On the Optimal Pre-processing for Non-profiling Differential Power Analysis

Suvadeep Hajra and Debdeep Mukhopadhyay

Indian Institute of Technology Kharagpur

COSADE'14, Paris, France
April 14-15, 2014

Outline

- Introduction
- Optimal Pre-processing of the Power Traces
- Experimental Evaluation
- Comparison with profiling Stochastic attack
- Conclusion

Introduction

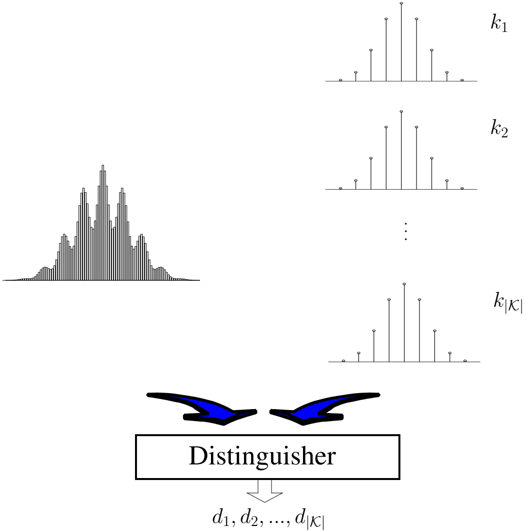

Figure: DPA Attack

Introduction (cont.)

- Univariate DPA
  - Univariate distinguisher is applied on a selected sample point
- Multivariate DPA
  - univariate distinguisher is applied on every sample point independently
  - best result is chosen
  - performs poorly when the SNR of the leakage are low
- Power traces are pre-processed to increase the SNR of the leakage

Introduction (cont.)

- Univariate DPA
  - Univariate distinguisher is applied on a selected sample point
- Multivariate DPA
  - univariate distinguisher is applied on every sample point independently
  - best result is chosen
  - performs poorly when the SNR of the leakage are low
- Power traces are pre-processed to increase the SNR of the leakage

Introduction (cont.)

- Univariate DPA
  - Univariate distinguisher is applied on a selected sample point
- Multivariate DPA
  - univariate distinguisher is applied on every sample point independently
  - best result is chosen
  - performs poorly when the SNR of the leakage are low
- Power traces are pre-processed to increase the SNR of the leakage

Introduction (cont.)

- Existing Pre-processing techniques
  1. Comb filter
  2. FFT
  3. Multiband filter
  4. Wavelet transform etc
- Mostly, heuristic in nature
- Optimal pre-processing using linear FIR has been proposed by Oswald et al. in [2]
  - requires semi-profiling approach
- Is optimal pre-processing possible in non-profiling DPA attacks?

Introduction (cont.)

- Existing Pre-processing techniques
  1. Comb filter
  2. FFT
  3. Multiband filter
  4. Wavelet transform etc
- Mostly, heuristic in nature
- Optimal pre-processing using linear FIR has been proposed by Oswald et al. in [2]
  - requires semi-profiling approach
- Is optimal pre-processing possible in non-profiling DPA attacks?

Introduction (cont.)

- Existing Pre-processing techniques
  1. Comb filter
  2. FFT
  3. Multiband filter
  4. Wavelet transform etc
- Mostly, heuristic in nature
- Optimal pre-processing using linear FIR has been proposed by Oswald et al. in [2]
  - requires semi-profiling approach
- Is optimal pre-processing possible in non-profiling DPA attacks?

Introduction (cont.)

- Existing Pre-processing techniques
  1. Comb filter
  2. FFT
  3. Multiband filter
  4. Wavelet transform etc
- Mostly, heuristic in nature
- Optimal pre-processing using linear FIR has been proposed by Oswald et al. in [2]
  - requires semi-profiling approach
- Is optimal pre-processing possible in non-profiling DPA attacks?

Matched Filter

- The output leakage l_o of a linear FIR of order T applied to the traces $\mathbf{l} = \{l_0, \cdots, l_{T-1}\}$

$$l_o = \sum_{t=0}^{T-1} h_t l_t \tag{1}$$

where $\mathbf{h} = \{h_0, \cdots, h_{T-1}\}$ is the impulse response of the filter

- Let centered (w.r.t. mean leakage) trace $\mathbf{l} = \{l_0, \ldots, l_{T-1}\}$ $= \{d_0 + n_0, \cdots, d_{T-1} + n_{T-1}\} = \mathbf{d} + \mathbf{n}$
- SNR of l_o is given by

$$SNR^{l_o} = \frac{|\mathbf{h}'\mathbf{d}|^2}{E[|\mathbf{h}'\mathbf{n}|^2]} = \frac{|\mathbf{h}'\mathbf{d}|^2}{\mathbf{h}'\Sigma_{\mathbf{N}}\mathbf{h}}$$

- Matched filter maximizes the SNR of l_o by suitably choosing the impulse response $\mathbf{h}$

- The output leakage l_o of a linear FIR of order T applied to the traces $\mathbf{l} = \{l_0, \cdots, l_{T-1}\}$

$$l_o = \sum_{t=0}^{T-1} h_t l_t \tag{1}$$

where $\mathbf{h} = \{h_0, \cdots, h_{T-1}\}$ is the impulse response of the filter

- Let centered (w.r.t. mean leakage) trace $\mathbf{l} = \{l_0, \ldots, l_{T-1}\}$ $= \{d_0 + n_0, \cdots, d_{T-1} + n_{T-1}\} = \mathbf{d} + \mathbf{n}$
- SNR of l_o is given by

$$SNR^{l_o} = \frac{|\mathbf{h}'\mathbf{d}|^2}{E[|\mathbf{h}'\mathbf{n}|^2]} = \frac{|\mathbf{h}'\mathbf{d}|^2}{\mathbf{h}'\Sigma_\mathbf{N}\mathbf{h}}$$

- Matched filter maximizes the SNR of l_o by suitably choosing the impulse response $\mathbf{h}$

Matched Filter

- The output leakage l_o of a linear FIR of order T applied to the traces $\mathbf{l} = \{l_0, \cdots, l_{T-1}\}$

$$l_o = \sum_{t=0}^{T-1} h_t l_t \tag{1}$$

  where $\mathbf{h} = \{h_0, \cdots, h_{T-1}\}$ is the impulse response of the filter
- Let centered (w.r.t. mean leakage) trace $\mathbf{l} = \{l_0, \ldots, l_{T-1}\}$ $= \{d_0 + n_0, \cdots, d_{T-1} + n_{T-1}\} = \mathbf{d} + \mathbf{n}$
- SNR of l_o is given by

$$SNR^{l_o} = \frac{|\mathbf{h}'\mathbf{d}|^2}{E[|\mathbf{h}'\mathbf{n}|^2]} = \frac{|\mathbf{h}'\mathbf{d}|^2}{\mathbf{h}'\Sigma_{\mathbf{N}}\mathbf{h}}$$

- Matched filter maximizes the SNR of l_o by suitably choosing the impulse response $\mathbf{h}$

Matched Filter

- The output leakage l_o of a linear FIR of order T applied to the traces $\mathbf{l} = \{l_0, \cdots, l_{T-1}\}$

$$l_o = \sum_{t=0}^{T-1} h_t l_t \tag{1}$$

  where $\mathbf{h} = \{h_0, \cdots, h_{T-1}\}$ is the impulse response of the filter

- Let centered (w.r.t. mean leakage) trace $\mathbf{l} = \{l_0, \ldots, l_{T-1}\}$ $= \{d_0 + n_0, \cdots, d_{T-1} + n_{T-1}\} = \mathbf{d} + \mathbf{n}$
- SNR of l_o is given by

$$SNR^{l_o} = \frac{|\mathbf{h}'\mathbf{d}|^2}{E[|\mathbf{h}'\mathbf{n}|^2]} = \frac{|\mathbf{h}'\mathbf{d}|^2}{\mathbf{h}'\Sigma_{\mathbf{N}}\mathbf{h}}$$

- Matched filter maximizes the SNR of l_o by suitably choosing the impulse response $\mathbf{h}$

Matched Filter (cont.)

- The impulse response of the matched filter for the trace $\mathbf{l}$ is given by ([3, 4])

$$\mathbf{h}_{MF} = \Sigma_{\mathbf{N}}^{-1}\mathbf{d}$$

- Both $\Sigma_{\mathbf{N}}$ and $\mathbf{d}$ need the *secret key* to estimate, thus are not feasible in non-profiling DPA

Matched Filter (cont.)

- The impulse response of the matched filter for the trace $\mathbf{l}$ is given by ([3, 4])
$$\mathbf{h}_{MF} = \Sigma_{\mathbf{N}}^{-1}\mathbf{d}$$
- Both $\Sigma_{\mathbf{N}}$ and $\mathbf{d}$ need the *secret key* to estimate, thus are not feasible in non-profiling DPA

Optimum Linear Filter in Non-profiling DPA

- We introduce *Signal Ratio* (SR) of the output signal l_o:

$$SR^{l_o} = \frac{|\mathbf{h}'\mathbf{d}|^2}{E[|\mathbf{h}'\mathbf{l}|^2]} = \frac{|\mathbf{h}'\mathbf{d}|^2}{\mathbf{h}'\Sigma_{\mathbf{L}}\mathbf{h}}$$

- The SNR of the output leakage l_o reaches its maximum if and only if SR of that also reaches its maximum
- Impulse response of the optimum linear filter which maximizes the SR of the output signal l_o

$$\mathbf{h}_{opt} = \Sigma_{\mathbf{L}}^{-1}\mathbf{d}$$

- The estimation of $\mathbf{d}$ still requires the correct key

Optimum Linear Filter in Non-profiling DPA

- We introduce *Signal Ratio* (SR) of the output signal l_o:

$$SR^{l_o} = \frac{|\mathbf{h}'\mathbf{d}|^2}{E[|\mathbf{h}'\mathbf{l}|^2]} = \frac{|\mathbf{h}'\mathbf{d}|^2}{\mathbf{h}'\Sigma_{\mathbf{L}}\mathbf{h}}$$

- The SNR of the output leakage l_o reaches its maximum if and only if SR of that also reaches its maximum
- Impulse response of the optimum linear filter which maximizes the SR of the output signal l_o

$$\mathbf{h}_{opt} = \Sigma_{\mathbf{L}}^{-1}\mathbf{d}$$

- The estimation of $\mathbf{d}$ still requires the correct key

Optimum Linear Filter in Non-profiling DPA

- We introduce *Signal Ratio* (SR) of the output signal l_o:

$$SR^{l_o} = \frac{|\mathbf{h}'\mathbf{d}|^2}{E[|\mathbf{h}'\mathbf{l}|^2]} = \frac{|\mathbf{h}'\mathbf{d}|^2}{\mathbf{h}'\Sigma_{\mathbf{L}}\mathbf{h}}$$

- The SNR of the output leakage l_o reaches its maximum if and only if SR of that also reaches its maximum
- Impulse response of the optimum linear filter which maximizes the SR of the output signal l_o

$$\mathbf{h}_{opt} = \Sigma_{\mathbf{L}}^{-1}\mathbf{d}$$

- The estimation of $\mathbf{d}$ still requires the correct key

Optimum Linear Filter in Non-profiling DPA

- We introduce *Signal Ratio* (SR) of the output signal l_o:

$$SR^{l_o} = \frac{|\mathbf{h}'\mathbf{d}|^2}{E[|\mathbf{h}'\mathbf{l}|^2]} = \frac{|\mathbf{h}'\mathbf{d}|^2}{\mathbf{h}'\Sigma_{\mathbf{L}}\mathbf{h}}$$

- The SNR of the output leakage l_o reaches its maximum if and only if SR of that also reaches its maximum
- Impulse response of the optimum linear filter which maximizes the SR of the output signal l_o

$$\mathbf{h}_{opt} = \Sigma_{\mathbf{L}}^{-1}\mathbf{d}$$

- The estimation of **d** still requires the correct key

Optimum Linear Filter in Non-profiling DPA (cont.)

- Extension of the conventional leakage model over multiple time instants [1]:
  - Conventional leakage model

$$L_{t^*} = a_{t^*}\Psi(S_{k^*}) + N_{t^*}$$

  - Multivariate leakage model

$$L_t = a_t\Psi(S_{k^*}) + N_t, \qquad t_0 \leq t < t_0 + \tau$$

  - Incorporating algorithmic noise

$$L_t = a_t(\Psi(S_{k^*}) + U + c) + N_t \tag{2}$$
$$= a_t(I + c) + N_t, \qquad t_0 \leq t < t_0 + \tau \tag{3}$$

where $\mathbf{N} = \{N_{t_0}, \cdots, N_{t_0+\tau-1}\}$ has mean vector $\mathbf{0}$

Optimum Linear Filter in Non-profiling DPA (cont.)

- Extension of the conventional leakage model over multiple time instants [1]:
  - Conventional leakage model

$$L_{t^*} = a_{t^*}\Psi(S_{k^*}) + N_{t^*}$$

  - Multivariate leakage model

$$L_t = a_t\Psi(S_{k^*}) + N_t, \qquad t_0 \leq t < t_0 + \tau$$

  - Incorporating algorithmic noise

$$\begin{aligned} L_t &= a_t(\Psi(S_{k^*}) + U + c) + N_t && (2) \\ &= a_t(I + c) + N_t, \qquad t_0 \leq t < t_0 + \tau && (3) \end{aligned}$$

where $\mathbf{N} = \{N_{t_0}, \cdots, N_{t_0+\tau-1}\}$ has mean vector $\mathbf{0}$

Optimum Linear Filter in Non-profiling DPA (cont.)

- Extension of the conventional leakage model over multiple time instants [1]:
  - Conventional leakage model

$$L_{t^*} = a_{t^*}\Psi(S_{k^*}) + N_{t^*}$$

  - Multivariate leakage model

$$L_t = a_t\Psi(S_{k^*}) + N_t, \qquad t_0 \leq t < t_0 + \tau$$

  - Incorporating algorithmic noise

$$\begin{aligned} L_t &= a_t(\Psi(S_{k^*}) + U + c) + N_t && (2) \\ &= a_t(I + c) + N_t, \qquad t_0 \leq t < t_0 + \tau && (3) \end{aligned}$$

where $\mathbf{N} = \{N_{t_0}, \cdots, N_{t_0+\tau-1}\}$ has mean vector $\mathbf{0}$

Optimum Linear Filter in Non-profiling DPA (cont.)

- We limit the attack window to $\{t_0, \cdots, t_0 + \tau - 1\}$
- From Eq. (3), $\mathbf{d} = (i - E[I] + c)\mathbf{a}$ where $\mathbf{a} = \{a_0, \cdots, a_{\tau-1}\}$
- Thus,

$$SR^{I_o} = \frac{|\mathbf{h}'(i - E[I] + c)\mathbf{a}|^2}{\mathbf{h}'\Sigma_{\mathbf{L}}\mathbf{h}} \propto \frac{|\mathbf{h}'\mathbf{a}|^2}{\mathbf{h}'\Sigma_{\mathbf{L}}\mathbf{h}}$$

- Resulting in

$$\mathbf{h}_{opt} = \Sigma_{\mathbf{L}}^{-1}\mathbf{a} \propto \Sigma_{\mathbf{L}}^{-1}\mu_{\mathbf{L}}$$

where $\mu_{\mathbf{L}}$ is the mean vector of leakage $\mathbf{L} = \{L_0, \cdots, L_{\tau-1}\}$ (i.e leakage of the selected window)

Optimum Linear Filter in Non-profiling DPA (cont.)

- We limit the attack window to $\{t_0, \cdots, t_0 + \tau - 1\}$
- From Eq. (3), $\mathbf{d} = (i - E[I] + c)\mathbf{a}$ where $\mathbf{a} = \{a_0, \cdots, a_{\tau-1}\}$

- Thus,

$$SR^{I_o} = \frac{|\mathbf{h}'(i - E[I] + c)\mathbf{a}|^2}{\mathbf{h}'\Sigma_{\mathbf{L}}\mathbf{h}} \propto \frac{|\mathbf{h}'\mathbf{a}|^2}{\mathbf{h}'\Sigma_{\mathbf{L}}\mathbf{h}}$$

- Resulting in

$$\mathbf{h}_{opt} = \Sigma_{\mathbf{L}}^{-1}\mathbf{a} \propto \Sigma_{\mathbf{L}}^{-1}\mu_{\mathbf{L}}$$

where $\mu_{\mathbf{L}}$ is the mean vector of leakage $\mathbf{L} = \{L_0, \cdots, L_{\tau-1}\}$ (i.e leakage of the selected window)

Optimum Linear Filter in Non-profiling DPA (cont.)

- We limit the attack window to $\{t_0, \cdots, t_0 + \tau - 1\}$
- From Eq. (3), $\mathbf{d} = (i - E[I] + c)\mathbf{a}$ where $\mathbf{a} = \{a_0, \cdots, a_{\tau-1}\}$

- Thus,

$$SR^{I_o} = \frac{|\mathbf{h}'(i - E[I] + c)\mathbf{a}|^2}{\mathbf{h}'\Sigma_{\mathbf{L}}\mathbf{h}} \propto \frac{|\mathbf{h}'\mathbf{a}|^2}{\mathbf{h}'\Sigma_{\mathbf{L}}\mathbf{h}}$$

- Resulting in

$$\mathbf{h}_{opt} = \Sigma_{\mathbf{L}}^{-1}\mathbf{a} \propto \Sigma_{\mathbf{L}}^{-1}\mu_{\mathbf{L}}$$

where $\mu_{\mathbf{L}}$ is the mean vector of leakage $\mathbf{L} = \{L_0, \cdots, L_{\tau-1}\}$ (i.e leakage of the selected window)

Optimum Linear Filter in Non-profiling DPA (cont.)

- We limit the attack window to $\{t_0, \cdots, t_0 + \tau - 1\}$
- From Eq. (3), $\mathbf{d} = (i - E[I] + c)\mathbf{a}$ where $\mathbf{a} = \{a_0, \cdots, a_{\tau-1}\}$
- Thus,

$$SR^{I_o} = \frac{|\mathbf{h}'(i - E[I] + c)\mathbf{a}|^2}{\mathbf{h}'\Sigma_{\mathbf{L}}\mathbf{h}} \propto \frac{|\mathbf{h}'\mathbf{a}|^2}{\mathbf{h}'\Sigma_{\mathbf{L}}\mathbf{h}}$$

- Resulting in

$$\mathbf{h}_{opt} = \Sigma_{\mathbf{L}}^{-1}\mathbf{a} \propto \Sigma_{\mathbf{L}}^{-1}\mu_{\mathbf{L}}$$

  where $\mu_{\mathbf{L}}$ is the mean vector of leakage $\mathbf{L} = \{L_0, \cdots, L_{\tau-1}\}$ (i.e leakage of the selected window)

Approximate Optimum Linear Filter in Non-profiling DPA

- Disadvantages of $\mathbf{h}_{opt}$
  - Estimation of $\Sigma_{\mathbf{L}}$ requires large number of power traces
  - Computationally intensive
- Approximation of $\mathbf{h}_{opt}$: $\mathbf{h}_{appr} = diag(\Sigma_{\mathbf{L}})^{-1}\mu_{\mathbf{L}}$ i.e.

$$\mathbf{h}_{appr} = \left\{ \frac{E[L_0]}{\sigma^2_{L_0}}, \dots, \frac{E[L_{\tau-1}]}{\sigma^2_{L_{\tau-1}}} \right\}$$

- The approximate optimum filter $\mathbf{h}_{appr}$ neglects the correlation between the leakages of two different sample points
- When leakages of the different sample points are significantly correlated: perform the attack on a linear transformation of the power traces such as in frequency domain (using FFT), eigenvector domain (using PCA)

Approximate Optimum Linear Filter in Non-profiling DPA

- Disadvantages of $\mathbf{h}_{opt}$
  - Estimation of $\Sigma_{\mathbf{L}}$ requires large number of power traces
  - Computationally intensive
- Approximation of $\mathbf{h}_{opt}$: $\mathbf{h}_{appr} = diag(\Sigma_{\mathbf{L}})^{-1}\mu_{\mathbf{L}}$ i.e.

$$\mathbf{h}_{appr} = \left\{ \frac{E[L_0]}{\sigma^2_{L_0}}, \cdots, \frac{E[L_{\tau-1}]}{\sigma^2_{L_{\tau-1}}} \right\}$$

- The approximate optimum filter $\mathbf{h}_{appr}$ neglects the correlation between the leakages of two different sample points
- When leakages of the different sample points are significantly correlated: perform the attack on a linear transformation of the power traces such as in frequency domain (using FFT), eigenvector domain (using PCA)

Approximate Optimum Linear Filter in Non-profiling DPA

- Disadvantages of $\mathbf{h}_{opt}$
  - Estimation of $\Sigma_{\mathbf{L}}$ requires large number of power traces
  - Computationally intensive
- Approximation of $\mathbf{h}_{opt}$: $\mathbf{h}_{appr} = diag(\Sigma_{\mathbf{L}})^{-1}\mu_{\mathbf{L}}$ i.e.

$$\mathbf{h}_{appr} = \left\{ \frac{E[L_0]}{\sigma^2_{L_0}}, \cdots, \frac{E[L_{\tau-1}]}{\sigma^2_{L_{\tau-1}}} \right\}$$

- The approximate optimum filter $\mathbf{h}_{appr}$ neglects the correlation between the leakages of two different sample points
- When leakages of the different sample points are significantly correlated: perform the attack on a linear transformation of the power traces such as in frequency domain (using FFT), eigenvector domain (using PCA)

Approximate Optimum Linear Filter in Non-profiling DPA

- Disadvantages of $\mathbf{h}_{opt}$
  - Estimation of $\Sigma_{\mathbf{L}}$ requires large number of power traces
  - Computationally intensive
- Approximation of $\mathbf{h}_{opt}$: $\mathbf{h}_{appr} = diag(\Sigma_{\mathbf{L}})^{-1}\mu_{\mathbf{L}}$ i.e.

$$\mathbf{h}_{appr} = \left\{ \frac{E[L_0]}{\sigma^2_{L_0}}, \cdots, \frac{E[L_{\tau-1}]}{\sigma^2_{L_{\tau-1}}} \right\}$$

- The approximate optimum filter $\mathbf{h}_{appr}$ neglects the correlation between the leakages of two different sample points
- When leakages of the different sample points are significantly correlated: perform the attack on a linear transformation of the power traces such as in frequency domain (using FFT), eigenvector domain (using PCA)

Experimental Evaluation

- The performed attacks are:
  - CPA on the unprocessed traces
  - CPA on the output of the Optimum filter (OF)
  - CPA on the output of the Approximate Optimum filter (AOF)
- The attacks are performed in the following domains:
  - Time domain.
  - Frequency domain
  - Eigenvector domain
- Experiments are performed in four scenarios:
  - Scenario (a): on the acquire power traces
  - Scenario (b): by adding high uncorrelated noise
  - Scenario (c): by adding small correlated noise
  - Scenario (d): by adding both the correlated and uncorrelated noise

Experimental Evaluation

- The performed attacks are:
  - CPA on the unprocessed traces
  - CPA on the output of the Optimum filter (OF)
  - CPA on the output of the Approximate Optimum filter (AOF)
- The attacks are performed in the following domains:
  - Time domain.
  - Frequency domain
  - Eigenvector domain
- Experiments are performed in four scenarios:
  - Scenario (a): on the acquire power traces
  - Scenario (b): by adding high uncorrelated noise
  - Scenario (c): by adding small correlated noise
  - Scenario (d): by adding both the correlated and uncorrelated noise

Experimental Evaluation

- The performed attacks are:
  - CPA on the unprocessed traces
  - CPA on the output of the Optimum filter (OF)
  - CPA on the output of the Approximate Optimum filter (AOF)
- The attacks are performed in the following domains:
  - Time domain.
  - Frequency domain
  - Eigenvector domain
- Experiments are performed in four scenarios:
  - Scenario (a): on the acquire power traces
  - Scenario (b): by adding high uncorrelated noise
  - Scenario (c): by adding small correlated noise
  - Scenario (d): by adding both the correlated and uncorrelated noise

Experimental Result: Scenario (a)

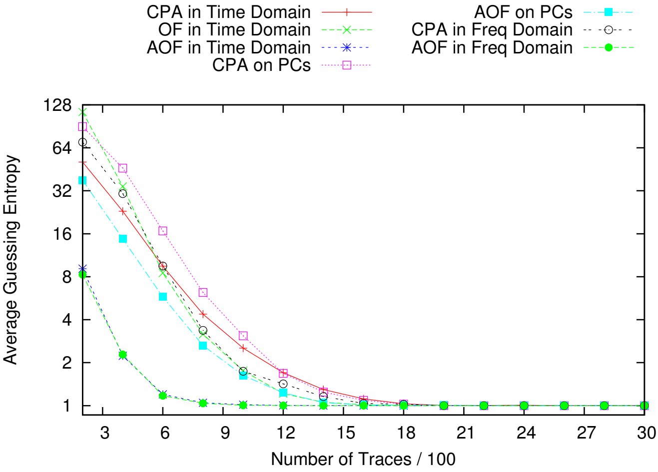

Figure: Results on Acquired Traces of AES Encryption

Experimental Result: Scenario (b)

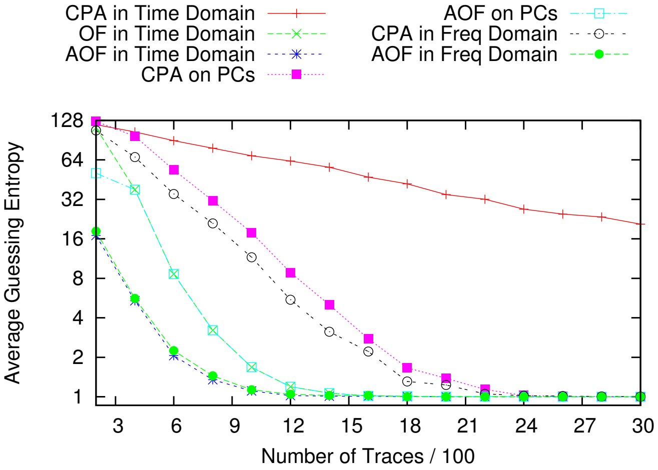

Figure: Results on Acquired Traces adding Uncorrelated Noise

Experimental Result: Scenario (c)

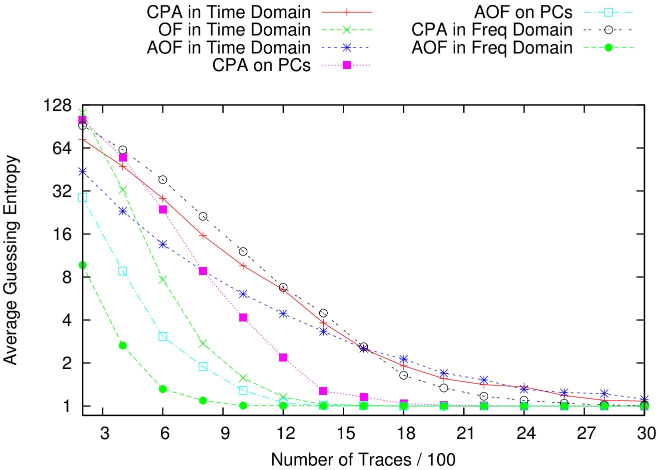

Figure: Results on Acquired Trace adding Correlated Noise

Experimental Result: Scenario (d)

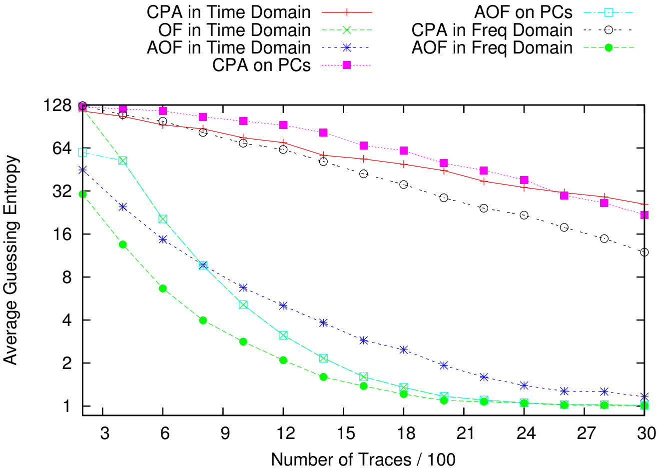

Figure: Results on Acquired Traces adding both the Correlated Noise and Uncorrelated Noise

Comparison with profiling Stochastic attack

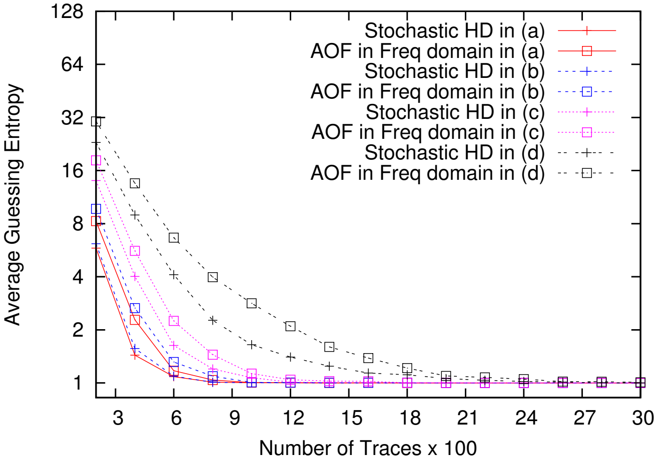

Figure: Results of Profiling Stochastic Attack using HD model and CPA using AOF in Frequency Domain

Summary

- Two linear filters have been proposed for optimal pre-processing in non-profiling DPA
- The experimental results show significant decrease in the average guessing entropy of CPA using the proposed filter
- One proposed filter has been compared with profiling Stochastic attack

Summary

- Two linear filters have been proposed for optimal pre-processing in non-profiling DPA
- The experimental results show significant decrease in the average guessing entropy of CPA using the proposed filter
- One proposed filter has been compared with profiling Stochastic attack

Summary

- Two linear filters have been proposed for optimal pre-processing in non-profiling DPA
- The experimental results show significant decrease in the average guessing entropy of CPA using the proposed filter
- One proposed filter has been compared with profiling Stochastic attack

Thank You!

Bibliography I

S. Hajra and D. Mukhopadhyay.
Pushing the Limit of Non-Profiling DPA using Multivariate Leakage Model.
Cryptology ePrint Archive, Report 2013/849, 2013.
http://eprint.iacr.org/.

D. Oswald and C. Paar.
Improving Side-Channel Analysis with Optimal Linear Transforms.
In S. Mangard, editor, *CARDIS*, volume 7771 of *Lecture Notes in Computer Science*, pages 219–233. Springer, 2012.

J. Sills and E. Kamen.
Time-varying matched filters.
Circuits, Systems and Signal Processing, 15(5):609–630, 1996.

Wikipedia.
Matched filter — Wikipedia, The Free Encyclopedia.
http://en.wikipedia.org/wiki/, 2013.
[Online; accessed 20-December-2013].