Physical Unclonable Functions (PUFs): Signal Processing and Information-Theoretic Aspects

Onur Günlü

Information Coding Division (ICG), Electrical Engineering Department,
Linköping University, Sweden

Workshop on Random Number Generators and PUFs, November 2024

Outline

- **Part I**: Signal Processing for PUFs with Security Guarantees
- **Part II**: Optimal Error-Correcting Code Designs for PUFs

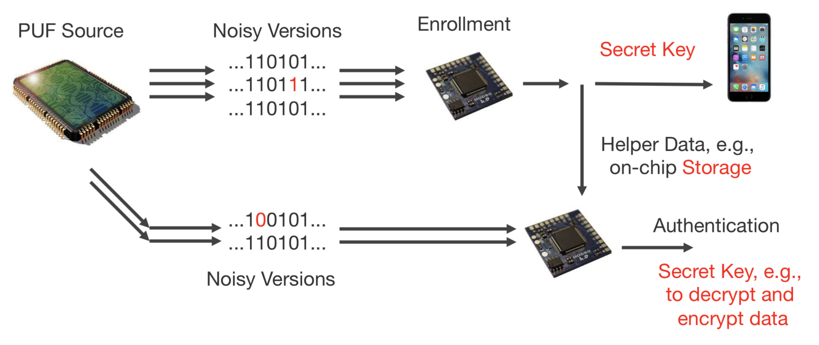
Part I

- **Signal Processing for PUFs with Security Guarantees**

Motivations for PUFs

Digital Secrecy and Privacy Example

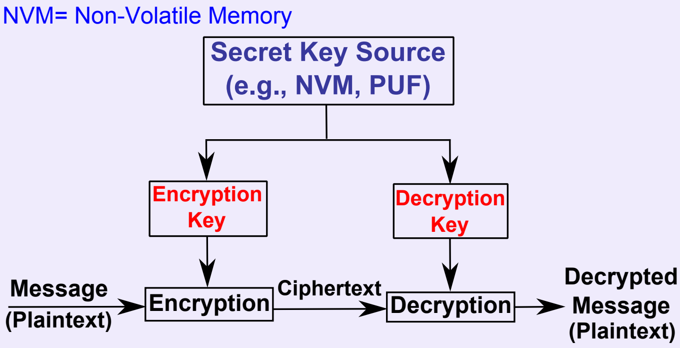
- Digital devices have to be protected/secured/authenticated/identified, similar to individuals, to provide security for Things and their Internet (in order to protect device owners and businesses):
  $\Rightarrow$ Hardware "Fingerprint" via a PUF



Motivations for PUFs II

Digital Secrecy and Privacy Example II

- **Encryption/Decryption with PUFs**



Motivations for PUFs III

Other Applications of PUFs

- **6G mobile devices that use SRAM outputs**, available in mobile devices, as a PUF to extract secret keys;
- A **PUF in a USB token to encrypt user data** before uploading it to the cloud;
- System developers want to **mutually authenticate an FPGA chip and the IP components** in the chip, while IP developers want to **protect the IP**. One symmetric cipher and one PUF can achieve these.

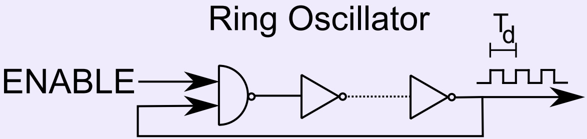
A Brief Definition of PUF

- A PUF is a challenge-response-mapping embodied by a physical device (e.g., digital circuit outputs) such that it is
  - **easy and fast** for the physical device **to evaluate** the PUF response;
  - **hard** for an attacker **to determine the PUF response** to a randomly chosen challenge, even if the attacker has access to a set of challenge-response pairs.
- PUFs are significantly **cheaper and safer alternatives** to storing keys in a non-volatile memory and they are the **only alternative** that fits perfectly to the hardware requirements of IoT networks to provide security to all digital devices, as well as to the whole network.
- PUFs can be used to also secure 6G networks, Cyber devices, Digital twins, Metaverse, etc.

A Simple PUF with Continuous-Valued Outputs

Ring Oscillator (RO) PUFs

- A delay-based intrinsic PUF scheme uses the **random variations in the oscillation frequencies** of ROs to generate a secret key.

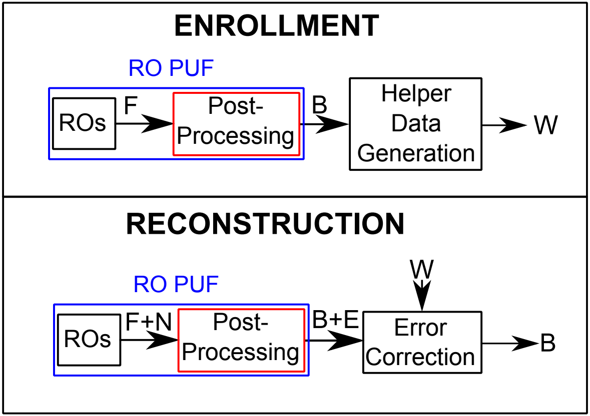


A Simple PUF with Continuous-valued Outputs II

RO PUFs

- **Source of randomness**: Uncontrollable silicon process variations on digital components' delays;
- **Hard macro designs** are used for each RO: identical implementations;
- **Temperature and voltage effects** are orders of magnitude greater than the random variations in RO outputs;
- **Correlations** in RO outputs decrease entropy in the extracted bit sequence;
- There is **noise** in every measurement of digital circuits.

Secret Key Generation with RO PUFs



F: Real-valued Oscillation Frequencies

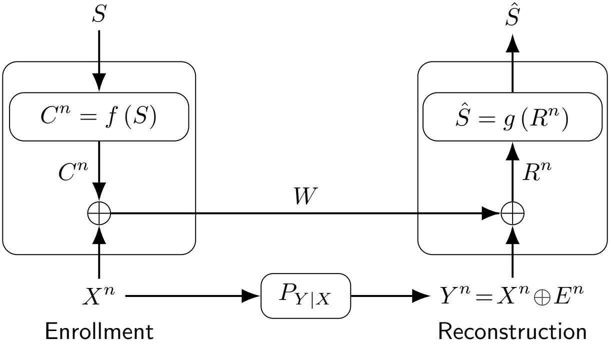
B: Uniform Bit Sequence

W: Side Information

N: Noise

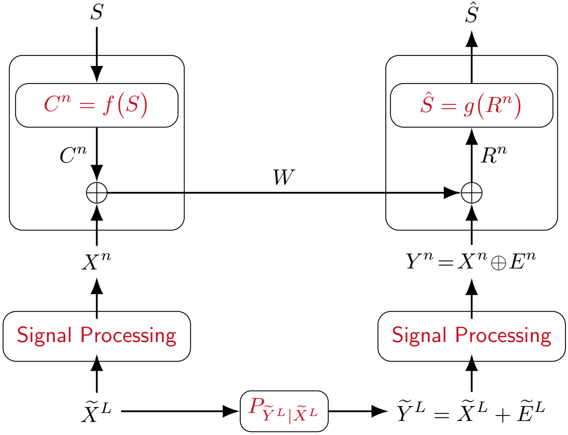
E: Error Vector

Fuzzy Commitment Scheme



- *Secret key* S and *helper data* W have to be independent,
- *Block error probability* should satisfy, e.g., $P_B = \Pr[S \neq \hat{S}] \leq 10^{-9}$;
- S should be uniformly random with entropy, e.g., $H(S) \geq 256$ bits.

Main Components to Design



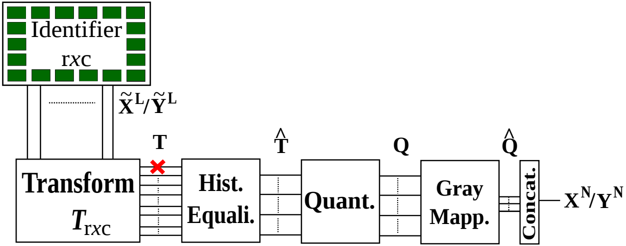
- *Block error probability* should satisfy, e.g., $P_B \leq 10^{-9}$.

Recall

RO PUFs

- **Source of randomness**: Uncontrollable silicon process variations on digital components' delays;
- **Hard macro designs** are used for each RO: identical implementations;
- **Temperature and voltage effects** are orders of magnitude greater than the random variations in RO outputs;
- **Correlations** in RO outputs decrease entropy in the extracted bit sequence;
- There is **noise** in every measurement of digital circuits.

How to Solve the 3 Problems Simultaneously

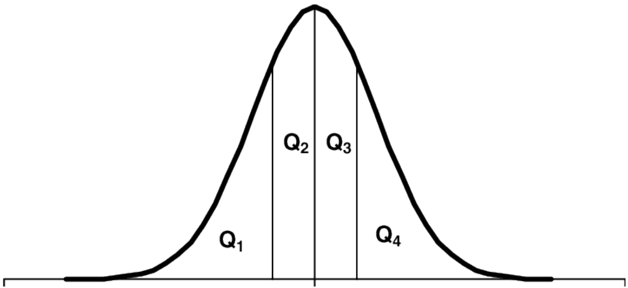


- Apply a **transform** $T_{r\times c}(\cdot)$ to decorrelate $\widetilde{X}^L$;
- Histogram equalization converts each transform-coefficient T output into a **standard (Gaussian) random variable**;

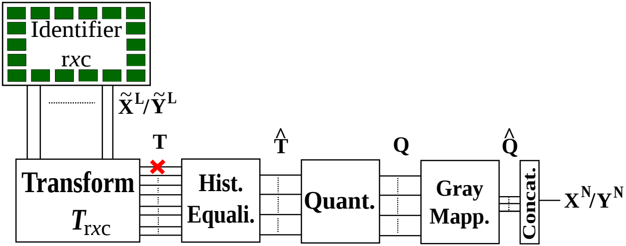
How to Solve the 3 Problems Simultaneously II

➤ Apply **scalar quantizers** that satisfy the **uniformity** property:

$$\Pr[\mathsf{Quant}(\widehat{T}_i) = (q_1, q_2, \ldots, q_{K_i})] = \frac{1}{2^{K_i}} \qquad \text{for} \qquad i = 1, 2, \ldots, L \quad (1)$$



How to Solve the 3 Problems Simultaneously III



- The noise components have zero mean, so use Gray mapping to extract bit sequences from quantized outputs;
- Concatenate all extracted bits to obtain X^N/Y^N;
- Error symbols $E_i = X_i \oplus Y_i$ need not be independent or identically distributed.

PUFs with Security Guarantees

- Model transform coefficients T as, e.g., **truncated Gaussian distributions**. Then, quantization boundaries, when $m \geq 1$ bits are extracted from a transform coefficient, are

$$b_k = Q^{-1}\left(Q(b_0)\cdot\left(1-\frac{k}{2^m}\right)+Q(b_{2^m})\cdot\frac{k}{2^m}\right) \quad \text{for } k=1,2,\ldots,(2^m-1) \tag{2}$$

- Consider any transform coefficient realization $T=t$ that is on the quantization boundary
$\Rightarrow$ Error probability is 0.5, so one cannot guarantee secrecy for all devices!!
$\Rightarrow$ **Current PUF products** only provide security guarantees for the **average over all devices**, so millions of intelligent IoT devices are likely **vulnerable** to malicious attacks!!

PUFs with Security Guarantees

- Model transform coefficients T as, e.g., **truncated Gaussian distributions**. Then, quantization boundaries, when $m \geq 1$ bits are extracted from a transform coefficient, are

$$b_k = Q^{-1}\left(Q(b_0)\cdot\left(1-\frac{k}{2^m}\right) + Q(b_{2^m})\cdot\frac{k}{2^m}\right) \quad \text{for } k = 1, 2, \ldots, (2^m - 1) \tag{2}$$

- Consider any transform coefficient realization $T = t$ that is on the quantization boundary
  $\Rightarrow$ Error probability is 0.5, so one cannot guarantee secrecy for all devices!!
  $\Rightarrow$ **Current PUF products** only provide security guarantees for the **average over all devices**, so millions of intelligent IoT devices are likely **vulnerable** to malicious attacks!!

PUFs with Security Guarantees II

- We propose to eliminate realizations

$$\bar{t} \in ((b_k - \delta/2),\, (b_k + \delta/2)] \tag{3}$$

for all transform coefficients and for some fixed $\delta \geq 0$ that is called the **Quality-of-Security-Service (QoSS) parameter** for all PUF outputs that are used for secure and private device authentication.

PUFs with Security Guarantees III

- Denote the **ratio of eliminated realizations vs. all realizations** as

$$\gamma(\delta) = \frac{\sum_{k=1}^{(2^m-1)} \left(Q\Big(b_k-\frac{\delta}{2}\Big)-Q\Big(b_k+\frac{\delta}{2}\Big)\right)}{Q(b_0)-Q(b_{2^m})}. \tag{4}$$

- The **percentage of realizations $\bar{t}$ used for secret key agreement**, i.e., manufacturing yield, is

$$\beta(\delta)=100\times(1-\gamma(\delta)) \tag{5}$$

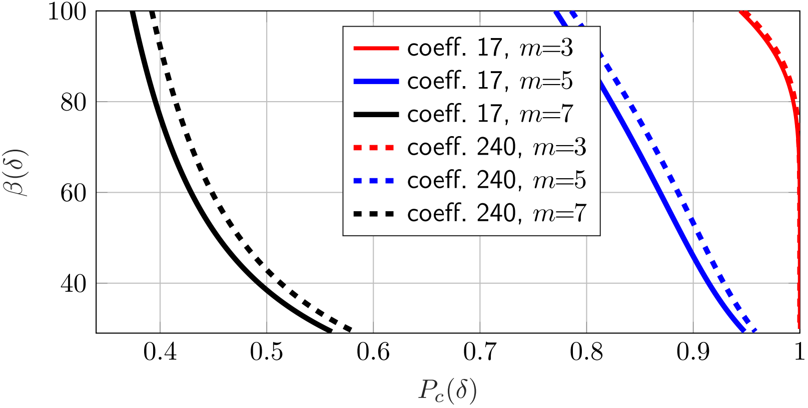
which decreases for increasing QoSS parameter δ
$\Rightarrow$ Stringent trade-off to be optimized!!

PUFs with Security Guarantees IV

- Define a reliability metric called **correctness probability** P_c that measures the probability that all bits are correct.
- **$\mathbf{P_c}$ increases for increasing δ.**

PUF Results from an RO Dataset

- $P_c(\delta)$ vs. $\beta(\delta)$ when a selected low-complexity transform with m-bit uniform quantization is applied to 16×16 RO arrays.
- We have $\beta = 100$ and P_c at its minimum when $\delta = 0$.



Part II

- **Optimal Error-Correcting Code Designs for PUFs**

Main Contributions

- We propose binning-based code constructions that are **Pareto optimal** and **improve on all** existing methods [GIS+'19].
- Polar codes designed for RO and SRAM PUFs **achieve rate tuples that cannot be achieved by existing methods**.
- **Significant performance improvements** are illustrated for
  - Multiple PUF measurements [GKS'15, GK'18],
  - Adaptive PUF measurements [KGS+'16, GKS+'18],
  - Multiple PUF enrollments (uses) [KGW'18],
  - Multiple rounds of communication [GGK'18], etc.

Main Contributions

- We propose binning-based code constructions that are **Pareto optimal** and **improve on all** existing methods [GIS+'19].

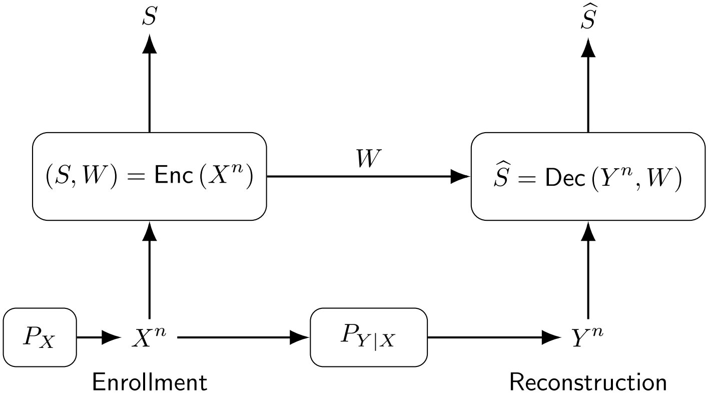
- Polar codes designed for RO and SRAM PUFs **achieve rate tuples that cannot be achieved by existing methods**.

- **Significant performance improvements** are illustrated for
  - Multiple PUF measurements [GKS'15, GK'18],
  - Adaptive PUF measurements [KGS+'16, GKS+'18],
  - Multiple PUF enrollments (uses) [KGW'18],
  - Multiple rounds of communication [GGK'18], etc.

Main Contributions

- We propose binning-based code constructions that are **Pareto optimal** and **improve on all** existing methods [GIS+'19].
- Polar codes designed for RO and SRAM PUFs **achieve rate tuples that cannot be achieved by existing methods**.
- **Significant performance improvements** are illustrated for
  - Multiple PUF measurements [GKS'15, GK'18],
  - Adaptive PUF measurements [KGS+'16, GKS+'18],
  - Multiple PUF enrollments (uses) [KGW'18],
  - Multiple rounds of communication [GGK'18], etc.

Problem Formulation – Generated-Secret (GS) Model



Notation

- The Shannon entropy measures the uncertainty, i.e.,
$H(X) = -\sum_{x \in \mathcal{X}} P_X(x) \log(P_X(x))$.

- Mutual information measures statistical dependency, i.e.,
$I(X;Y) = H(X) - H(X|Y)$.

- Note that min-entropy is relevant to but different from the Shannon entropy, and we can discuss why the Shannon entropy is the right metric for secret key generation from PUFs/biometrics with nested codes!

Key-Leakage-Storage Region

Definition

A key-leakage-storage tuple (R_s, R_ℓ, R_w) is *achievable* if, given any $\epsilon > 0$, there is some $n \geq 1$ for which $R_s = \dfrac{\log|\mathcal{S}|}{n}$ and

$$\Pr[\widehat{S} \neq S] \leq \epsilon \qquad \text{(reliability)} \tag{6}$$

$$\frac{1}{n} I(S;W) \leq \epsilon \qquad \text{(secrecy leakage)} \tag{7}$$

$$\frac{1}{n} H(S) \geq R_s - \epsilon \qquad \text{(key uniformity)} \tag{8}$$

$$\frac{1}{n} I(X^n;W) \leq R_\ell + \epsilon \qquad \text{(privacy leakage)} \tag{9}$$

$$\frac{1}{n} \log\left|\mathcal{W}\right| \leq R_w + \epsilon \qquad \text{(public storage).} \tag{10}$$

Key-Leakage-Storage Region (Cont'd)

Theorem (Ignatenko and Willems'09)

The key-leakage-storage region for the GS model is

$$\mathcal{R}_{\text{gs}} = \bigcup_{P_{U|X}} \Big\{ (R_s, R_\ell, R_w) : 0 \leq R_s \leq I(U;Y),$$
$$R_\ell \geq I(U;X) - I(U;Y),$$
$$R_w \geq I(U;X) - I(U;Y) \text{ for}$$
$$P_{UXY} = P_{U|X} P_X P_{Y|X} \Big\}. \tag{11}$$

Main Existing Methods

- *Code-offset fuzzy extractors* (COFE) [Dodis et al.'08] for the GS model,
- *Fuzzy-commitment scheme* (FCS) [Juels and Wattenberg'99] for the chosen-secret (CS) model,
- *Syndrome-based Polar Code Construction* [Chen et al.'17] for the GS model.

Existing Methods (Cont'd)

- COFE and FCS result in a storage rate of 1 bit/symbol since they apply **one-time padding**.

- Syndrome-based polar code construction
  - improved on existing methods because it is a **Slepian-Wolf coding (i.e., lossless compression)** construction,
  - achieves only a single point on the region $\mathcal{R}_{\text{gs}}$ boundary.

- We now show that our **Wyner-Ziv (WZ)-coding (i.e., lossy compression)** constructions [Shamai et al.'98, Korada et al.'10] are **Pareto-optimal**.

WZ-Coding with Random Linear Codes (RLCs)

Assume

- $X^n \sim \text{Bern}^n\left(\frac{1}{2}\right)$, i.e., $\Pr[X_i = 1] = \Pr[X_i = 0] = 0.5$ for all $i = 1, 2, \ldots, n$.
- $P_{Y|X}$ is a binary symmetric channel **(BSC) with crossover probability** p_A, i.e., $\Pr[Y \neq X] = p_A$.

WZ-Coding with RLCs (Cont'd)

- Choose **uniformly at random** full-rank parity-check matrices $\mathbf{H}_1$, $\mathbf{H}_2$, and $\mathbf{H}$ as

$$\mathbf{H} = \begin{bmatrix} \mathbf{H}_1 \\ \mathbf{H}_2 \end{bmatrix} \tag{12}$$

  - $\mathbf{H}_1 \in \{0,1\}^{m_1 \times n}$ defines a binary linear code $\mathcal{C}_1$ with parameters $(n, n-m_1)$, meaning that the codewords have size n and there are 2^{n-m_1} codewords.
  - $\mathbf{H} \in \{0,1\}^{(m_1+m_2) \times n}$ defines a binary linear code $\mathcal{C}$ with generator matrix $\mathbf{G}$ and parameters $(n, n-m_1-m_2)$,
  - Codes are **nested**, i.e., $\mathcal{C} \subseteq \mathcal{C}_1$.

WZ-Coding with RLCs (Cont'd)

- Impose the conditions, for some $q \in [0, 0.5]$ and $\delta > 0$ (not to be confused with the QoSS parameter),

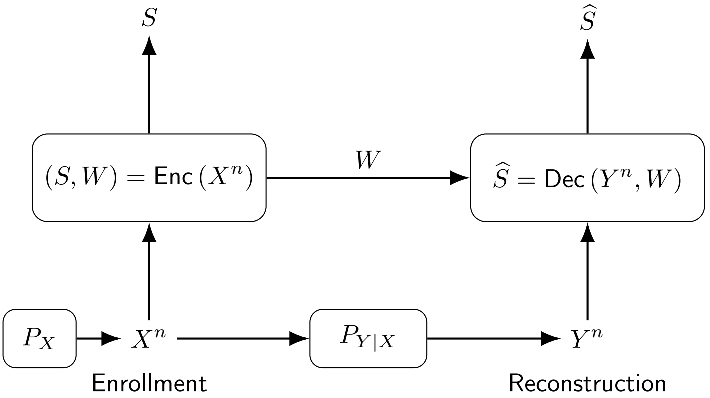
$$\frac{k_1}{n} \triangleq \frac{n - m_1}{n} = 1 - H_b(q) - \delta, \tag{13}$$

$$\frac{k}{n} \triangleq \frac{n - m_1 - m_2}{n} = 1 - H_b(q * p_A) - 2\delta \tag{14}$$

where

  - $H_b(q) = -q \log q - (1 - q) \log(1 - q)$,
  - $q * p_A = q(1 - p_A) + (1 - q)p_A$.

Problem Formulation (Recall)



WZ-Coding with RLCs (Cont'd)

Enrollment:

- Observe X^n and find the codeword $X_q^n \in \mathcal{C}_1$ such that

$$X_q^n = \underset{C^n \in \mathcal{C}_1}{\arg\min}\, d_H(X^n, C^n) \tag{15}$$

  where $d_H(\cdot)$ is the Hamming distance,

- Error sequence $X^n \oplus X_q^n \triangleq E_q^n \sim \text{Bern}^n(q)$ when $n \to \infty$,

- Assign $W = X_q^n \mathbf{H}_2^T$ as **helper data** since $X_q^n \mathbf{H}^T = [0\ W]$,

WZ-Coding with RLCs (Cont'd)

Enrollment (Cont'd):

- Sum X_q^n with the sequence L_W^n that is in the same coset as X_q^n and that has the minimum Hamming weight. The sum is $X_q^n \oplus L_W^n = X_c^n \in \mathcal{C}$,
- Assign the **secret key** S such that $X_c^n = S\mathbf{G}$,

WZ-Coding with RLCs (Cont'd)

Enrollment (Cont'd):

- Sum X_q^n with the sequence L_W^n that is in the same coset as X_q^n and that has the minimum Hamming weight. The sum is $X_q^n \oplus L_W^n = X_c^n \in \mathcal{C}$,

- Assign the **secret key** S such that $X_c^n = S\mathbf{G}$,

WZ-Coding with RLCs (Cont'd)

Enrollment (Cont'd):

- Codewords in blue and green belong to $\mathcal{C}_1$,
- Codewords in green belong to $\mathcal{C}$.

	$W=0$	$W=1$	...	$W=2^{m_2}-1$
$S=0$	$C_0^n=L_0^n=00..0$	$L_1^n=00..1$	...	$L_{2^{m_2}-1}^n=01..1$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
$S=s$	C_s^n	$C_s^n\oplus L_1^n$	...	$C_s^n\oplus L_{2^{m_2}-1}^n$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
$S=2^k-1$	$C_{2^k-1}^n$	$C_{2^k-1}^n\oplus L_1^n$	...	$C_{2^k-1}^n\oplus L_{2^{m_2}-1}^n$

WZ-Coding with RLCs (Cont'd)

Enrollment (Cont'd):

- Codewords in blue and green belong to $\mathcal{C}_1$,
- Codewords in green belong to $\mathcal{C}$.

	$W=0$	$W=1$	...	$W=2^{m_2}-1$
$S=0$	$C_0^n=L_0^n=00..0$	$L_1^n=00..1$	...	$L_{2^{m_2}-1}^n=01..1$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
$S=s$	C_s^n	X_q^n	...	$C_s^n \oplus L_{2^{m_2}-1}^n$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
$S=2^k-1$	$C_{2^k-1}^n$	$C_{2^k-1}^n \oplus L_1^n$	...	$C_{2^k-1}^n \oplus L_{2^{m_2}-1}^n$

WZ-Coding with RLCs (Cont'd)

Enrollment (Cont'd):

- Codewords in blue and green belong to $\mathcal{C}_1$,
- Codewords in green belong to $\mathcal{C}$.

	$W=0$	$W=1$	...	$W=2^{m_2}-1$
$S=0$	$C_0^n = L_0^n = 00..0$	$L_1^n = 00..1$	...	$L_{2^{m_2}-1}^n = 01..1$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
$S=s$	C_s^n	X_q^n	...	$C_s^n \oplus L_{2^{m_2}-1}^n$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
$S=2^k-1$	$C_{2^k-1}^n$	$C_{2^k-1}^n \oplus L_1^n$	...	$C_{2^k-1}^n \oplus L_{2^{m_2}-1}^n$

WZ-Coding with RLCs (Cont'd)

Enrollment (Cont'd):

- Codewords in blue and green belong to $\mathcal{C}_1$,
- Codewords in green belong to $\mathcal{C}$.

	$W=0$	$W=1$	...	$W=2^{m_2}-1$
$S=0$	$C_0^n=L_0^n=00..0$	$L_1^n=00..1$	...	$L_{2^{m_2}-1}^n=01..1$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
$S=s$	C_s^n	X_q^n	...	$C_s^n\oplus L_{2^{m_2}-1}^n$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
$S=2^k-1$	$C_{2^k-1}^n$	$C_{2^k-1}^n\oplus L_1^n$	...	$C_{2^k-1}^n\oplus L_{2^{m_2}-1}^n$

WZ-Coding with RLCs (Cont'd)

Enrollment (Cont'd):

- Codewords in blue and green belong to $\mathcal{C}_1$,
- Codewords in green belong to $\mathcal{C}$.

	$W=0$	$W=1$	...	$W=2^{m_2}-1$
$S=0$	$C_0^n=L_0^n=00..0$	$L_1^n=00..1$	...	$L_{2^{m_2}-1}^n=01..1$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
$S=s$	$X_c^n=X_q^n\oplus L_1^n$	X_q^n	...	$C_s^n\oplus L_{2^{m_2}-1}^n$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
$S=2^k-1$	$C_{2^k-1}^n$	$C_{2^k-1}^n\oplus L_1^n$	...	$C_{2^k-1}^n\oplus L_{2^{m_2}-1}^n$

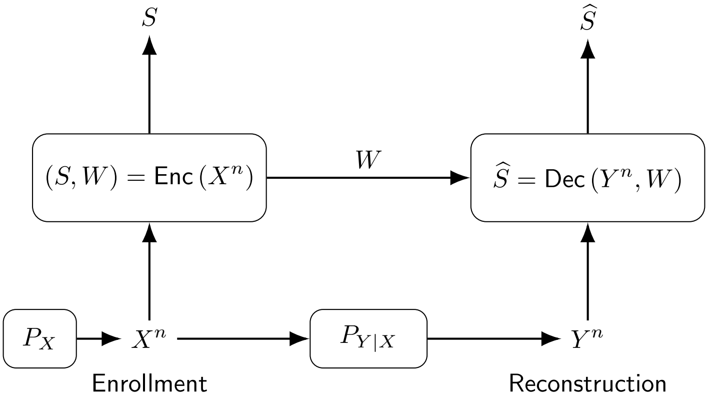
WZ-Coding with RLCs (Cont'd)

Enrollment (Cont'd):

- Codewords in blue and green belong to $\mathcal{C}_1$,
- Codewords in green belong to $\mathcal{C}$.

	$W=0$	$W=1$	...	$W=2^{m_2}-1$
$S=0$	$C_0^n=L_0^n=00..0$	$L_1^n=00..1$	...	$L_{2^{m_2}-1}^n=01..1$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
$S=s$	$X_c^n=X_q^n\oplus L_1^n$	X_q^n	...	$C_s^n\oplus L_{2^{m_2}-1}^n$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
$S=2^k-1$	$C_{2^k-1}^n$	$C_{2^k-1}^n\oplus L_1^n$	...	$C_{2^k-1}^n\oplus L_{2^{m_2}-1}^n$

Problem Formulation (Recall)



WZ-Coding with RLCs (Cont'd)

Reconstruction:

- The channel $P_{Y^n|X_q^n} \sim \mathrm{Bern}^n(q * p_A)$ when $n \to \infty$,
- $\mathcal{C}$ **can correct errors in** $P_{Y^n|X_q^n}$ with high probability to estimate X_q^n,
- $\widehat{X}_q^n$ determines $\widehat{S}$.

WZ-Coding with RLCs (Cont'd)

Reconstruction:

- The channel $P_{Y^n|X_q^n} \sim \text{Bern}^n(q * p_A)$ when $n \to \infty$,
- $\mathcal{C}$ **can correct errors in** $P_{Y^n|X_q^n}$ with high probability to estimate X_q^n,
- $\widehat{X}_q^n$ determines $\widehat{S}$.

WZ-Coding with RLCs (Cont'd)

Reconstruction:

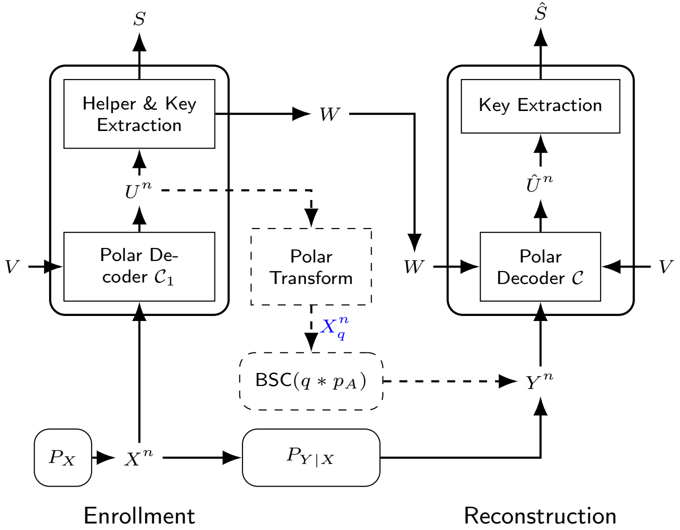
- The channel $P_{Y^n|X_q^n} \sim \text{Bern}^n(q * p_A)$ when $n \rightarrow \infty$,
- $\mathcal{C}$ **can correct errors in** $P_{Y^n|X_q^n}$ with high probability to estimate X_q^n,
- $\widehat{X}_q^n$ determines $\widehat{S}$.

WZ Polar Code Construction

Polar Codes (used in the 5G wireless communications standard)

- A polar transform converts an input sequence U^n with frozen and unfrozen bits to a codeword X^n.
- Polar codes [Arıkan'08] rely on **converting** the physical channel $P^n_{Y|X}$ **into virtual channels** $P_{Y^nU^{i-1}|U_i}$.

WZ Polar Code Construction (Cont'd)



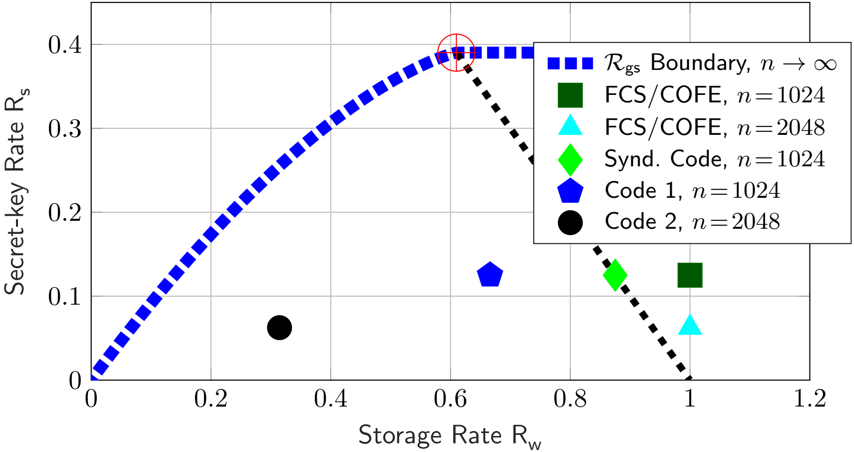
Rate-Tuple Comparisons

- Key length 128 bits,
- Block error probability $P_B = 10^{-6}$,
- $P_{Y|X} \sim \text{BSC}(p_A = 0.15)$.
- Design **nested polar codes** in combination with successive cancellation list **(SCL) decoders** with **list size** 8.

Rate-Tuple Comparisons

- Key length 128 bits,
- Block error probability $P_B = 10^{-6}$,
- $P_{Y|X} \sim \text{BSC}(p_A = 0.15)$.
- Design **nested polar codes** in combination with successive cancellation list **(SCL) decoders** with **list size** 8.

Rate-tuple Comparisons (Cont'd)



Conclusion

- We proved that **security guarantees** can be given (**unlike some of the current PUF products**) to **every digital device with a PUF**;
- Illustrated that **by removing a small percentage** of manufactured PUF circuits, it is possible to **significantly simplify the error-correcting code design** due to increased reliability;
- Conversely, we proved that **without removing any PUF** circuit output, **no security guarantee per PUF**;
- We illustrated that the proposed nested linear block code constructions are **optimal for key extraction from PUFs**;
- We estimated the information leakage of nested polar codes by using neural estimators to showcase that **practical PUF designs with our proposed code constructions leak only a negligible amount of information**.

THANK YOU!

Onur Günlü
Information Theory and Security Laboratory (ITSL)
onur.gunlu@liu.se

References for Part II

[Gassend et. al'02] B. Gassend, D. Clarke, M. Van Dijk, and S. Devadas, "Silicon Physical Random Functions,ïn *ACM Conf. Computer Commun. Security*, Washington, DC, USA, Nov. 2002, pp. 148–160.

[GI'14] O. Günlü and O. İşcan, "DCT Based Ring Oscillator Physical Unclonable Functions,ïn *IEEE Int. Conf. Acoust., Speech Sign. Proc.*, Florence, Italy, Sep. 2014, pp. 8198–8201.

[GIK'15] O. Günlü, O. İşcan, and G. Kramer, "Reliable Secret Key Generation from Physical Unclonable Functions Under Varying Environmental Conditions,ïn *IEEE Int. Workshop Inf. Forensics Security*, Rome, Italy, Nov. 2015, pp. 1–6.

[GIS+'16] O. Günlü, O. İşcan, V. Sidorenko, and G. Kramer, "Reliable Secret-key Binding for Physical Unclonable Functions with Transform Coding,ïn *IEEE Global Conf. Sign. Inf. Proc.*, Greater Washington, D.C., USA, Dec. 2016, pp. 986–991.

[GBG'17] O. Günlü, A. Belkacem, and B. Geiger, "Secret-key Binding to Physical Identifiers with Reliability Guarantees,ïn *IEEE Int. Conf. Commun.*, Paris, France, May 2017, pp. 1-6.

[GKI+'18] O. Günlü, T. Kernetzky, O. İşcan, V. Sidorenko, G. Kramer, and R. F. Schaefer, "Secure and Reliable Key Agreement with Physical Unclonable Functions," *Entropy*, vol. 20, no. 5, May 2018.

[GIS+'19] O. Günlü, O. İşcan, V. Sidorenko, and G. Kramer, "Code Constructions for Physical Unclonable Functions and Biometric Secrecy Systems,ßubmitted to *IEEE Trans. Inf. Forensics Security*, Aug. 2018.

[GKS'15] O. Günlü, G. Kramer, and M. Skorski, "Privacy and Secrecy with Multiple Measurements of Physical and Biometric Identifiers,ïn *IEEE Conf. Commun. Network Security*, Florence, Italy, Sep. 2015, pp. 89–94.

[GK'18] O. Günlü and G. Kramer, "Privacy, Secrecy, and Storage with Multiple Noisy Measurements of Identifiers," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 11, pp. 2872–2883, Nov. 2018.

[KGS+'16] K. Kittichokechai, O. Günlü , R. F. Schaefer, and G. Caire, "Private Authentication with Controllable Meauserement,ïn *Asilomar Conf. Sign., Sys. Comput.*, Pacific Grove, CA, USA, Nov. 2016, pp. 1680–1684.

References for Part II (cont'd)

[GKS+'18] O. Günlü, K. Kittichokechai, R. F. Schaefer, and G. Caire, "Controllable Identifier Measurements for Private Authentication With Secret Keys." *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 8, pp. 1945–1959, Aug. 2018.

[KGW'18] L. Kusters, O. Günlü, and F. M. J. Willems, "Zero Secrecy Leakage for Multiple Enrollments of Physical Unclonable Functions,ïn *Symp. Inf. Theory Sign. Process. the Benelux*, Enschede, The Netherlands, May 2018.

[GGK'18] A. Gohari, O. Günlü, and G. Kramer, "On Achieving a Positive Rate in the Source Model Key Agreement Problem,ïn *IEEE Int. Symp. Inf. Theory*, Vail, CO, USA, June 2018, pp. 2659–2663.

[Dodis et al.'08] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, "Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data," *SIAM J. Comput.*, vol. 38, no. 1, pp. 97–139, Jan. 2008.

[Juels and Wattenberg'99] A. Juels and M. Wattenberg, "A Fuzzy Commitment Scheme,ïn *ACM Conf. Comp. Commun. Security*, New York City, NY, USA, Nov. 1999, pp. 28–36.

[Chen et al.'17] B. Chen, T. Ignatenko, F. MJ Willems, R. Maes, E. van der Sluis, and G. Selimis, "A Robust SRAM-PUF Key Generation Scheme Based on Polar Codes,ïn *IEEE Global Commun. Conf.*, Singapore, Dec. 2017, pp. 1–6.

[Arıkan'09] E. Arikan, "Channel Polarization: A Method for Constructing Capacity-Achieving Codes for Symmetric Binary-Input Memoryless Channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 7, pp. 3051–3073, July 2009.

[Shamai et al.'98] S. Shamai, S. Verdú, and R. Zamir, "Systematic Lossy Source/Channel Coding," *IEEE Trans. Inf. Theory*, vol. 44, no. 2, pp. 564–579, Mar. 1998.

[Korada et al.'10] S. B. Korada and R. L. Urbanke, "Polar Codes are Optimal for Lossy Source Coding," *IEEE Trans. Inf. Theory*, vol. 56, no. 4, pp. 1751–1768, Apr. 2010.