Robust PUF based Authentication

Andrea Grigorescu[1], Holger Boche[1] and Rafael F. Schaefer[2]

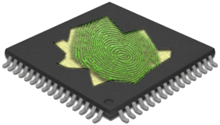
[1]Lehrstuhl für Theoretische Informationstechnik, Technische Universität München, 80333 München, Germany

[2]Department of Electrical Engineering, Princeton University, Princeton, NJ 08544, USA

Lehrstuhl für Nachrichtentechnik
Technische Universität Dresden
Dresden, September 22, 2015

Motivation

- Physical Unclonable Functions (***PUFs***): functions that use the production variability to generate device-specific data $\Rightarrow$ fingerprint of device
- PUF are used for ***device authentication***
- Security on higher layers is usually based on the assumption of insufficient computational capabilities of non-legitimate receivers $\Rightarrow$ use of ***information theoretic secrecy concepts***
- Practical systems often suffer from uncertainty in source state information $\Rightarrow$ ***compound sources***



Physical Unclonable Functions[1]

PUFs consist of:

- Input signal: ***Challenge***
- Output signal: ***Response***

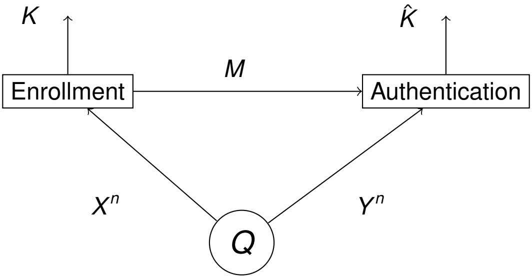
PUF based authentication

- Enrollment Phase
  - Gather a number of challenge response pairs (CRPs)
  - Store the CRPs in a CRPs database together with ID
- Authentication phase
  - Claim ID
  - Apply a challenge from the CRP data base
  - Compare the response made by the PUF with the one stored.

[1] C. Böhm and M. Hofer: Physical Unclonable Functions in Theory and Practice, Springer Science Business Media 2014.

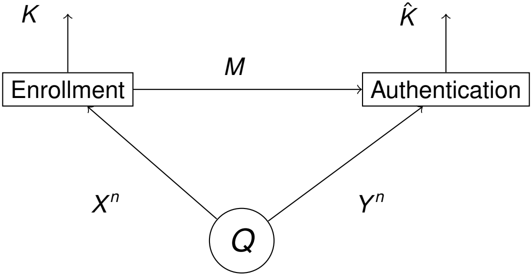
Authentication Model

- $\mathcal{X}$ and $\mathcal{Y}$ finite.
- Discrete memoryless source: $Q \in \mathcal{P}(\mathcal{X} \times \mathcal{Y})$
- Enrollment sequence: $x^n \in \mathcal{X}^n$
- Authentication sequence: $y^n \in \mathcal{Y}^n$



Protocol

- Enrollment Phase
  - Observe X^n at the enrollment terminal
  - Generate secret key K and helper data M
  - Apply one way function f to K
  - Store M, $f(K)$ and f in a public data base
- Authentication Phase
  - Observe Y^n and M at the authentication terminal
  - Calculate key estimate $\hat{K}$
  - Apply one way function f to $\hat{K}$
  - **IF** $f(K) = f(\hat{K})$ **THEN** authentication successful



Attention!

- M may reveal information about $K \rightarrow \frac{1}{n} I(K; M)$
- M may reveal too much information about $X^n \rightarrow \frac{1}{n} I(X^n; M)$

- Block-processing of fixed length n large enough.
- Helper data set: $\mathcal{M} := \{1, \dots, M_n\}$
- Secret key set: $\mathcal{K} := \{1, \dots, K_n\}$

Definition

An (n, K_n, M_n)-code for authentication of the joint source $Q \in \mathcal{P}(\mathcal{X} \times \mathcal{Y})$ consists of an encoder f at the enrollment terminal with

$$f : \mathcal{X}^n \to \mathcal{K} \times \mathcal{M}$$

and a decoder φ at the authentication terminal

$$\varphi : \mathcal{Y}^n \times \mathcal{M} \to \mathcal{K}$$

An achievable secrecy privacy rate pair

Definition

A secrecy privacy rate pair $(R_K, R_M) \in \mathbb{R}_+^2$ *is called* ***achievable*** *for a joint source Q, if for any* $\delta > 0$ *there exist an* $n(\delta) \in \mathbb{N}$ *and a sequence of* (n, K_n, M_n)*-codes such that for all* $n \geq n(\delta)$ *we have*

$$\Pr\{\hat{K} \neq K\} \leq \delta$$

$$\frac{1}{n}H(K) + \delta \geq \frac{1}{n}\log K_n \geq R_K - \delta$$

$$\frac{1}{n}I(K; M) \leq \delta$$

$$\frac{1}{n}I(X^n; M) \leq R_M + \delta$$

Secrecy Privacy Capacity Region[2,3]

For some U with alphabet $|\mathcal{U}| \leq |\mathcal{X}| + 1$ and $V\colon \mathcal{X} \to \mathcal{P}(\mathcal{U})$, we define the region $\mathcal{R}(Q, V)$ as the set of all $(R_K, R_M) \in \mathbb{R}_+^2$ satisfying

$$R_K \leq I(U; Y)$$
$$R_M \geq I(U; X) - I(U; Y)$$

with $P_{UXY}(u, x, y) = V(u|x)Q(x, y)$

Theorem

The set of all achievable secrecy privacy rate pairs for the joint source $Q \in \mathcal{P}(\mathcal{X} \times \mathcal{Y})$ is called secrecy privacy capacity region and is given by

$$\mathcal{C}(Q) = \bigcup_{V:\mathcal{X}\to\mathcal{P}(\mathcal{U})} \mathcal{R}(Q, V)$$

[2] L. Lai, S. Ho and H.V. Poor: Privacy–Security Trade-Offs in Biometric Security Systems—Part I: Single Use Case, IEEE Trans IFS 2010.

[3] T. Ignatenko and F. Willems: Biometric systems: Privacy and secrecy aspects, IEEE Trans IFS 2009.

Question

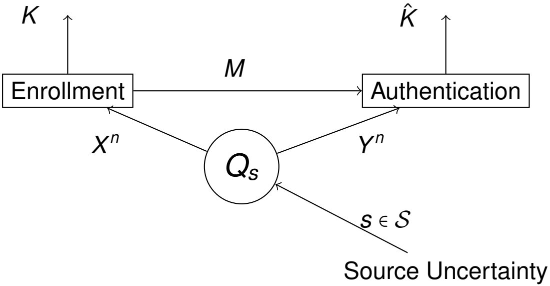
What happens when we have source uncertainty? Can we still authenticate securely?

- Let $\mathcal{S}$ be a finite state set
- Discrete memoryless joint source
  $Q_s^n(x^n, y^n) \coloneqq \prod_{i=1}^n Q_s(x_i, y_i) = \prod_{i=1}^n p_s(x_i) W_s(y_i|x_i)$ with $s \in \mathcal{S}$, $p_s \in \mathcal{P}(\mathcal{X})$ and $W_s\colon \mathcal{X} \to \mathcal{P}(\mathcal{Y})$

Definition

The discrete memoryless compound joint source $\mathfrak{Q}_{\mathcal{X}\mathcal{Y}}$ is given by the family of joint probability distributions on $\mathcal{X} \times \mathcal{Y}$ as

$$\mathfrak{Q}_{\mathcal{X}\mathcal{Y}} \coloneqq \{Q_s \in \mathcal{P}(\mathcal{X} \times \mathcal{Y})\colon s \in \mathcal{S}\}$$



A subset representation for compound sources

- Unique marginal distributions over $\mathcal{X}$
  $\mathfrak{Q}_{\mathcal{X}} := \left\{p_s \in \mathcal{P}(\mathcal{X}) \colon s \in \mathcal{S} \;\; p_s(x) = \sum_{y \in \mathcal{Y}} Q_s(x,y) \;\text{ for every } x \in \mathcal{X}\right\}$
- Index of unique marginal distributions over $\mathcal{X}$
  $\mathcal{L} := \{\ell \colon p_\ell \in \mathfrak{Q}_{\mathcal{X}}\}$
- Sources with same marginal distribution over $\mathcal{X}$
  $\mathfrak{Q}_{\mathcal{X}\mathcal{Y},\ell} := \left\{Q_s \in \mathfrak{Q}_{\mathcal{X}\mathcal{Y}} : Q_s(x,y) = p_\ell(x) W_s(y|x) \;\text{ for every } (x,y) \in \mathcal{X} \times \mathcal{Y}\right\}$
- Index of sources with same marginal distribution over $\mathcal{X}$
  $\mathcal{S}_\ell := \{s \in \mathcal{S} \colon Q_s \in \mathfrak{Q}_{\mathcal{X}\mathcal{Y},\ell}\}$

An achievable secrecy privacy rate pair

Definition

A secrecy privacy rate pair $(R_K, R_M) \in \mathbb{R}_+^2$ *is called* ***achievable*** *for the compound joint source* $\mathfrak{Q}_{\mathcal{X}\mathcal{Y}}$*, if for any* $\delta > 0$ *there exist an* $n(\delta) \in \mathbb{N}$ *and a sequence of* (n, K_n, M_n)*-codes such that for all* $n \geq n(\delta)$ *and for every* $s \in \mathcal{S}$ *we have*

$$\Pr\{\hat{K} \neq K \| Q_s \in \mathfrak{Q}_{\mathcal{X}\mathcal{Y}}\} \leq \delta$$

$$\frac{1}{n} H(K \| Q_s \in \mathfrak{Q}_{\mathcal{X}\mathcal{Y}}) + \delta \geq \frac{1}{n} \log K_n \geq R_K - \delta$$

$$\frac{1}{n} I(K; M \| Q_s \in \mathfrak{Q}_{\mathcal{X}\mathcal{Y}}) \leq \delta$$

$$\frac{1}{n} I(X^n; M \| Q_s \in \mathfrak{Q}_{\mathcal{X}\mathcal{Y}}) \leq R_M + \delta$$

An Achievable Rate Region[4]

- Compound joint source $\mathfrak{Q}_{\mathcal{X}\mathcal{Y}}$
- Fixed $\ell \in \mathcal{L}, V : \mathcal{X} \to \mathcal{P}(\mathcal{U})$ and for every $s \in \mathcal{S}_\ell$
- $\mathcal{R}(V, \ell, s)$ set of all $(R_K, R_M) \in \mathbb{R}_+^2$ such that

$$\begin{aligned} R_K &\leq I(U; Y \| Q_s \in \mathfrak{Q}_{\mathcal{X}\mathcal{Y},\ell}) \\ R_M &\geq I(U; X | L = \ell \| Q_s \in \mathfrak{Q}_{\mathcal{X}\mathcal{Y},\ell}) - I(U; Y \| Q_s \in \mathfrak{Q}_{\mathcal{X}\mathcal{Y},\ell}) \end{aligned}$$

with $P_{UXY,s}(u, x, y) = V(u|x) Q_s(x, y)$.

Theorem

A secrecy privacy achievable rate region for the compound joint source $\mathfrak{Q}_{\mathcal{X}\mathcal{Y}}$ is given by $\mathcal{C}(\mathfrak{Q}_{\mathcal{X}\mathcal{Y}})$

$$\mathcal{C}(\mathfrak{Q}_{\mathcal{X}\mathcal{Y}}) = \bigcap_{\ell \in \mathcal{L}} \bigcup_{V : \mathcal{X} \to \mathcal{P}(\mathcal{U})} \bigcap_{s \in \mathcal{S}_\ell} \mathcal{R}(V, \ell, s).$$

[4] A. Grigorescu, H. Boche and R. Schaefer: Robust PUF based Authentication, WIFS 2015.

Sketch of proof

- At the enrollment terminal, having observed X^n, the index of the marginal distribution $p_\ell \in \mathcal{P}(\mathcal{X})$ is computed
- Compute the key K and the psudo-helper data M' based on X^n and the index of the marginal distribution L
- Store the helper data $M = M'L$ in the public database
- Estimate the key $\hat{K}$ at the authentication terminal, based on the observations M and Y^n

Marginal distribution estimation

- For every $\ell, \ell' \in \mathcal{L}$ define $\delta_\ell = \frac{1}{2} \min_{\ell' \neq \ell} \| p_\ell - p_{\ell'} \|_{TV}$
- Choose $0 < \delta < \min_{\ell \in \mathcal{L}} \delta_\ell$ and consider $\mathcal{T}^n_{p_\ell, \delta}$. for every $\ell, \ell' \in \mathcal{L}$ with $\ell' \neq \ell$ we have that $\mathcal{T}^n_{p_{\ell'}, \delta} \cap \mathcal{T}^n_{p_\ell, \delta} = \varnothing$
- Error: If x^n was generated by the source p_ℓ, however $x^n \notin \mathcal{T}^n_{p_\ell, \delta}$
- Probability of error: $p_\ell([\mathcal{T}^n_{p_\ell, \delta}]^c) \leq \epsilon_\delta(n, |\mathcal{X}|)$

Random coding
For a fixed $\ell \in \mathcal{L}$

- Code construction: Generate $2^{n(R_K+R_M)}$ codewords $U^n_{k,m}$ with $k \in \mathcal{K} := \{1, \dots, 2^{nR_K}\}$ and $m \in \mathcal{M} := \{1, \dots, 2^{nR_M}\}$ by choosing each symbol independently at random according to $p_u \in \mathcal{P}(\mathcal{U})$. Codebook $U = \{U^n_{k,m}\}_{(k,m)\in\mathcal{K}\times\mathcal{M}}$
- For every $s \in \mathcal{S}_\ell$ we define following channels $\Sigma_{\mathcal{X}_\ell}:\mathcal{U} \to \mathcal{P}(\mathcal{X}), \Sigma_{\mathcal{Y}_s}:\mathcal{U} \to \mathcal{P}(\mathcal{Y})$ and $\Sigma_{\mathcal{X}\mathcal{Y}_s}:\mathcal{U} \to \mathcal{P}(\mathcal{X} \times \mathcal{Y})$ that satisfy

$$\Sigma_{\mathcal{X}_\ell}(x|u) = \frac{p_\ell(x)V(u|x)}{\sum_{x\in\mathcal{X}} p_\ell(x)V(u|x)}$$

$$\Sigma_{\mathcal{Y}_s}(y|u) = \frac{\sum_{x\in\mathcal{X}} V(u|x)Q_s(x,y)}{\sum_{(x,y)\in\mathcal{X}\times\mathcal{Y}} V(u|x)Q_s(x,y)}$$

$$\Sigma_{\mathcal{X}\mathcal{Y}_s}(x,y|u) = \frac{V(u|x)Q_s(x,y)}{\sum_{(x,y)\in\mathcal{X}\times\mathcal{Y}} V(u|x)Q_s(x,y)}$$

for every $(u,x,y) \in \mathcal{U} \times \mathcal{X} \times \mathcal{Y}$

Encoder and decoder Sets

For every $(k, m, \ell) \in \mathcal{K} \times \mathcal{M} \times \mathcal{L}$

- Encoder set: $\mathcal{E}_{k,m,\ell}(U) = \mathcal{T}^n_{\Sigma_{\mathcal{X}_\ell},\delta'}(U^n_{k,m})$
- Decoder set:

$$\mathcal{D}'_k(m(U),\ell) := \bigcup_{s\in\mathcal{S}_\ell} \mathcal{T}^n_{\Sigma_{\mathcal{Y}_s},\delta''}(U^n_{k,m})$$

$$\mathcal{D}_k(m(U),\ell) := \mathcal{D}'_k(m(U),\ell) \cap \Big(\bigcup_{\substack{k'\neq k\\ k'\in\mathcal{K}}} \mathcal{D}'_{k'}(m(U),\ell) \Big)^c$$

- Encoder-decoder pair set:
  $\mathcal{C}_{k,m,\ell}(U) := (\mathcal{E}_{k,m,\ell}(U) \times \mathcal{D}_k(m(U),\ell)) \cap \Big(\bigcup_{s\in\mathcal{S}_\ell} \mathcal{T}^n_{\Sigma_{\mathcal{X}\mathcal{Y}_s},\tilde{\delta}}(U^n_{k,m}) \Big)$

Error Analysis

For a fixed $\ell \in \mathcal{L}$

- Encoder: $\epsilon_{E,n}(U) = p_\ell^n\Big(\big(\bigcup_{(k,m)\in\mathcal{K}\times\mathcal{M}} \mathcal{E}_{k,m,\ell}(U)\big)^c\Big)$

$$\mathbb{E}_U(\epsilon_{E,n}(U)) \leq \exp\Big(-(n+1)^{-|\mathcal{U}||\mathcal{X}|}\Big)\exp\Big(2^{n(R_K+R_M-I(U;X|L=\ell\|Q_s)-\psi(\delta',|\mathcal{U}||\mathcal{X}|))}\Big)$$

$\Rightarrow R_K + R_M > I(U;X|L=\ell\|Q_s) + \psi(\delta',|\mathcal{U}|,|\mathcal{X}|)$

- Decoder: For some $t \in \mathcal{S}_\ell$ and $k \in \mathcal{K}$ we have

$$\epsilon_{n,k}^t(U) = \Sigma^n_{\mathcal{X}\mathcal{Y}_t}(\mathcal{C}_{\mathcal{E}_{k,m,\ell}}(U)^c|U^n_{k,m})$$

$$\mathbb{E}_U(\epsilon^t_{n,k}(U)|U^n_{k,m}) \leq |\mathcal{S}_\ell|2^{-n(\min_{s\in\mathcal{S}_\ell} I(U;Y\|Q_s)-R_K-\phi(\delta'',|\mathcal{U}|,|\mathcal{Y}|))}$$

$\Rightarrow R_K < I(U;Y\|Q_s) - \phi(\delta'',|\mathcal{U}|,|\mathcal{Y}|)$

$\Rightarrow R_M > I(U;X|L=\ell\|Q_s) - I(U;Y\|Q_s) + \phi(\delta'',|\mathcal{U}|,|\mathcal{Y}|) + \psi(\delta',|\mathcal{U}|,|\mathcal{X}|)$

Sketch of Proof

Conditions

- *Key Distribution*:

$$\left|\frac{1}{n}H(K\|Q_s \in \mathfrak{Q}_{\mathcal{X}\mathcal{Y},\ell}) - I(U;Y\|Q_s \in \mathfrak{Q}_{\mathcal{X}\mathcal{Y},\ell})\right|$$
$$\leq \frac{2\log|\mathcal{L}|}{n} + \epsilon_\delta(n,|\mathcal{X}|)\log|\mathcal{X}| + \phi(\delta,''|\mathcal{U}|,|\mathcal{Y}|) + \psi(\delta',|\mathcal{U}|,|\mathcal{X}|)$$

- *Privacy Leakage*:

$$\frac{1}{n}I(X^n;M'L\|Q_s \in \mathfrak{Q}_{\mathcal{X}\mathcal{Y},\ell})$$
$$\leq I(U;X|L=\ell\|Q_s \in \mathfrak{Q}_{\mathcal{X}\mathcal{Y},\ell}) - I(U;Y\|Q_s \in \mathfrak{Q}_{\mathcal{X}\mathcal{Y},\ell})$$
$$+ \frac{\log|\mathcal{L}|}{n} + \gamma_{n,\ell} + \epsilon_\delta(n,|\mathcal{X}|)\log|\mathcal{X}|$$

Conditions

- *Secrecy Leakage*:

$$\frac{1}{n} I(K; M'L \| Q_s \in \mathfrak{Q}_{\mathcal{X}\mathcal{Y},\ell}) \leq \frac{\log|\mathcal{L}|}{n} + \epsilon_\delta(n, |\mathcal{X}|) \log|\mathcal{X}| + \lambda_{n,\ell} + \frac{1}{n}$$

Capacity region[5]

Theorem

*The **secrecy privacy capacity region** for the compound joint source $\mathfrak{Q}_{\mathcal{X}\mathcal{Y}}$ is given by $\mathcal{C}(\mathfrak{Q}_{\mathcal{X}\mathcal{Y}})$*

$$\mathcal{C}(\mathfrak{Q}_{\mathcal{X}\mathcal{Y}}) = \bigcap_{\ell\in\mathcal{L}} \bigcup_{V:\mathcal{X}\to\mathcal{P}(\mathcal{U})} \bigcap_{s\in\mathcal{S}_\ell} \mathcal{R}(V,\ell,s).$$

[5] A. Grigorescu, H. Boche and R. Schaefer: Robust PUF based Authentication, WIFS 2015.

Converse

For a fixed $\ell \in \mathcal{L}$, $s \in \mathcal{S}_\ell$ and $V\colon \mathcal{X} \to \mathcal{P}(\mathcal{U})$ it holds

- $R_K - \delta \leq I(U; Y, L = \ell \| Q_s \in \mathfrak{Q}_{\mathcal{X}\mathcal{Y},\ell}) + \lambda_{n,\ell} + \frac{1}{n} + \frac{1+\delta \log K_n}{n}$
- $R_M + \delta \geq I(U; X|L = \ell \| Q_s \in \mathfrak{Q}_{\mathcal{X}\mathcal{Y},\ell}) - I(U; Y|L = \ell \| Q_s \in \mathfrak{Q}_{\mathcal{X}\mathcal{Y},\ell}) + \frac{1+\delta \log K_n}{n}$
- Assume $(R_K^*, R_M^*) \notin \bigcap_{\ell \in \mathcal{L}} \mathcal{C}_\ell$
  $\Rightarrow$ there exists a $\ell \in \mathcal{L}$ such that for all auxiliary channel V we have that $(R_K^*, R_M^*) \notin \mathcal{R}(V, \ell)$
  $\Rightarrow (R_K^*, R_M^*) \notin \mathcal{C}(\mathfrak{Q}_{\mathcal{X}\mathcal{Y}})$

Conclusion

Take away

- Robust authentication at ***positive key rates*** is **possible**!

Future Work

- Extend the model to compound sources with infinite alphabets

Thanks for Your Attention!