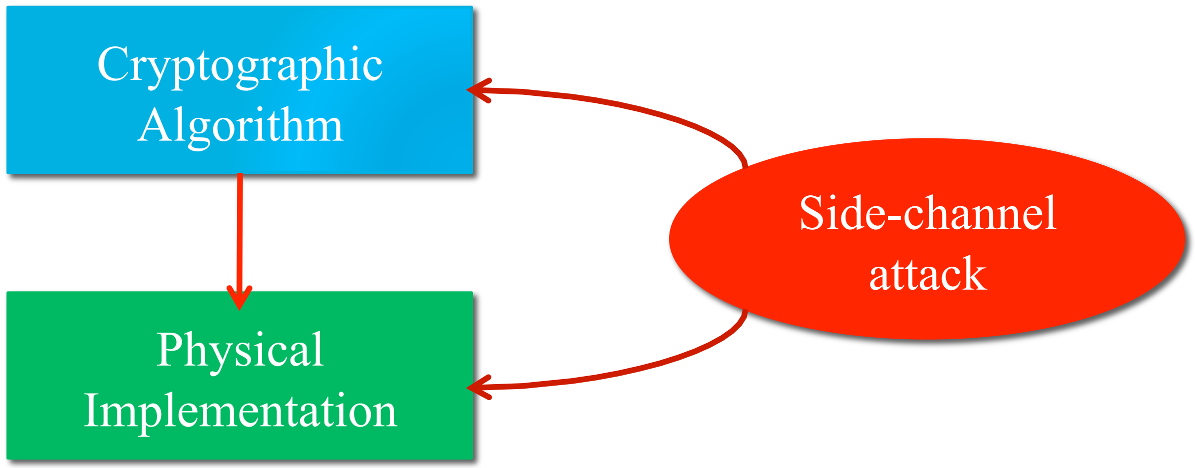
Northeastern University

Outline

- Introduction and preliminaries
- Algorithmic confusion analysis – $\kappa\ (k_i, k_j)$
- Statistical model for DPA – success rate formula
- Experimental results
- Conclusion

Side-channel Attacks

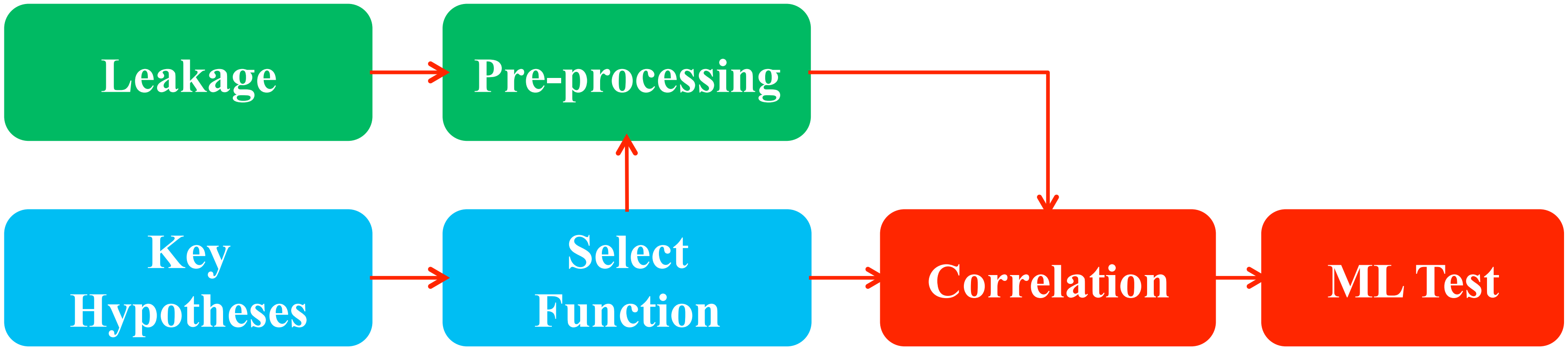
- SCA: Explore the correlation of physical leakage (power consumption, timing, or electromagnetic emanation) of a cryptographic system with its internal computations to retrieve secrete information, e.g., the private key
- Both ***algorithm*** and ***implementation*** affect SCA resilience of a cryptographic system
  - How to implement SCA-secure hardware?
  - How to design leakage-resilient cryptographic algorithm?



Differential Power Analysis (DPA) Procedure

- Implementation:
  - Leakage: $W=\{W_1, \ldots, W_{Nm}\}, W_i=\{W_{i,1}, \ldots, W_{i,p}\}$
- Algorithm:
  - Select function: $V=\psi(d)$, where $d=\text{Sbox}(x\oplus k)$
- Attack:
  - Correlation: For DPA, Difference-of-means (DoM):

$$\delta = \frac{\sum W_{\psi=1}}{N_{\psi=1}} - \frac{\sum W_{\psi=0}}{N_{\psi=0}} \qquad N_m = N_{\psi=1} + N_{\psi=0}$$



Maximum Likelihood Estimation

- Neyman-Pearson Lemma (Maximum Likelihood):

$$\widehat{\theta} = \arg\max \sum_{i=1}^{n} \log f_Y(y_i;\theta)$$

  - $f_Y(y;\theta)$: the probability density function for the random variable Y with parameters θ
  - In SCA, Y is the physical leakage, θ is the embedded key
  - In DPA, choosing the key that maximizes the DoM, δ, is equivalent to ML attack on the select function
- Central limit theorem
  - A random variable $\boldsymbol{X}$ with distributed population: (μ, σ)
  - Randomly select a sample of size n, $\{X_1, \ldots, X_n\}$, and get the sample mean : $\overline{X} = \frac{1}{n}\sum_{i=1}^{n} X_i$
  - As $n \rightarrow \infty$, $\overline{X}$ is a random variable with normal distribution $N(\mu, \frac{\sigma}{\sqrt{n}})$

Central Limit Theorem and DPA

- DPA: a sampling process on the entire waveform population
  - $W_{\psi=1}$ and $W_{\psi=0}$: random variables with normal distribution:

$$N(\varepsilon + b, \frac{\sigma_w}{\sqrt{N_{\psi=1}}}) \qquad N(b, \frac{\sigma_w}{\sqrt{N_{\psi=0}}})$$

    - b: mean power consumption for the waveform group $\psi=0$
    - ε: power difference related to the bit under DPA attack $\lim_{N_m \to \infty} \delta_c = \varepsilon$

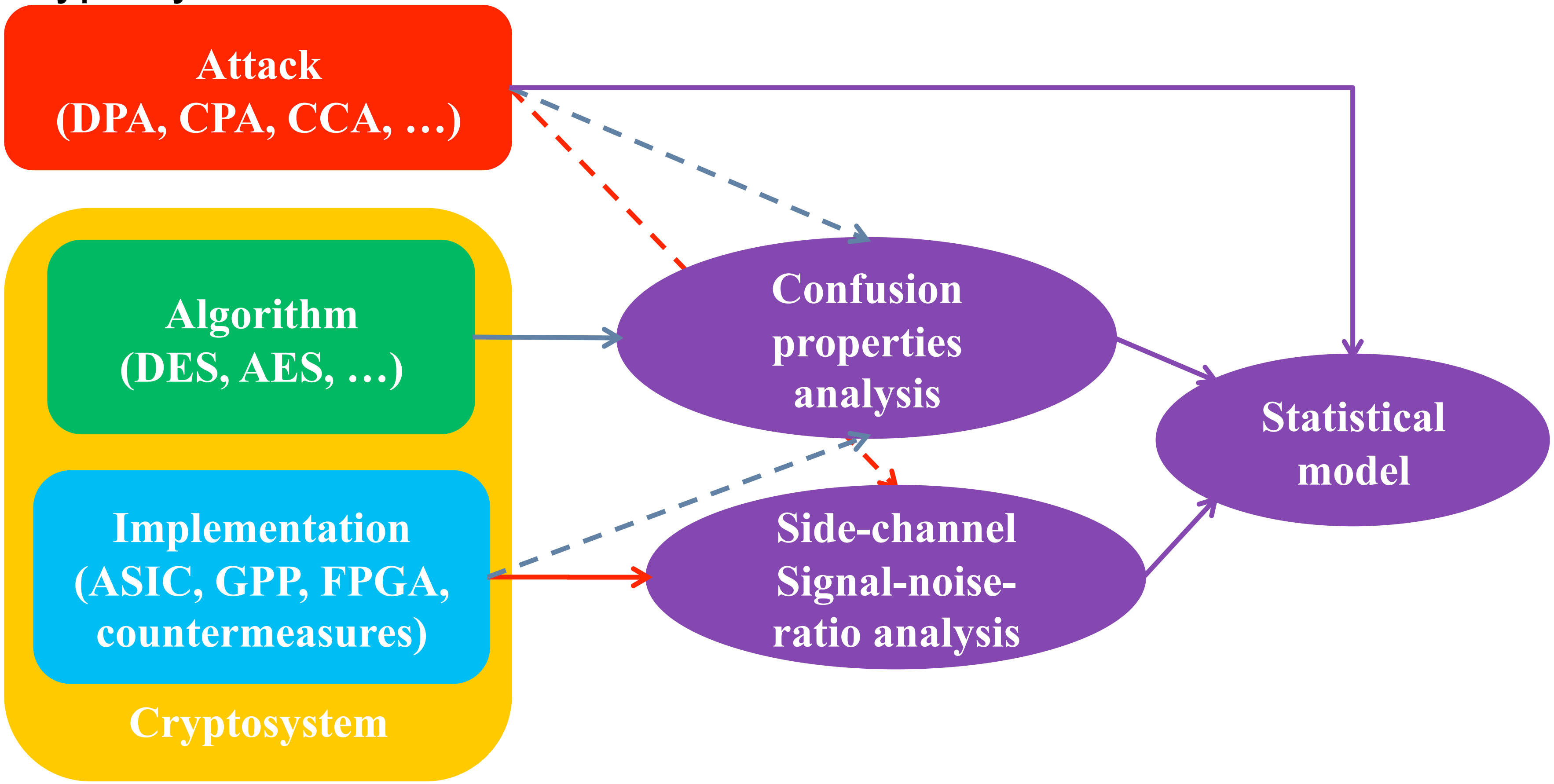
  - Therefore, the DoM of the correct key (k_c), δ_c, is a random variable with normal distribution:

$$N(\varepsilon, 2\frac{\sigma_w}{\sqrt{N_m}})$$

$$\delta = \frac{\sum W_{\psi=1}}{N_{\psi=1}} - \frac{\sum W_{\psi=0}}{N_{\psi=0}}$$

Overview of the Statistical Framework

- Algorithmic confusion analysis: for the algorithm with a certain attack considered
- Signal-noise-ratio: for the implementation under a certain attack
- Statistical model for the success rate of the attack against a chosen cryptosystem



Algorithmic Confusion Analysis

- Confusion coefficient between two keys (k_i, k_j):

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

  - N_t: the total number of values for the relevant ciphertext bits
  - $N(\psi|k_i) \neq (\psi|k_j)$: the number of occurrences (ciphertext) for which different key hypotheses k_i and k_j result in different ψ values

Confusion Lemmas

- Lemma 1: Confusion Lemma

$$\Pr[(\psi \mid k_i) = 0, (\psi \mid k_j) = 1] = \Pr[(\psi \mid k_i) = 1, (\psi \mid k_j) = 0] = \frac{1}{2}\kappa$$

$$\Pr[(\psi \mid k_i) = 1, (\psi \mid k_j) = 1] = \Pr[(\psi \mid k_i) = 0, (\psi \mid k_j) = 0] = \frac{1}{2}(1-\kappa)$$

- Lemma 2: Three-way confusion coefficient

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

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

Confusion Coefficient and DPA

- Denote the embedded key as k_c and an incorrect key as k_g, the DoMs for k_c and k_g are δ_c and δ_g
- The difference between the two DoMs is:

$$\Delta(k_c, k_g) = (\delta_c - \delta_g)$$

$$E[\Delta(k_c, k_g)] = 2\kappa(k_c, k_g)\varepsilon$$

$$Var[\Delta(k_c, k_g)] = 16\kappa(k_c, k_g)\frac{\sigma_w^2}{N_m} + 16\kappa(k_c, k_g)[1 - \kappa(k_c, k_g)]\frac{\varepsilon^2}{N_m}$$

$$\lim_{N_m \to \infty} \Delta(k_c, k_g) = 2\kappa(k_c, k_g)\varepsilon$$

A Statistical Model for DPA

- To successfully distinguish key k_c from other key guesses, the DoM of k_c should be larger than all other keys'
- The success rate to recover the correct key:

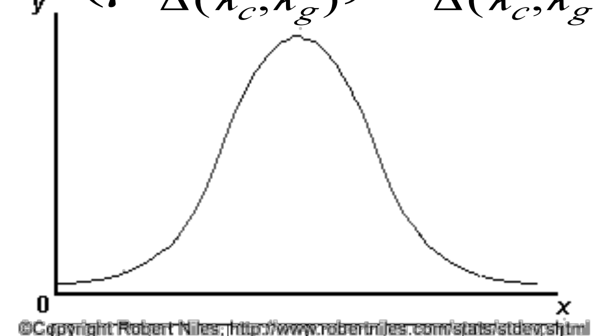
$$SR = SR[k_c, \langle \overline{k_c} \rangle] = \Pr[\delta_{k_c} > \delta_{\langle \overline{k_c} \rangle}]$$

1-key success rate

- The success rate of k_c over an incorrect key k_g chosen out of $\langle \overline{k_c} \rangle$:

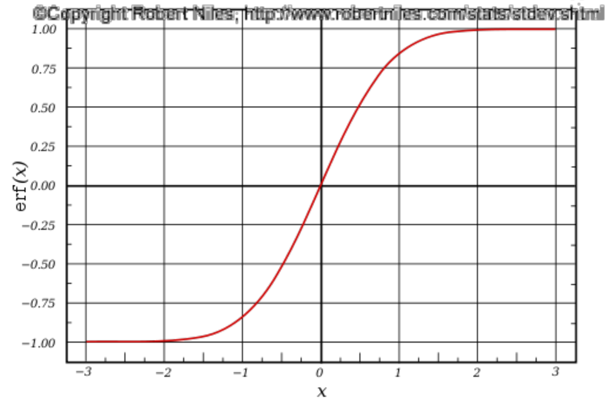
$$SR_1 = SR[k_c, k_g] = \Pr[\delta_{k_c} > \delta_{k_g}] = \Pr[\Delta(k_c, k_g) > 0]$$

- As $\Delta(k_c, k_g)$ follows distribution of: $\mathcal{N}(\mu_{\Delta(k_c,k_g)}, \sigma_{\Delta(k_c,k_g)})$



$$SR_1 = \Pr[\Delta(k_c, k_g) > 0]$$

$$= \frac{1}{2}[1 + erf(\sqrt{\frac{\kappa(k_c, k_g)}{(\frac{2\sigma_w}{\varepsilon})^2 + (1 - \kappa(k_c, k_g))}}\sqrt{\frac{N_m}{2}})]$$



2-key Success Rate

- The success rate of k_c over two chosen incorrect keys k_{g1} and k_{g2}:

$$SR_2 = SR[k_c, \{k_{g1}, k_{g2}\}] = \Pr[\delta_{k_c} > \delta_{k_{g1}}, \delta_{k_c} > \delta_{k_{g2}}]$$

$$= \Pr[y_1 > 0, y_2 > 0] = \Pr[\mathbf{Y_2} > 0]$$

- Where $y_1 = \Delta(k_c, k_{g1}) = \delta_{k_c} - \delta_{k_{g1}}$

$$y_2 = \Delta(k_c, k_{g2}) = \delta_{k_c} - \delta_{k_{g2}}$$

- y_1 and y_2 are random variables with normal distribution, $\mathbf{Y_2}=[y_1, y_2]^T$ is a random vector with 2-d normal distribution $N(\boldsymbol{\mu}_2, \Sigma_2)$

$$\boldsymbol{\mu}_2 = \begin{bmatrix} \mu_{y_1} \\ \mu_{y_2} \end{bmatrix} = \begin{bmatrix} 2\kappa(k_c, k_{g1})\varepsilon \\ 2\kappa(k_c, k_{g2})\varepsilon \end{bmatrix} \quad \sum\nolimits_2 = \begin{bmatrix} Cov(y_1, y_1) & Cov(y_1, y_2) \\ Cov(y_1, y_2) & Cov(y_2, y_2) \end{bmatrix}$$

2-key Success Rate (Contd.)

$$Cov(y_1, y_1) = 16\kappa(k_c, k_{g1})\frac{\sigma_w^2}{N_m} + 4\kappa(k_c, k_{g1})[1 - \kappa(k_c, k_{g1})]\frac{\varepsilon^2}{N_m}$$

$$Cov(y_2, y_2) = 16\kappa(k_c, k_{g2})\frac{\sigma_w^2}{N_m} + 4\kappa(k_c, k_{g2})[1 - \kappa(k_c, k_{g2})]\frac{\varepsilon^2}{N_m}$$

$$Cov(y_1, y_2) = 16\tilde{\kappa}(k_c, k_{g1}, k_{g2})\frac{\sigma_w^2}{N_m} + 4[\tilde{\kappa}(k_c, k_{g1}, k_{g2}) - \kappa(k_c, k_{g1})\kappa(k_c, k_{g2})]\frac{\varepsilon^2}{N_m}$$

- $\Phi_2(x)$ denotes the cdf of the 2-dimension standard normal distribution:

$$SR_2 = \Phi_2\left(\sum\nolimits_2^{-1/2} \boldsymbol{\mu}_2\right)$$

$(N_k$-1)-keys Success Rate

- The overall success rate:

$$SR = SR_{N_k-1} = SR[k_c, \langle \overline{k_c} \rangle] = \Pr[\delta_{k_c} > \{\delta_{\langle \overline{k_c} \rangle}\}] = \Pr[\mathbf{Y} > 0]$$

- $\mathbf{Y}$ is the $(N_k$-$1)$-dimension vector of differences between δ_{k_c} and $\delta_{\langle \overline{k_c} \rangle}$

$$SR = SR_{N_k-1} = \Phi_{N_k-1}\left(\sum\nolimits_Y^{-1/2} \boldsymbol{\mu}_Y\right)$$

$$\boldsymbol{\mu}_{\mathbf{Y}} = 2\varepsilon\boldsymbol{\kappa} \qquad \sum\nolimits_Y = 16\frac{\sigma_w^2}{N_m}\mathbf{K} + 4\frac{\varepsilon^2}{N_m}(\mathbf{K} - \kappa\kappa^T)$$

- $\mathbf{K}$ is the $(N_k$-$1) \times (N_k$-$1)$ confusion matrix $\{\chi_{ij}\}$

$$\chi_{ij} = \begin{cases} \kappa(k_c, k_{gi}) & if\ i = j \\ \tilde{\kappa}(k_c, k_{gi}, k_{gj}) & if\ i \neq j \end{cases}$$

Experimental Results

- Empirical and theoretical success rates of DPA on DES and AES

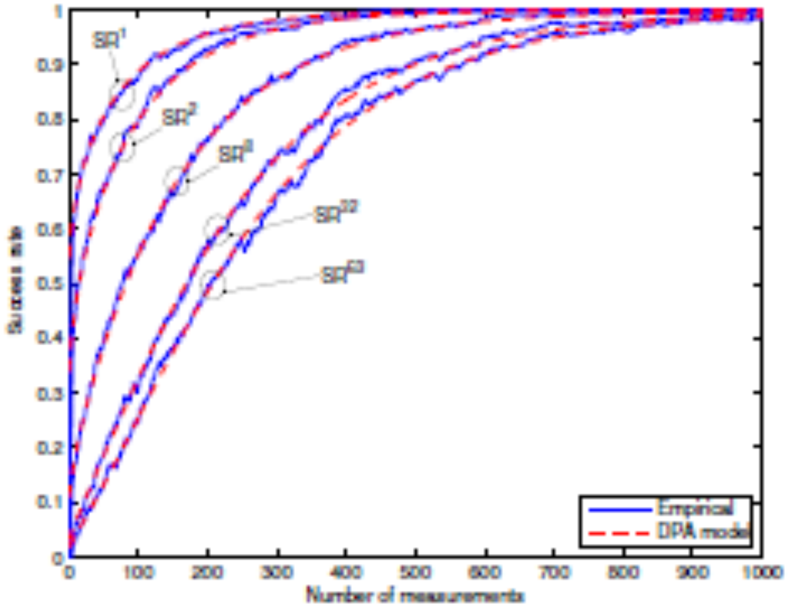


Fig. 1. Empirical and theoretical success rates of DPA on DES.

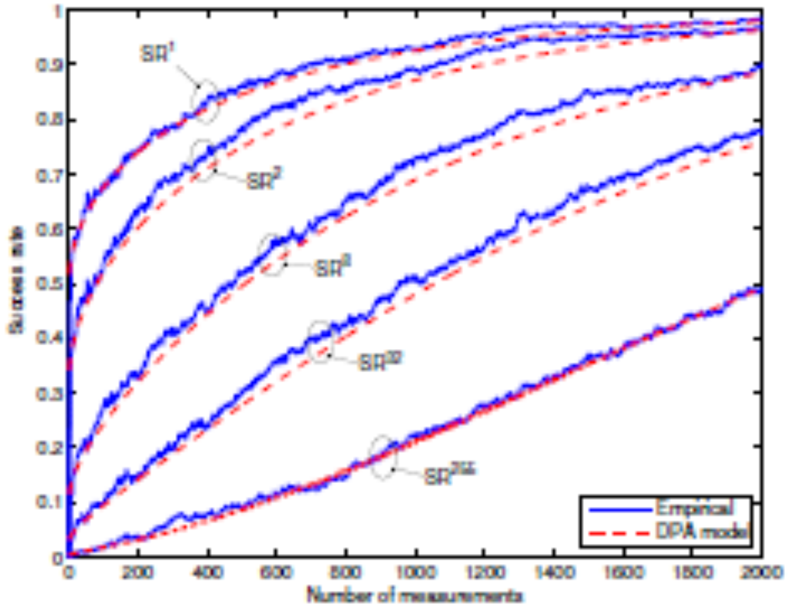


Fig. 2. Empirical and theoretical success rates of DPA on AES.

Discussions

- Signal-to-noise ratio of the side channel: $SNR = \varepsilon / \sigma_w$
- Other attacks:
  - CPA: Select function – Hamming weight of multi-bits

    Correlation - Pearson Correlation

    Confusion coefficients – the mean value of differences between the squared select function values (for two keys)
- Evaluation of DPA countermeasures
  - Masking: change the algorithm, no change to the implementation (SNR)
  - Power balance logic: change the implementation by trying to reduce ε to zero
  - Random delay: no change to the algorithm, change the signal level

Yunsi Fei

Associate Professor

Department of Electrical and Computer Engineering

Northeastern University Energy-efficient and Secure Systems Lab

URL: http://nueess.coe.neu.edu

Kappas

- DPA on DES:

  {0.25, 0.3125, 0.375, 0.4375, 0.5, 0.5625, 0.625, 0.6875, 0.75}

- DPA on AES:

  {0.4375, 0.453125, 0.46875, 0.484375, 0.5, 0.515625, 0.53125, 0.546875, 0.5625}