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

WIFS 2015

Rome, November 18th, 2015

Motivation

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

Physical Unclonable Functions[1]

PUFs consist of:

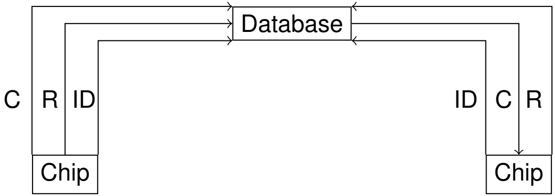
- Input signal: ***Challenge***
- Output signal: ***Response***

$$\text{Challenge} \longrightarrow \boxed{\text{Chip}} \longrightarrow \text{Response}$$

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

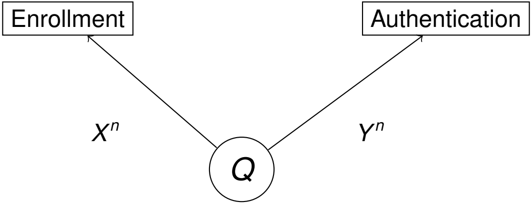
PUF based authentication

- 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.



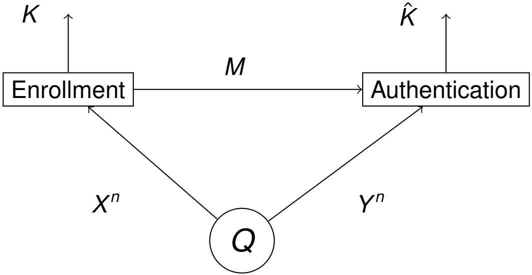
Authentication Model

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

- Helper data M is public and can easily be eavesdropped upon
- 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: $\mathcal{M} \coloneqq \{1, \ldots, M_n\}$
- Secret key set: $\mathcal{K} \coloneqq \{1, \ldots, K_n\}$

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

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

and a decoder φ at the authentication terminal

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

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.

Compound Sources

Question

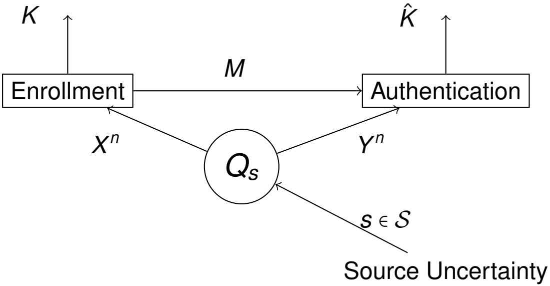
- What happens when we have source uncertainty?
- Can we still authenticate securely at positive rates?
- What is the secrecy privacy capacity of the system?

- Let $\mathcal{S}$ be a finite state set
- Discrete memoryless joint source $Q_s^n(x^n, y^n) := \prod_{i=1}^n Q_s(x_i, y_i) = \prod_{i=1}^n p_s(x_i) W_s(y_i|x_i)$ 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 $\mathfrak{Q}_{\mathcal{XY}}$ is given by the family of joint probability distributions on $\mathcal{X} \times \mathcal{Y}$ as

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



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*

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

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

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

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

A subset representation for compound sources

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

Secrecy Privacy Capacity Region

- 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

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

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

Theorem

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

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

Marginal distribution estimation $p_\ell \in \mathcal{P}(\mathcal{X})$

- 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 $\mathcal{T}^n_{p_{\ell'},\delta} \cap \mathcal{T}^n_{p_\ell,\delta} = \emptyset$
- 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

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

Sketch of Proof

Error Analysis

- Encoder: $\mathbb{E}_U(\epsilon_{E,n}(U)) = \mathbb{E}_U(p_\ell^n((\bigcup_{(k,m)\in\mathcal{K}\times\mathcal{M}} \mathcal{E}_{k,m,\ell}(U))^c)) \to 0$ for $n \to \infty$ and

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

- Decoder: For some $t \in \mathcal{S}_\ell$ we have $\mathbb{E}_U(\epsilon_{n,k}^t(U)) = \mathbb{E}_U(\Sigma_{\mathcal{X}\mathcal{Y}_t}^n(\mathcal{C}_{\mathcal{E}_{k,m,\ell}}(U)^c|U_{k,m}^n)) \to 0$ for $n \to \infty$ and

$$R_K < \min_{s\in\mathcal{S}_\ell} I(U;Y\|Q_s) - \phi(\delta'', |\mathcal{U}|, |\mathcal{Y}|)$$

$\Rightarrow R_K < \min_{s\in\mathcal{S}_\ell} I(U;Y\|Q_s) - \phi(\delta'', |\mathcal{U}|, |\mathcal{Y}|)$
$\Rightarrow R_M > I(U;X|L=\ell\|Q_s) - I(U;Y\|Q_s) + \phi(\delta'', |\mathcal{U}|, |\mathcal{Y}|) + \psi(\delta', |\mathcal{U}|, |\mathcal{X}|)$

Conclusion

Take away

- Robust authentication at ***positive key rates*** is **possible**!
- We established a single letter characterization of the capacity!

Future Work

- Extend the model to compound sources with infinite alphabets

Thanks for Your Attention!