TELECOM ParisTech

Institut Mines-Télécom

Template Attacks, Optimal Distinguishers & Perceived Information Metric

Cryptarchi – June 29-30, 2015 – Leuven

Sylvain Guilley*, Annelie Heuser*,
Olivier Rioul* and François-Xavier Standaert**

*Telecom ParisTech, **UCL

Overview

Introduction
- Motivation
- Notations
- Perceived Information

Derivations
- Maximum a posteriori probability
- Maximum Likelihood

Experiments
- Believing or seeing ?

Conclusion

Motivation

- Consolidate state-of-the-art about optimal distinguisher with a deeper look an the probabilities to estimate
- Perceived Information (PI) : information-theoretic metric quantifying the amount of leakage
- Show that PI is related to maximizing the success rate through the *Maximum a posteriori probability*
- Use the maximum likelihood to derive the template attack
- Experiments : If probabilities are known should they be used or estimated on-the-fly ?

Notations

- Secret key k^* deterministic but unknown
- m independent measurements $\mathbf{x} = (x_1, ..., x_m)$ and independent and uniformly distributed inputs $\mathbf{t} = (t_1, ..., t_m)$
- leakage model $\mathbf{y}(k) = \varphi(f(k, \mathbf{t}))$, where φ is a device specific leakage function and f maps the inputs to an intermediate algorithmic state.
- $\mathbf{x} = \mathbf{y}(k^*) + \mathbf{n}$ with independent noise $\mathbf{n}$.
- $\mathbb{P}$ exact probability profiled device
- $\hat{\mathbb{P}}$ for an estimation offline (when profiling)
- $\tilde{\mathbb{P}}$ estimated online on-the-fly (when attacking)

Assumptions

The leakage model follows the

Markov condition

The leakage $\mathbf{x}$ depends on the secret key k only through the computed model y(k). Thus, we have the Markov chain :

$$(k, t) \to y = \varphi(f(t, k)) \to x.$$

This assumption is related to the EIS assumption [SLP05].

Perceived information

Idea [RSVC+11]

- Metric quantifying degraded leakage models
- Generalization of mutual information
- Testing models against each other, e.g., from the true distribution against estimations

Ideal case

- the distribution $\mathbb{P}$ is known
- PI is MI

$$MI(K;X,T) = H(K) + \sum_k \mathbb{P}(k) \sum_t \mathbb{P}(t) \sum_x \mathbb{P}(x|t,k) \log_2 \mathbb{P}(k|t,x)$$

Perceived information

Profiled case

- the distribution is known $\mathbb{P}$
- test a profiled model $\hat{\mathbb{P}}$ against $\mathbb{P}$

$$PI(K;X,T) = H(K) + \sum_k \mathbb{P}(k) \sum_t \mathbb{P}(t) \sum_x \mathbb{P}(x|t,k) \log_2 \hat{\mathbb{P}}(k|t,x)$$

Real case

- the distribution is unknown $\mathbb{P}$
- test a profiled model $\hat{\mathbb{P}}$ against an online estimated model $\tilde{\mathbb{P}}$

$$\hat{PI}(K;X,T) = H(K) + \sum_k \mathbb{P}(k) \sum_t \mathbb{P}(t) \sum_x \tilde{\mathbb{P}}(x|t,k) \log_2 \hat{\mathbb{P}}(k|t,x)$$

Maximum a posteriori probability

MAP

The optimal distinguishing rule is given by the *maximum a posteriori probability (MAP)* rule

$$\mathcal{D}(\mathbf{x}, \mathbf{t}) = \arg\max_{k} \ \mathbb{P}(k|\mathbf{x}, \mathbf{t}).$$

With the help of Bayes...

$$\mathbb{P}(k|\mathbf{x}, \mathbf{t}) = \frac{\mathbb{P}(\mathbf{x}|k, \mathbf{t}) \cdot \mathbb{P}(k)}{\mathbb{P}(\mathbf{x}|\mathbf{t})} = \frac{\mathbb{P}(\mathbf{x}|k, \mathbf{t}) \cdot \mathbb{P}(k)}{\sum_k \mathbb{P}(k)\mathbb{P}(\mathbf{x}|\mathbf{t}, k)}.$$

Relation between MAP and PI

Let $\mathbb{P}$ be any distribution such that $\mathbb{P}(k|\mathbf{x},\mathbf{t}) \propto \prod_{i=1}^{m} \mathbb{P}(k|x_i,t_i)$. We start by maximizing MAP :

$$\begin{aligned}\arg\max_k \ \hat{\mathbb{P}}(k|\mathbf{x},\mathbf{t}) &= \arg\max_k \ \prod_{i=1}^{m} \hat{\mathbb{P}}(k|x_i,t_i) \\ &= \arg\max_k \ \prod_{x,t} \hat{\mathbb{P}}(k|x,t)^{m\tilde{\mathbb{P}}_k(x,t)},\end{aligned}$$

where $\tilde{\mathbb{P}}_k(x,t) = \tilde{\mathbb{P}}(x,t|k)$ is the "counting" estimation (online) of x and t that depends on k. Now talking the log_2 gives

$$= \arg\max_k \ \sum_{x,t} \tilde{\mathbb{P}}_k(x,t) \log_2 \hat{\mathbb{P}}(k|x,t)$$

Relation between MAP and PI (cont'd)

$$
\begin{aligned}
&= \arg\max_k \sum_{x,t} \tilde{\mathbb{P}}_k(x,t) \log_2 \hat{\mathbb{P}}(k|x,t) \\
&= \arg\max_k \sum_{x,t} \tilde{\mathbb{P}}(x,t|k) \log_2 \hat{\mathbb{P}}(k|x,t) \\
&= \arg\max_k \sum_{t} \tilde{\mathbb{P}}(t) \sum_{x} \tilde{\mathbb{P}}(x|t,k) \log_2 \hat{\mathbb{P}}(k|x,t)
\end{aligned}
$$

Taking the average over k and adding $H(K)$ gives $\hat{P}I(K;X,T)$

$$H(K) + \sum_k \mathbb{P}(k) \sum_t \tilde{\mathbb{P}}(t) \sum_x \tilde{\mathbb{P}}(x|t,k) \log_2 \hat{\mathbb{P}}(k|x,t).$$

(except $\tilde{\mathbb{P}}(t)$ vs. $\mathbb{P}(t)$)

Relation between MAP and PI (cont'd)

PI $\Leftrightarrow$ MAP

$\hat{P}I$ is the expectation of the MAP over the keys.

Profiled case

If we have an infinite number of traces to estimate $\tilde{\mathbb{P}} \rightarrow \mathbb{P}$ then we recover PI(K ;X,T).

Ideal case

If we have an infinite number of traces to estimate $\tilde{\mathbb{P}} \rightarrow \mathbb{P}$ and $\hat{\mathbb{P}} \rightarrow \mathbb{P}$ then we recover MI(K ;X,T).

Maximum Likelihood Attack

Maximum Likelihood Attack

Assuming we have $y(k) = \varphi(f(t,k))$ that follows the Markov condition, then the optimal distinguishing rule is given by the maximum likelihood (ML) rule

$$\mathcal{D}(\mathbf{x}, \mathbf{t}) = \arg\max_{k} \ \mathbb{P}(\mathbf{x}|\mathbf{y}).$$

In practise...

- $\mathbb{P}$ is most likely not known perfectly by the attacker
- either estimated offline by $\hat{\mathbb{P}}$
- or online on-the-fly $\tilde{\mathbb{P}}$

Maximum Likelihood Attack

Similarly, as in the previous derivation we have

$$\arg\max_k \; \mathbb{P}(\mathbf{x}|\mathbf{y}) = \prod_{i=1}^{m} \mathbb{P}(x_i|y_i) = \prod_{x,y} \mathbb{P}(x|y)^{m\tilde{\mathbb{P}}(x,y)}.$$

Taking the $\log_2$ gives us

$$\sum_{x,y} \tilde{\mathbb{P}}(x,y) \log_2 \mathbb{P}(x|y)$$

Now we add the cross entropy term that does not depend on a key guess k

$$-\sum_{x,y} \tilde{\mathbb{P}}(x,y) \log_2 \mathbb{P}(x)$$

Maximum Likelihood Attack

This results to

$$\arg\max_k \ \tilde{\mathbb{P}}(x,y)\log_2 \frac{\mathbb{P}(y|x)}{\mathbb{P}(y)}.$$

Profiled

$\mathbb{P}$ is estimated offline $\hat{\mathbb{P}}$ on a training device

$$\arg\max_k \ \tilde{\mathbb{P}}(x,y)\log_2 \frac{\hat{\mathbb{P}}(y|x)}{\hat{\mathbb{P}}(y)},$$

which is the *template attack*.

Maximum Likelihood Attack

Non-Profiled

$\mathbb{P}$ is estimated online $\tilde{\mathbb{P}}$ on a the device under attack

$$\arg\max_k \; \tilde{\mathbb{P}}(x,y)\log_2\frac{\tilde{\mathbb{P}}(y|x)}{\tilde{\mathbb{P}}(y)},$$

which gives the Mutual Information Analysis [GBTP08].

Believing or seeing ?

Should probabilities considered as precise as possible ?

- Many recent works (e.g., [VCS09]) showed that using kernel estimation is more efficient than using histograms
- Accordingly, if $\mathbb{P}(Y)$ is known, should it be used instead of $\tilde{P}(Y)$ and $\hat{\mathbb{P}}(Y)$?

Believing or seeing ?

Simple scenario

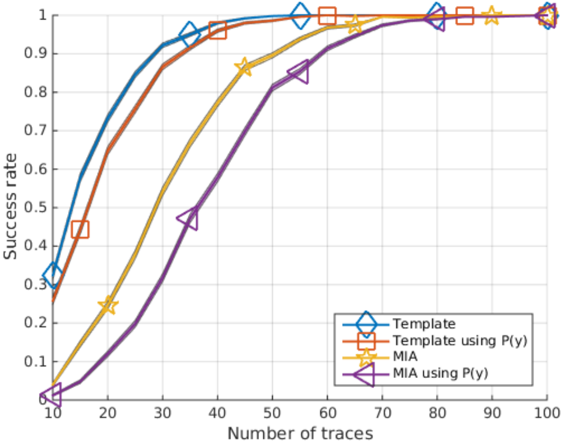
$$X = Y(k^*) + N,$$
$$Y(k) = HW(Sbox(T \oplus k))$$

As Y follows a binomial distribution with parameters $(n, 1/2)$, we have

$$\mathbb{P}(Y) = \{1/256, 8/256, 28/256, 56/256, 28/256, 8/256, 1/256\}.$$

- Template attack : replace $\tilde{\mathbb{P}}(Y)$ and $\hat{\mathbb{P}}(Y)$ by $\mathbb{P}(Y)$
- MIA : replace : $\tilde{\mathbb{P}}(Y)$ by $\mathbb{P}(Y)$

Believing or seeing ?



Conclusion

- $\hat{P}I(K;X,T)$ is the expectation of the MAP over the keys
- Maximum likelihood to recover
  - template attack when probabilities are estimated offline $(\hat{\mathbb{P}})$
  - MIA when probabilities are estimated online on-the-fly $(\tilde{\mathbb{P}})$
- In the attack phase : probabilities should be estimated instead of using the true distributions

References I

Benedikt Gierlichs, Lejla Batina, Pim Tuyls, and Bart Preneel.
Mutual information analysis.
In *CHES, 10th International Workshop*, volume 5154 of *Lecture Notes in Computer Science*, pages 426–442. Springer, August 10-13 2008.
Washington, D.C., USA.

Mathieu Renauld, François-Xavier Standaert, Nicolas Veyrat-Charvillon, Dina Kamel, and Denis Flandre.
A Formal Study of Power Variability Issues and Side-Channel Attacks for Nanoscale Devices.
In *EUROCRYPT*, volume 6632 of *LNCS*, pages 109–128. Springer, May 2011.

References II

Tallinn, Estonia.

- Werner Schindler, Kerstin Lemke, and Christof Paar.
A Stochastic Model for Differential Side Channel Cryptanalysis.
In LNCS, editor, *CHES*, volume 3659 of *LNCS*, pages 30–46. Springer, Sept 2005.
Edinburgh, Scotland, UK.

- Nicolas Veyrat-Charvillon and François-Xavier Standaert.
Mutual Information Analysis : How, When and Why ?
In *CHES*, volume 5747 of *LNCS*, pages 429–443. Springer, September 6-9 2009.
Lausanne, Switzerland.