Tutorial 1: Key Agreement and Secure Identification with Physical Unclonable Functions (PUFs)

Onur Günlü and Rafael F. Schaefer

Information Theory and Applications Chair, TU Berlin

{**guenlue, rafael.schaefer**}**@tu-berlin.de**

IEEE WIFS, Dec. 2019

Outline

1. PUF Basics
2. Models and Rate Regions for Key Agreement with PUFs
3. Optimal Code Constructions for Key Agreement with PUFs
4. Secure Identification with PUFs

Part I

PUF Basics

Motivations

- Many assumptions for biometric secrecy systems and PUFs are common.
- Motivations for biometric secrecy systems will pave the way for the slightly different motivations for PUFs.
- We will motivate the similarities between these two systems to ease understanding, but we will also discuss differences to choose the correct model for key agreement with PUFs.

Motivations for Biometric Identifiers

- Passwords, secret answers to a question, or secret questions for an answer are used for individual authentication or identification. Such information
  - should be memorized every time it is renewed,
  - can be possibly guessed if it is not strong enough,
  - can be stolen easily by seeing it once.

Motivations for Biometric Identifiers (Cont'd)

- Alternative: biometric identifiers such as fingerprints, iris, shape of a hand, DNA, and blood that are
  - always there without memorizing,
  - mostly reliable over time without renewal,
  - hard to steal or guess.

Motivations for Physical Identifiers

- Secure secret-key storage and execution in Non-volatile Memory (NVM) are not trivial due to
  - non-uniform key generation,
  - possible physical access to the storage medium,
  - information leakage via side-channels.

Motivations for Physical Identifiers (Cont'd)

- Alternative: physical identifiers such as fine variations in the osciallation frequency of ring oscillators (ROs) for **on-demand** key generation so that
  - invasive attacks permanently change the identifier output,
  - randomness is provided by the uncontrollable manufacturing variations,
  - new identifiers can be inserted when there is leakage.

Recent Security and Privacy Issues in IoT

- In October 2016, a series of Distributed Denial of Service attacks targeted the Domain Name System.
- Twitter, Reddit, GitHub, Etsy, Spotify, PayPal, the Guardian, and the New York Times websites did not work.
- During cyberattacks, learning attacks were extensively applied to "test" the core defensive capabilities of the companies that provide critical internet services.

Recent Security and Privacy Issues in IoT

- Massive number of poorly-secured IoT devices, e.g., routers and surveillance cameras, were used for the attack
  $\Rightarrow$ Secrecy leakage.

- The infections were made possible by the use of **default passwords on these devices**.

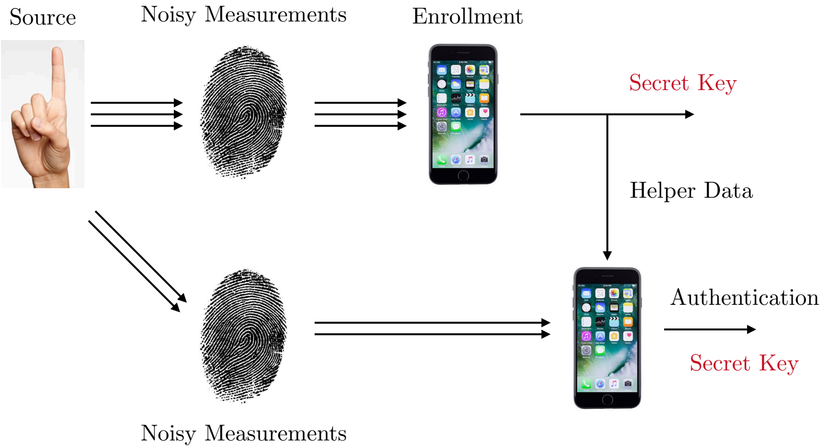
- Impersonation is possible via infected IoT devices
  $\Rightarrow$ Privacy leakage.

Solutions to Privacy Issues in IoT

- Physical-layer solutions are preferred.
- Independent hardware-intrinsic security is required $\Rightarrow$ PUFs!
- Force IoT to require an identification sequence to take any online action.
- PUFs provide higher security than passwords and biometrics since
  - PUF outputs are not controllable by the manufacturer/user/attacker;
  - Any invasive attack permanently changes the PUF outputs;
  - PUFs generate their outputs only when powered up.

Biometric Application

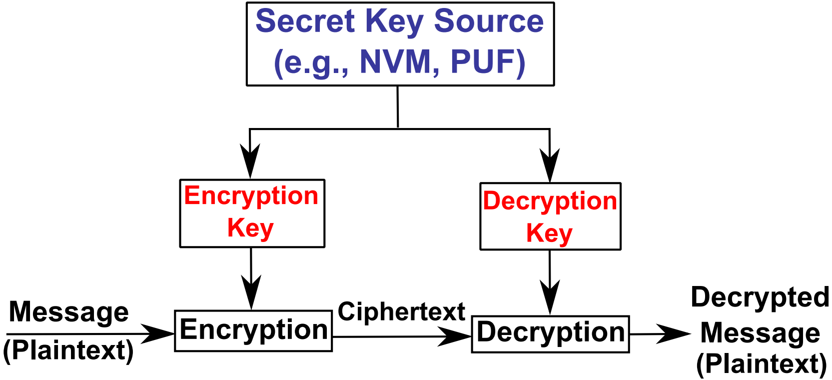
- **Mobile Device User Authentication with Fingerprints**



PUF Application 1

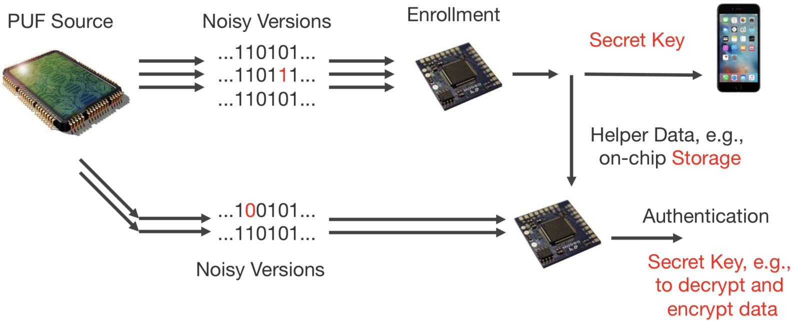
- **Encryption/Decryption with Physical Unclonable Functions (PUFs)**

NVM= Non-Volatile Memory



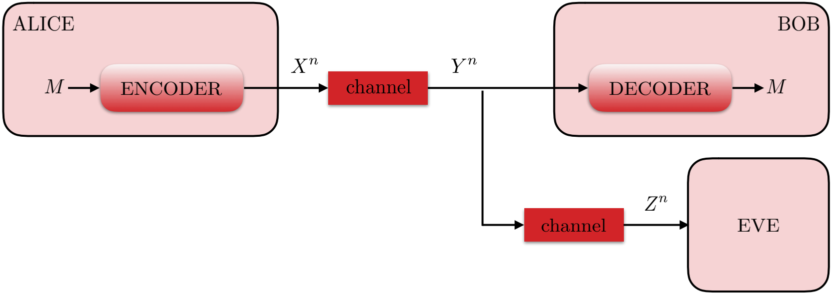
PUF Application 2

- **PUF Outputs Used As a Local Key for a Digital Device**



PUF Application 3

- **Wiretap channel (WTC) Communication with a PUF Output as the Local Randomizer at the WTC Encoder**



➤ Consider the PUF output as an additional input to the WTC encoder.

Other PUF Applications

- Other applications of PUFs:
  - ➤ Security of an item with an RFID tag can be provided by using lightweight PUF designs as a source of secret key that protects the RFID tag from being copied.
  - ➤ Non-repudiation, i.e., undeniable transmission or reception of data, proof of execution on a specific processor, and remote integrated circuit (IC) enabling, can be provided by PUFs.

Other PUF Applications (Cont'd)

- Every application of PUFs has **different assumptions** about the PUF properties, computational complexity of the system that takes PUF outputs as input, and the specific system models. There are different constraints and system parameters for each application.
- We focus mainly on the application where a secret key is generated from a PUF for user, or device, authentication.

A Definition of PUF

- A PUF is a challenge response mapping embodied by a physical device such that it is
  - easy and fast for the physical device to evaluate the PUF response;
  - hard for an attacker, who cannot access the PUF, to determine the PUF response to a randomly chosen challenge, even if he has access to a set of challenge-response pairs.

Physical vs. Physically

- There are alternative expansions of the term PUF such as "physically unclonable function", which suggests that it is a function that is only physically unclonable.
- Physically unclonable functions may provide a weaker security guarantee since they allow their functions to be digitally cloned.
- For any practical application of a PUF, we need the property of unclonability both physically and digitally.
- We therefore use only the term **"physical unclonable function"**.

PUF Types

- There are many ways to group PUF types, e.g., electronic vs. non-electronic PUFs or weak vs. strong PUFs.

- **Weak PUFs** are identified by having a limited number of challenge response pairs (CRPs) and by keeping the responses internal and secret.

- **Strong PUFs** must allow many CRPs with the feature of unpredictability of a uniformly-at-random chosen CRP from a small set of known CRPs.

- We focus on weak PUFs such as ring oscillators (ROs) and SRAM PUFs.

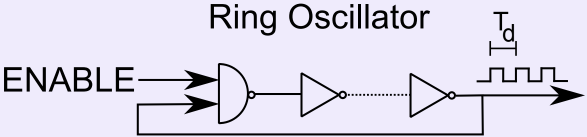
PUF Types (Cont'd)

- Weak PUFs were not preferred due to the *"small entropy"* one can extract from them, but we show that
  - If the random sequence is extracted over the dimension of the set of devices/PUFs, one can extract **infitinitely many secure bits from weak PUFs**,
  - The **optimal number of secure bits** extracted from weak PUFs with noisy outputs **can be achieved by using a nested code construction** proposed,
  - The **transform-coding algorithm** is shown to require a **smaller hardware area than benchmark PUF designs**.

RO PUF Review

RO PUFs

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

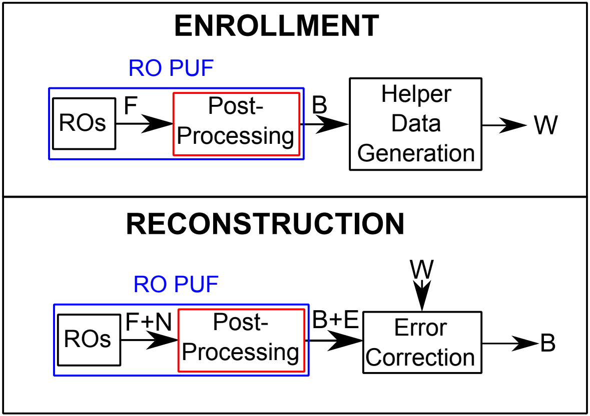


RO PUF Review (Cont'd)

RO PUFs

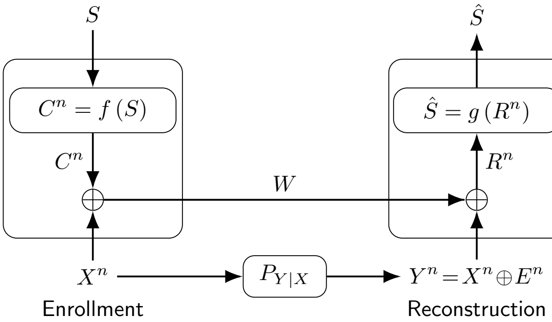
- **Source of randomness**: the uncontrollable silicon process variations on digital components' delays.
- **Hard macro designs** are used for each RO: identical implementations.
- **Temperature and voltage effects** are orders of magnitude greater than the random variations in RO outputs.
- **Correlations**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

Secret Key Generation with RO PUFs



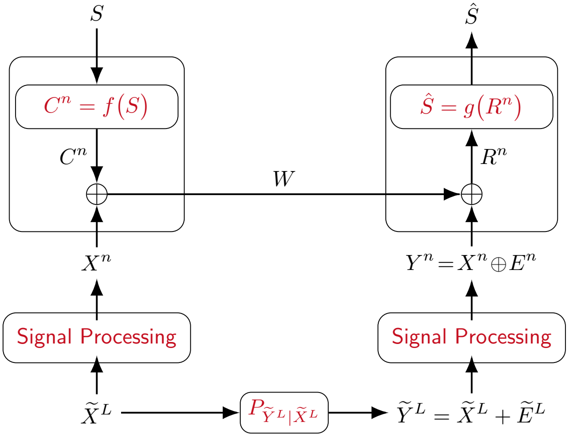
F: Real-valued Oscillation Frequencies
B: Uniform Bit Sequence
W: Side Information
N: Noise
E: Error Vector

Fuzzy Commitment Scheme



- *Secret key* S and *helper data* W have to be independent,
- *Block error probability* should satisfy $P_B \leq 10^{-9}$,
- S should be uniformly random with entropy ≥ 128 bits.

Main Aims



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

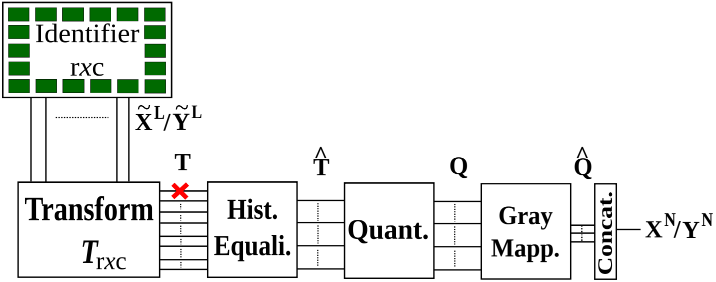
$f(\cdot)$ and $g(\cdot)$

- Suppose *binary linear block codes* with bounded minimum distance decoders (BMDD) are used for low complexity.

- A block code has
  - blocklength n,
  - dimension k,
  - minimum distance d.

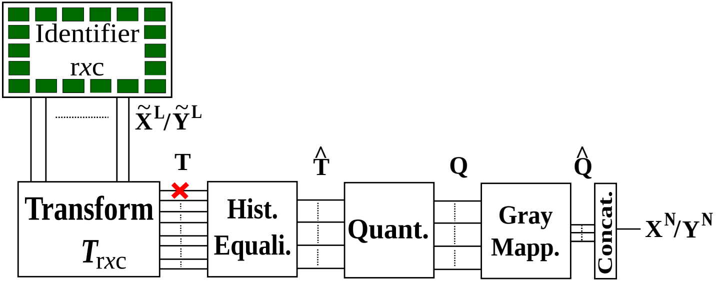
- A BMDD for a block code can correct all error patterns with at most $e = \left\lfloor \dfrac{d-1}{2} \right\rfloor$ errors.

Signal Processing Steps



- Apply a transform $T_{r\times c}(\cdot)$ to decorrelate $\widetilde{X}^L$,
- Histogram equalization converts all transform-coefficient outputs into standard Gaussian random variables,
- Each scalar quantizer satisfies the **uniformity** property
$$\Pr[\text{Quant}(\widehat{T}_i) = (q_1, q_2, \ldots, q_{K_i})] = \frac{1}{2^{K_i}} \text{ for } i = 1, 2, \ldots, L,$$

Signal Processing Steps (Cont'd)



- The noise components have zero mean, so use Gray mapping,
- 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.

Previous Approach

Average Fractional Hamming Distance $D(K)$ Metric

$$D_i(L)=\frac{1}{L}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\left(\sum_{l=1}^{2^L}\Pr[Q(\hat{t}+\hat{n})=l]\mathrm{HD}_l(\hat{t})\right)\cdot p_{\widehat{T}_i}(\hat{t})p_{\widehat{N}_i}(\hat{n})\mathrm{d}\hat{t}\mathrm{d}\hat{n}$$

- L: Number of bits extracted from the i-th transform coefficient;
- $\mathrm{HD}_l(\hat{t})$: Hamming distance between sequences assigned to the l-th interval and to the interval $Q(\hat{t})$ with **equiprobable** quantization intervals;
- $\widehat{T}_i$: Standard normal distributed transform coefficient;
- $\widehat{N}_i$: Gaussian noise in the i-th coefficient after equalization.

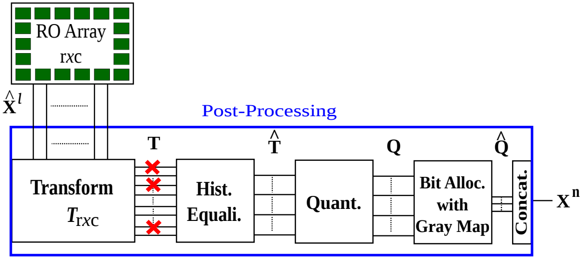
Previous Approach (Cont'd)

1. Fix a crossover probability p_b for all binary symmetric channels (BSCs) $P_{Y|X}$ of all transform coefficients.

2. Determine the number of bits $L_i(p_b)$ extracted from the i-th coefficient as the greatest number of bits L such that $D_i(L) \leq p_b$.

3. Design channel codes for the BSC $P_{Y|X}$ with crossover probability p_b in combination with the fuzzy-commitment scheme.

Improvements to the Previous Approach



➢ Keep the structure of the post-processing steps.

➢ Satisfy the same security and privacy constraints, i.e.,

- Code dimension, e.g., $k \geq 128$ bits,
- Code rate is at its maximum,
- Extracted bit sequence X^n is i.i.d. according to Ber(0.5),
- Equivalent channel $P_{Y|X}$ is memoryless.

Improvements to the Previous Approach (Cont'd)

- ✗ Model the channel (conservatively) as a BSC;
  ✓ Success probability is used without a channel model.

- ✗ Maximize the total number L_{total} of bits extracted;
  ✓ Give reliability guarantees for a fixed-length sequence.

- Find "low-complexity" block codes that satisfy the block-error probability constraint $P_B \leq 10^{-9}$ by ensuring that a fixed number t_{required} of errors can be corrected.

Code-based Quantizer Design

- Suppose a BMDD can correct all patterns with up to e errors,
- We order the transform coefficients such that the numbers of bits K_i extracted are non-increasing, i.e., $K_i \geq K_{i+1}$ for all $i = 1, 2, \ldots, L-1$,
- Consider the correctness metric (**conservative**!)

$$P_{\mathsf{C},i}(K_i) = \Pr[(X_1, X_2, \ldots, X_{K_i}) = (Y_1, Y_2, \ldots, Y_{K_i})],$$

- If C_{max} coefficients are erroneous, the BMDD should satisfy (**conservative**!)

$$e \geq \sum_{i=1}^{C_{\mathsf{max}}} K_i,$$

Code-based Quantizer Design (Cont'd)

- Determine $K_i = \max K$ such that $P_{c,i}(K) \geq \bar{P}_c(C_{\text{max}})$,
  - $\bar{P}_c(C_{\text{max}}) = \min P$ satisfying (**conservative**!)

$$\sum_{c=C_{\text{max}}+1}^{L} \binom{L}{c} (1-P)^c P^{L-c} = P_B \leq 10^{-9}.$$

- For a fixed C_{max}, the binary block code should satisfy
  - blocklength $n \leq N = \sum_{i=1}^{L} K_i$,
  - dimension $k \geq 128$,
  - minimum distance $d \geq 2e + 1 \geq 2\left(\sum_{i=1}^{C_{\text{max}}} K_i\right) + 1$.

RO Dataset

- We use a public dataset with ring oscillator (RO) outputs.
- The dataset contains multiple measurements of 16×16 arrays of ROs, i.e., $L = 255$, with identical circuit designs.
- Measurements are taken from multiple devices from **the same chip family** under ideal temperature and voltage conditions.

Code-based Quantizer Design for ROs

$\mathbf{C}_{\mathsf{max}}$	**16**	**17**	**18**	**19**	**20**
$\bar{P}_c$	0.9902	0.9889	0.9875	0.9860	0.9844
K_{max}	3	3	3	3	3
N	144	224	250	255	259
e	18	20	21	23	25

- We apply the two-dimensional discrete cosine transform (DCT) to decorrelate the identifier outputs in the dataset.

Code-based Quantizer Design for ROs

$\mathbf{C}_{\mathsf{max}}$	**16**	**17**	**18**	**19**	**20**
$\bar{P}_c$	0.9902	0.9889	0.9875	0.9860	0.9844
K_{max}	3	3	3	3	3
N	144	224	250	255	259
e	18	20	21	23	25

- $\bar{P}_c(C_{\mathsf{max}}) = \min P$ satisfying

$$\sum_{c=C_{\mathsf{max}}+1}^{L} \binom{L}{c} (1-P)^c P^{L-c} = P_B \leq 10^{-9}$$

Code-based Quantizer Design for ROs

$\mathbf{C}_{\mathsf{max}}$	**16**	**17**	**18**	**19**	**20**
$\bar{P}_c$	0.9902	0.9889	0.9875	0.9860	0.9844
K_{max}	3	3	3	3	3
N	144	224	250	255	259
e	18	20	21	23	25

- $K_i = \max K$ such that $P_{c,i}(K) \geq \bar{P}_c(C_{\mathsf{max}})$

Code-based Quantizer Design for ROs

$\mathbf{C_{max}}$	**16**	**17**	**18**	**19**	**20**
$\bar{P}_c$	0.9902	0.9889	0.9875	0.9860	0.9844
K_{max}	3	3	3	3	3
N	144	224	250	255	259
e	18	20	21	23	25

- Total bit length: $N = \sum_{i=1}^{L} K_i$

Code-based Quantizer Design for ROs

$\mathbf{C_{max}}$	**16**	**17**	**18**	**19**	**20**
$\bar{P}_c$	0.9902	0.9889	0.9875	0.9860	0.9844
K_{max}	3	3	3	3	3
N	144	224	250	255	259
e	18	20	21	23	25

- $e \geq \sum_{i=1}^{C_{\mathsf{max}}} K_i$

Code-based Quantizer Design for ROs

$\mathbf{C_{max}}$	**16**	**17**	**18**	**19**	**20**
$\bar{P}_c$	0.9902	0.9889	0.9875	0.9860	0.9844
K_{max}	3	3	3	3	3
N	144	224	250	255	259
e	18	20	21	23	25

- None of the binary (extended) Bose-Chaudhuri-Hocquenghem (BCH) and Reed-Solomon (RS) codes satisfy any $[N(C_{\mathsf{max}}),\, e(C_{\mathsf{max}})]$ pair
- The requirements used for the table are **conservative**!

Code Selection

- Consider the pair $[N(20) = 259, e(20) = 25]$ but enforce $\mathbf{K_i = 1}$. Then, we obtain $\mathbf{N = L = 255}$ and $\mathbf{e = C_{\textsf{max}} = 20}$!
- Choose the binary BCH code with
  - blocklength $n = 255$,
  - dimension $k = 131$,
  - minimum distance $d = 2e_{\textsf{BCH}} + 1 = 2 \times 18 + 1$.
- $e_{\textsf{BCH}} = 18$ is smaller than the requirement $e = 20$. **However, the requirements are still conservative!**

Code Selection (Cont'd)

BCH$(255, 131, 18)$ **actually** satisfies the constraint $P_B \leq 10^{-9}$ since

- Each coefficient has a different success probability
  $\Rightarrow$ Poisson binomial distribution of success probabilities;

- From the DFT Characteristic Function (CF) method, we obtain

$$\sum_{e=19}^{255} \left\{ \sum_{A \in F_e} \prod_{j \in A} (1 - T_j) \prod_{j \in A^c} T_j \right\} \leq 10^{-9}$$

where T_js are success probabilities and F_e is the set of all subsets of e integers that can be selected from $\{1, 2, \ldots, 255\}$.

➤ **Remark**: We need to consider $\approx 10^{27}$ cases if we do not use the DFT-CF method!

Code Selection

- Calculate the block-error probability with this code as $\mathbf{P_B \approx 1.26 \times 10^{-11}} < 10^{-9}$!

- BCH$(255, 131)$ has better **secret-key and privacy-leakage rates** than other proposed codes for the *fuzzy commitment scheme*, *syndrome-based methods*, and *fuzzy extractors*.

Discussions

- There is still a gap between the optimal rate pairs and the proposed code.
- This gap can be closed **by using other channel encoders and decoders at the cost of higher hardware complexity** or **by designing other schemes**.
- We will discuss **the first optimal code construction** for PUFs and biometrics with privacy preservation. This construction improves on all previous schemes.

Discussions (Cont'd)

The choice of transform is **vital** since

- Decorrelation efficiency of the transform (i.e., **Uniformity and Secrecy Leakage**),
- The bit error probability of each extracted bit (i.e., **Reliability**),
- Complexity of post-processing (i.e., **Hardware complexity**)

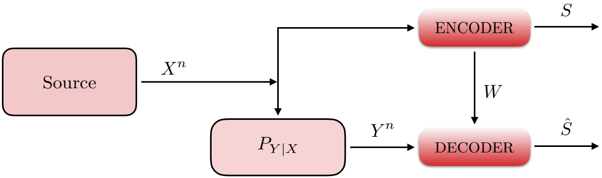
are determined by the transform.

- We compared many transforms and suggest to use the Discrete Walsh Hadamard Transform (DWHT) due to low complexity, high reliability, and high decorrelation efficiency.

Part II

Models and Rate Regions for Key Agreement with PUFs

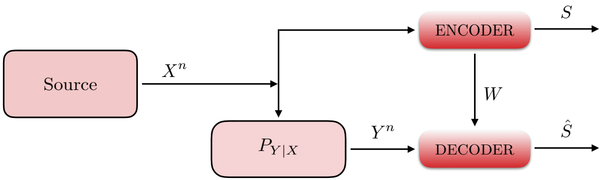
PUF Models and Problem Definition



Consider

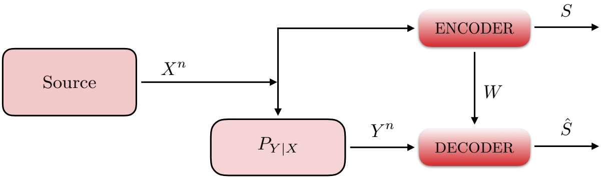
- noiseless biometric identifier or PUF outputs $X^n \sim P_X^n$,
- noisy outputs Y^n measured through the DMC $P_{Y|X}$,
- secret key S and public side information (*helper data*) generated from X^n,
- secret key $\hat{S}$ estimated from (Y^n, W).

PUF Models and Problem Definition (Cont'd)



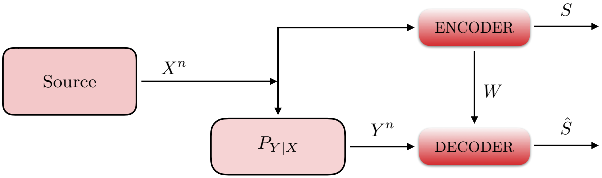
- This model is called **generated-secret (GS)** model.
- The model where a secret key S that is independent of (X^n, Y^n) is embedded to the encoder, is called **chosen-secret (CS)** model.

PUF Models and Problem Definition (Cont'd)



- Make error probability $\Pr[S \neq \hat{S}]$ **negligible**,
- Make secrecy leakage $I(S;W)$ **negligible**,
- **Maximize** secret key S rate $R_\mathsf{s} = \dfrac{H(S)}{n}$,
- **Minimize** public helper data W rate $R_\mathsf{w} = \dfrac{\log|\mathcal{W}|}{n}$,
- **Minimize** privacy-leakage rate $R_\ell = \dfrac{1}{n} I(X^n;W)$.

PUF Models and Problem Definition (Cont'd)



- Reliability: Block error probability $P_\mathsf{e} = \Pr[\hat{S} \neq S]$ should **vanish**,
- Secrecy: S should be **independent** of W and R_s should be **maximized**,
- Privacy: R_ℓ should be **minimized**,
- Storage: R_w should be **minimized**.

Motivations for Privacy Leakage Analysis

- **Security and Privacy are not the same!**
- The actions taken, e.g., computations, requests from a database, transactions, are related to **security**.
- Anything that leaks information about your identity is related to **privacy**.

Motivations for Privacy Leakage Analysis (Cont'd)

- For instance, one can make money transfer and every node in the network can obtain all the details of the transaction (e.g., the amount and time of the transaction), except the identity of the node who made the transfer. Then, **secrecy is fully leaked but privacy is preserved**.

- The **same biometric or physical identifier** can be used by **multiple applications**. Every time an application uses the same identifier output, some information has to be leaked about the noiseless source output although the secrecy leakage can be limited. **One can show that privacy leakage from an application might result in secrecy leakage for another application that uses the same identifier output.**

Generated-Secret (GS) Model

Definition

A key-leakage-storage rate tuple (R_s, R_ℓ, R_w) is achievable for the GS model with noiseless encoder measurement and noisy decoder measurements through the $P_{Y|X}$ if, given any $\delta > 0$, there is some blocklength $n \geq 1$, and an encoder and a decoder for which $R_\mathsf{s} = \dfrac{\log|\mathcal{S}|}{n}$ and

$$\Pr[S \neq \hat{S}] \leq \delta \qquad \text{(reliability)} \qquad (1)$$

$$I(S;W) \leq \delta \qquad \text{(strong secrecy)} \qquad (2)$$

$$\frac{1}{n} I(X^n;W) \leq R_\ell + \delta \qquad \text{(privacy)} \qquad (3)$$

$$\frac{1}{n} H(S) \geq R_\mathsf{s} - \delta \qquad \text{(key uniformity)} \qquad (4)$$

$$\frac{1}{n} \log|\mathcal{W}| \leq R_\mathsf{w} + \delta \qquad \text{(storage).} \qquad (5)$$

Key-Leakage-Storage Region for the GS Model

Theorem 1

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

$$\mathcal{R}_{\text{gs}} = \bigcup_{P_{U|X}} \Big\{ (R_s, R_\ell, R_w) :$$

$$0 \leq R_s \leq I(U;Y), \tag{6}$$

$$R_\ell \geq I(U;X) - I(U;Y), \tag{7}$$

$$R_w \geq I(U;X) - I(U;Y) \Big\}. \tag{8}$$

- Proof uses the output statistics of random binning (OSRB) method.

Key-Leakage-Storage Region for the CS Model

Theorem 2

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

$$\mathcal{R}_{\mathsf{cs}} = \bigcup_{P_{U|X}} \Big\{ (R_s, R_\ell, R_w) :$$

$$0 \leq R_s \leq I(U;Y), \tag{9}$$

$$R_\ell \geq I(U;X) - I(U;Y), \tag{10}$$

$$R_w \geq I(U;X) \Big\}. \tag{11}$$

- Proof uses the proof for the GS model in combination with a one-time padding step.

BSC Example

- Consider the binary symmetric source (BSS) P_X and binary symmetric channel (BSC) $P_{Y|X}$ such that

$$\Pr[X = 0] = 0.5 \tag{12}$$
$$\Pr[Y = 1|X = 0] = \Pr[Y = 0|X = 1] = p \text{ for some } 0 \le p < 0.5. \tag{13}$$

- An equivalent model is $Y = X \oplus Z$, where
  - X and Z are independent,
  - (12) is satisfied and Z is binary source with $\Pr[Z = 1] = p$.

- We will evaluate the key-leakage-storage region $\mathcal{R}_{\text{gs}}$ for this example.

BSC Example (Cont'd)

- The rate region $\mathcal{R}_{\text{gs}}$ requires us to maximize $I(U;Y)$ and minimize $I(U;X)$ **simultaneously**! This is an **information bottleneck problem.**
- Since X is binary and $P_{Y|X}$ is a BSC, we can use **Mrs. Gerber's lemma**.
- Define the *binary entropy function* $H_b(\cdot)$ as

$$H_b(p) = -p\log_2(p) - (1-p)\log_2(1-p) \tag{14}$$

with an inverse $H_b^{-1}(\cdot)$ that takes on values in $[0, 0.5]$ and define the *cyclic convolution operator* $*$ as

$$p * q = p(1-q) + (1-p)q = p(1-2q) + q. \tag{15}$$

BSC Example (Cont'd)

- The rate region $\mathcal{R}_{\text{gs}}$ requires us to maximize $I(U;Y)$ and minimize $I(U;X)$ **simultaneously**!
- This is equivalent to minimize $H(Y|U) = H(X \oplus Z|U)$ and maximize $H(X|U)$ **simultaneously**!
- Mrs. Gerber's lemma proves for any valid $H(X|U) \in [0,1]$ that

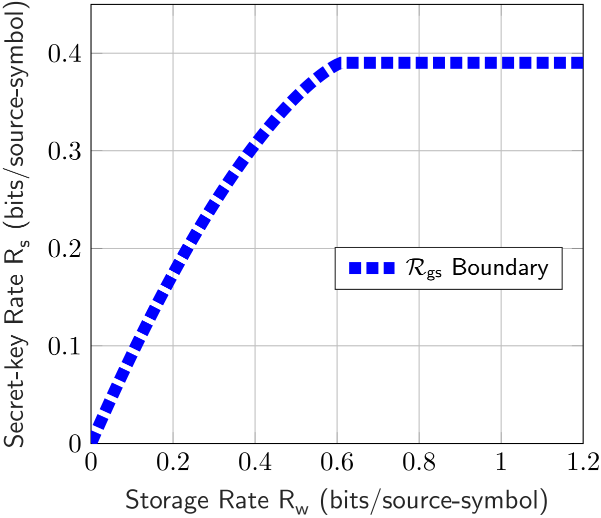
$$H(X \oplus Z|U) \geq H(p * H_b^{-1}(H(X|U))) \tag{16}$$

  with equality if $P_{X|U}$ is a BSC with crossover probability $H_b^{-1}(H(X|U))$.

- We therefore evaluate the key-leakage-storage region $\mathcal{R}_{\text{gs}}$ for this example by achieving the equality in Mrs. Gerber's lemma.

BSC Example (Cont'd)

Storage-key projection of $\mathcal{R}_{\text{gs}}$ for BSS $\mathrm{P}_{\mathbf{X}}$ and $\mathrm{P}_{\mathbf{Y}|\mathbf{X}}$ ∼BSC(0.15).

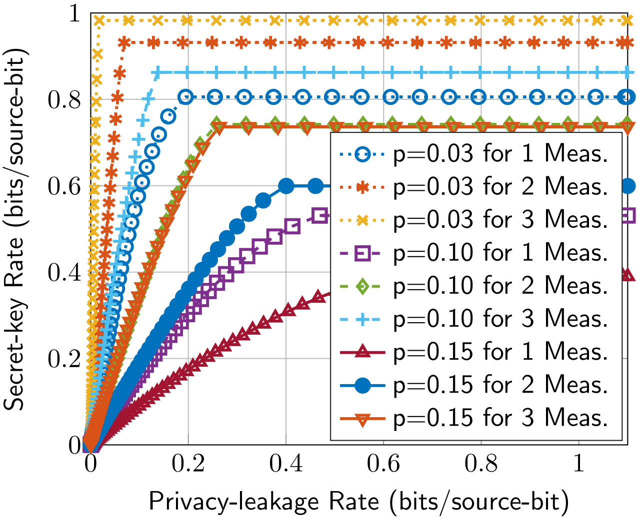


Multiple Measurements at the Decoder

- Mrs. Gerber's lemma extends to the case with M_D measurements at the decoder if the channel $P_{Y_1 Y_2 \cdots Y_{M_D}|X}$ is a **binary-input symmetric output** (BISO) channel, which can be decomposed into a mixture of BSCs.
- We now illustrate the gains from multiple measurements at the decoder through independent BSCs each with crossover probability p.
- Note that independent BSCs can be decomposed into BSCs, so Mrs. Gerber's lemma will be applied.

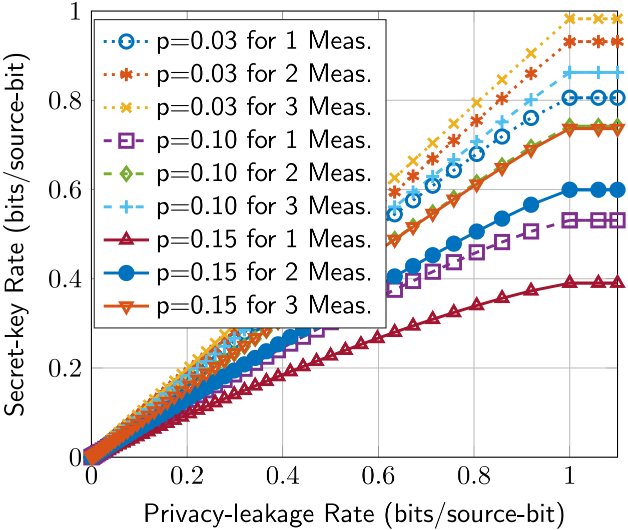
Multiple Measurements at the Decoder (Cont'd)

Leakage-key projection of $\mathcal{R}_{\mathbf{gs}}$ for $\mathbf{P_{Y_m|X}} \sim$ BSC$(\mathbf{p})$ for $\mathbf{m = 1, 2, \ldots, M_D}$.



Multiple Measurements at the Decoder (Cont'd)

Leakage-key projection of $\mathcal{R}_{\text{cs}}$ for $\mathbf{P_{Y_m|X}} \sim$ BSC$(\mathbf{p})$ for $\mathbf{m = 1, 2, \ldots, M_D}$.



Multiple Measurements at the Decoder (Cont'd)

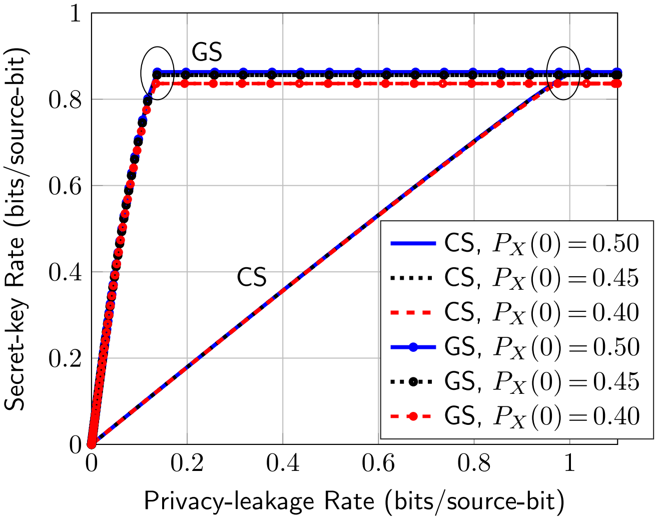
- Since the decoder sees M_D noisy versions $Y_{1:M_D}$ of the same source symbol X, it can "combine" the measurements to form a less noisy equivalent channel.
- This is entirely similar to using maximal ratio combining (MRC) to obtain a sufficient statistic about a symbol that is transmitted several times over an additive white Gaussian noise (AWGN) channel.
- The resulting gain may thus be interpreted as a **diversity gain**, in analogy to multiple-antenna wireless communication systems.

Effects of Bias in the Source Output

- We illustrate the effects of bias in the source outputs, i.e., $P_X(0) \neq 0.5$.
- If we decrease $P_X(0)$, then both $H(X)$ and $H(Y_{1:M_D})$ decrease, so we need to evaluate the limits to see the total effects of a bias..

Effects of Bias in the Source Output (Cont'd)

R_ℓ vs. R_s projection of the key-leakage-storage region $\mathcal{R}_\mathsf{gs}$ for $p = 0.10$, and $M_D = 3$

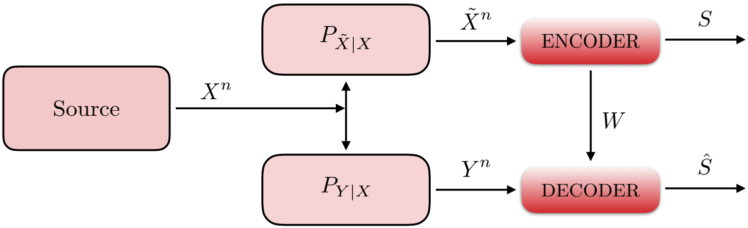


Effects of Bias in the Source Output (Cont'd)

- We can conclude that the effects of bias on the asymptotically achievable rate regions are not big if multiple measurements are considered at the decoder.

- The optimal code construction for the biased case is different than the optimal code construction for the uniform source output case, which **might increase the complexity of code construction and of the decoding** for the biased cases.

Hidden Source Model Extension



- Take *noisy enrollment* into account to model uncertainty about the source
  ➠ **Hidden source model (HSM)**
- Intuitions and Insights:
  - Every identifier measurement is noisy, including encoder measurements.
  - Two separate measurement channels model that the noise components on the encoder and decoder measurements are independent.
  - Multiple measurements at the encoder can be shown to be useful to enlarge the rate region.
  - The privacy leakage definition should be chosen carefully.

Hidden Source Model Extension (Cont'd)

Definition

A key-leakage-storage rate tuple (R_s, R_ℓ, R_w) is achievable for the hidden GS or CS model with noisy encoder and decoder measurements through $P_{\widetilde{X}|X}$ and $P_{Y|X}$, respectively, if given any $\delta > 0$ there is some blocklength $n \geq 1$, and an encoder and a decoder for which $R_{\mathsf{s}} = \dfrac{\log|\mathcal{S}|}{n}$ and

$$\Pr[S \neq \hat{S}] \leq \delta \qquad \text{(reliability)} \qquad (17)$$

$$I(S;W) \leq \delta \qquad \text{(strong secrecy)} \qquad (18)$$

$$\frac{1}{n} I(X^n; W) \leq R_\ell + \delta \qquad \text{(privacy)} \qquad (19)$$

$$\frac{1}{n} H(S) \geq R_{\mathsf{s}} - \delta \qquad \text{(key uniformity)} \qquad (20)$$

$$\frac{1}{n} \log|\mathcal{W}| \leq R_{\mathsf{w}} + \delta \qquad \text{(storage).} \qquad (21)$$

Rate Region for the Hidden GS Model

Theorem 3

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

$$\mathcal{R}_{\mathsf{hgs}} = \bigcup_{P_{U|\widetilde{X}}} \Big\{ (R_s, R_\ell, R_w) \colon$$

$$0 \le R_s \le I(U;Y),$$

$$R_\ell \ge I(U;X) - I(U;Y),$$

$$R_w \ge I(U;\widetilde{X}) - I(U;Y) \Big\}.$$

Rate Region for the Hidden CS Model

Theorem 4

The key-leakage-storage region for the hidden CS model is

$$\mathcal{R}_{\mathsf{hcs}} = \bigcup_{P_{U|\widetilde{X}}} \Big\{ (R_s, R_\ell, R_w) \colon$$
$$0 \leq R_s \leq I(U;Y),$$
$$R_\ell \geq I(U;X) - I(U;Y),$$
$$R_w \geq I(U;\widetilde{X}) \Big\}.$$

Hidden Source Example

- Suppose the binary sequence $\widetilde{X}^n$ corresponds to a **single noisy measurement of the binary hidden source** X^n at the encoder. Assume that the inverse channel $P_{X|\widetilde{X}}$ is a BSC, an assumption that is fulfilled if P_X is uniform and $P_{\widetilde{X}|X}$ is a BSC.
- Consider a **BISO channel** $P_{Y_{1:M_D}|X}$ with a binary input and M_D binary measurements as output, i.e., the channel has 2^{M_D} possible output symbols.
- We decompose the channel into $L = 2^{M_D - 1}$ BSCs to use the extension of Mrs. Gerber's lemma. We index these BSCs from 1 to L.
- Let $A = a$ represent the BSC index chosen by the channel and let p_a be the crossover probability of a-th subchannel.

Hidden Source Example (Cont'd)

- We now simplify the key-leakage-storage regions for the measurement channels $P_{\widetilde{X}|X}$ and $P_{Y_{1:M_D}|X}$ considered above so that a single parameter characterizes the regions.

Theorem 5

Suppose $P_{X|\widetilde{X}}$ is a BSC with crossover probability p, where $0 \leq p \leq 0.5$, and $P_{Y_{1:M_D}|X}$ is a mixture of BSCs. The boundary points of $\mathcal{R}_{\text{hgs}}$ and $\mathcal{R}_{\text{hcs}}$ are achieved by channels $P_{\widetilde{X}|U}$ that are BSCs.

Visible vs. Hidden Source Models

- We will illustrate **the problems occurring if one mistakenly models a hidden source as a visible source**, which is what the big part of the PUF industry is doing right now.
- We study the GS model with a hidden binary symmetric source (BSS).
- Suppose $P_{\widetilde{X}|X}$ is a BSC with crossover probability p_{E}. The inverse channel $P_{X|\widetilde{X}}$ is also a BSC with crossover probability p_{E} due to **source symmetry**.
- $P_{Y_{1:M_D}|X}$ consists of M_D independent BSCs each with crossover probability p_{D}.

Visible vs. Hidden Source Models (Cont'd)

- The encoder, e.g., a hardware manufacturer (for PUFs) or a trusted entity (for biometrics), models the source as visible or hidden, and a code is then constructed for the assumed model. Therefore, the assumed model determines the performance of the actual system.

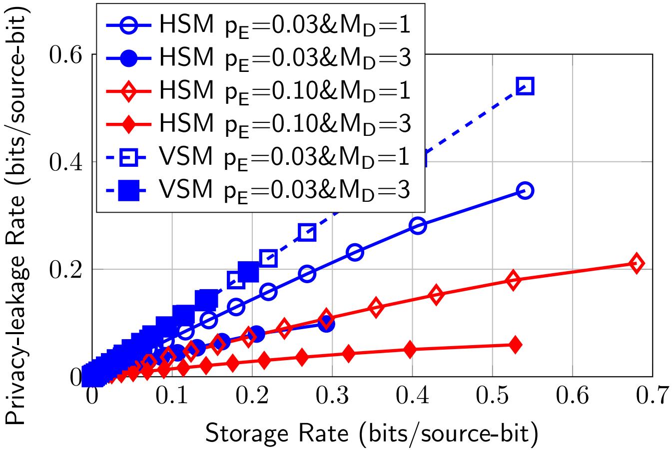
- We first illustrate that treating the hidden source model (HSM) as if it were a visible source model (VSM) might give pessimistic privacy-leakage rate results for $M_D \geq 1$ and over-optimistic secret-key and storage rate results for $M_D > 1$. The latter results in **unnoticed secrecy leakage** and **reduced reliability**.

Visible vs. Hidden Source Models (Cont'd)

- For the supposed VSM, $\widetilde{X}^n$ is mistakenly considered to be a noise-free source, i.e., $p_{\mathsf{E}}^{\mathsf{VSM}}\!=\!0$, and the corresponding decoder-output channel $P^{\mathsf{VSM}}_{Y_{1:M_D}|\widetilde{X}}$ consists of M_D independent BSCs each with crossover probability $p_{\mathsf{E}} * p_{\mathsf{D}}$ because $P_{Y|\widetilde{X}}$ is estimated from identifier measurements.
- However, the HSM considers an encoder measurement through a BSC with crossover probability p_{E} and M_D independent decoder measurements through BSCs, each with crossover probability p_D.
- Therefore, the HSM results in a conditional probability distribution $P_{Y_{1:M_D}|\widetilde{X}}$ that is different from the supposed VSM distribution $P^{\mathsf{VSM}}_{Y_{1:M_D}|\widetilde{X}}$ for $M_D\!>\!1$ and in a key-leakage-storage region $\mathcal{R}_{\mathsf{hgs}}$ that is different from the supposed VSM region $\mathcal{R}_{\mathsf{gs}}^{\mathsf{VSM}}$ for $M_D\!\geq\!1$.

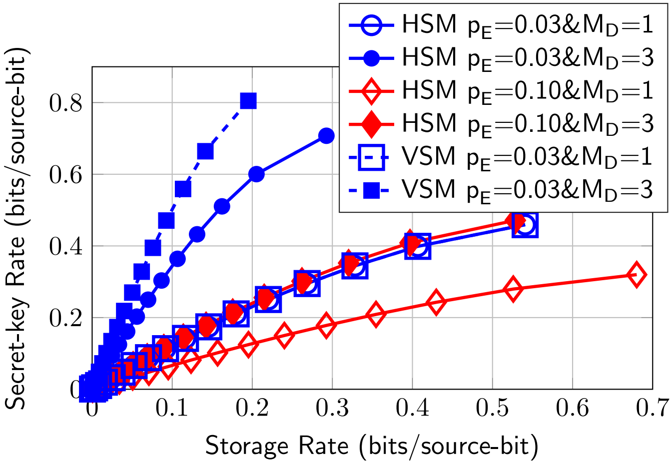
Visible vs. Hidden Source Models (Cont'd)

Storage-leakage projection of the boundary triples for the GS model with $p_{\mathbf{D}} = 0.10$.



Visible vs. Hidden Source Models (Cont'd)

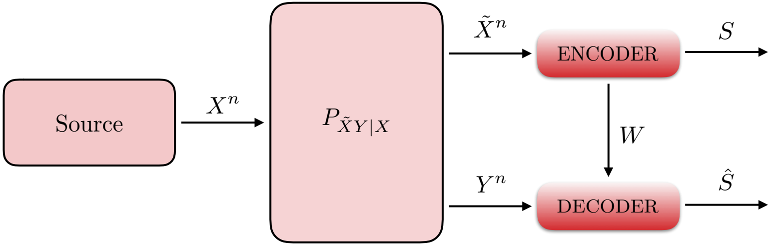
Storage-key projection of the boundary triples for the GS model with $p_{\mathbf{D}} = 0.10$.



Visible vs. Hidden Source Models (Cont'd)

- Figure on page 72 shows that
  - the supposed VSM gives pessimistic privacy-leakage rate results.
- Figure on page 73 shows that
  - The R_s^* of the HSM and supposed VSM are equal if $M_D = 1$, but the supposed VSM gives over-optimistic secret-key and storage rate results for $M_D > 1$.
- These comparisons show that designing a code for the supposed VSM can lead to substantial secrecy leakage and reliability reduction.

Further Model Extensions



- A broadcast channel (BC) $P_{\widetilde{X}Y|X}$ measurement models the correlation between the noise components on the encoder and decoder measurements.

Further Model Extensions (Cont'd)

- Introducing a **cost-constrained action sequence** A^n that is a function of the helper data W to control the quality, number, or reliability of the decoder measurement channel $P_{Y|XA}$ enlarges the key-leakage-storage(-cost) region.

- Similar to the BC model, we allow **correlation** between the noise components on the encoder and decoder measurements of the cost-constraint action dependent model above by considering a decoder measurement channel $P_{Y|X\widetilde{X}A}$ such that $\widetilde{X}^n$ is an additional input. This correlation possibly shrinks the key-leakage-storage-cost region.

Part III

Optimal Code Constructions for Key Agreement with PUFs

Main Discussions

- We discuss binning-based code constructions that are **Pareto optimal** and **improve on all** existing methods.

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

Existing Methods

- *Code-offset fuzzy extractors* (COFE) for the GS model,
- *Fuzzy-commitment scheme* (FCS) for the CS model,
- *Syndrome-based Polar Code Construction* 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** construction,
  - achieves only a single point on the region $\mathcal{R}_{\text{gs}}$ boundary.
- We now show that our Wyner-Ziv **(WZ)-coding** constructions are **Pareto optimal**.

WZ-coding with Random Linear Codes (RLCs)

Assume

- $X^n \sim \mathsf{Bern}^n\left(\frac{1}{2}\right)$,
- $P_{Y|X}$ is a **BSC with crossover probability** p_A.

WZ-coding with RLCs (Cont'd)

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

$$\mathbf{H} = \begin{bmatrix}\mathbf{H}_1\\ \mathbf{H}_2\end{bmatrix} \tag{22}$$

  - $\mathbf{H}_1 \in \{0,1\}^{m_1\times n}$ defines a binary linear code $\mathcal{C}_1$ with parameters $(n, n-m_1)$,
  - $\mathbf{H} \in \{0,1\}^{(m_1+m_2)\times n}$ 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., $\mathcal{C} \subseteq \mathcal{C}_1$.

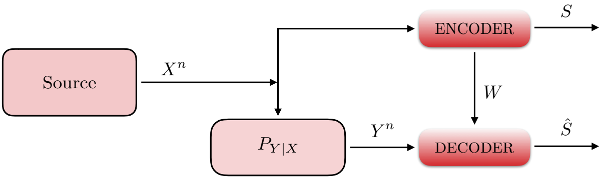
WZ-coding with RLCs (Cont'd)

- Impose the conditions, for some $q \in [0, 0.5]$ and $\delta > 0$,

$$\frac{k_1}{n} \triangleq \frac{n - m_1}{n} = 1 - H_b(q) + \delta, \tag{23}$$

$$\frac{k}{n} \triangleq \frac{n - m_1 - m_2}{n} = 1 - H_b(q * p_A) - \delta. \tag{24}$$

GS Model (Recall)



WZ-coding with RLCs (Cont'd)

Encoder:

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

$$X_q^n = \arg\min_{C^n \in \mathcal{C}_1} d_H(X^n, C^n) \tag{25}$$

  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)

Encoder (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)

Encoder (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)

Encoder (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)

Encoder (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)

Encoder (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)

Encoder (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)

Encoder (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)

Encoder (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)

Decoder:

- 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)

Decoder:

- 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)

Decoder:

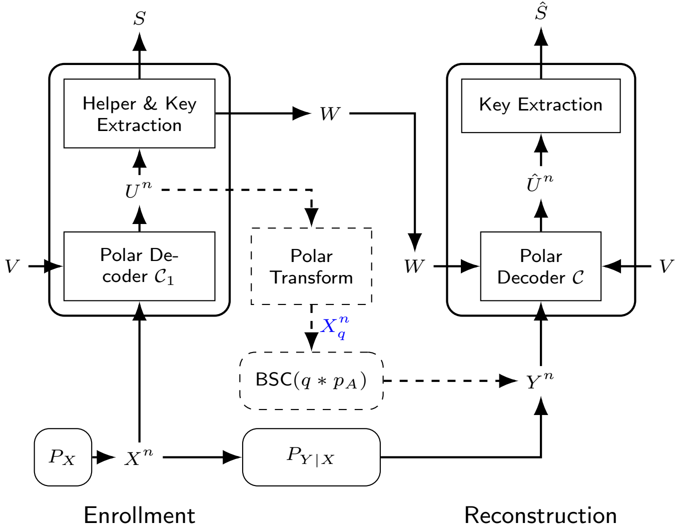
- The channel $P_{Y^n|X_q^n} \sim \text{Bern}^n(q * p_A)$ when $n \to \infty$,
- $\mathcal{C}$ **can correct errors in** $P_{Y^n|X_q^n}$ with high probability to estimate X_q^n,
- $\widehat{X}_q^n$ determines $\widehat{S}$.

WZ Polar Code Construction

Polar Codes

- A polar transform converts an input sequence U^n with frozen and unfrozen bits to a codeword X^n.
- Polar codes rely on **converting** the physical channel $P^n_{Y|X}$ **into virtual channels** $P_{Y^nU^{i-1}|U_i}$.
- Polar codes **achieve the symmetric capacity**, i.e., the highest rate achievable subject to using the input letters of the channel with equal probability, of a discrete memoryless channel.

WZ Polar Code Construction (Cont'd)



WZ Polar Code Construction (Cont'd)

- Use two polar codes $\mathcal{C}_1(n, \mathcal{F}_1, V)$ and $\mathcal{C}(n, \mathcal{F}, \overline{V})$ with $\mathcal{F} = \mathcal{F}_1 \cup \mathcal{F}_w$ and $\overline{V} = [V, W]$, where
  - V has length m_1,
  - W has length m_2,
  - m_1 and m_2 satisfy (23) and (24).

- The indices in $\mathcal{F}_1$ represent frozen channels with assigned values V for both codes and $\mathcal{C}$ has additional frozen channels with assigned values W denoted by $\mathcal{F}_w$, i.e., the codes are nested.

WZ Polar Code Construction (Cont'd)

- The code $\mathcal{C}_1$ serves as a VQ with a desired distortion q, and the code $\mathcal{C}$ serves as the error correcting code for a BSC($q * p_A$). The idea is to obtain W during enrollment and store it as public helper data.
- W is used by the decoder to estimate the secret key S of length $n - m_1 - m_2$.

WZ Polar Code Construction (Cont'd)

Construction of $\mathcal{C}$ and $\mathcal{C}_1$: Since $\mathcal{C} \subseteq \mathcal{C}_1$ are nested codes, they must be constructed jointly. For a given secret key size $n - m_1 - m_2$, block length n, crossover probability p_A, and target block-error probability $P_B = \Pr[S \neq \widehat{S}]$, we propose the following procedure.

1. Construct a polar code of rate $(n - m_1 - m_2)/n$ and use it as the code $\mathcal{C}$, i.e., define the set of frozen indices $\mathcal{F}$.

WZ Polar Code Construction (Cont'd)

2. Evaluate the error correction performance of $\mathcal{C}$ with a decoder for a BSC with a range of crossover probabilities to obtain the crossover probability p_c, resulting in a target block-error probability of P_B. Using $p_c = E[q] * p_A =$, we obtain the target distortion $E[q]$ averaged over a large number of realizations of X^n.

3. Find an $\mathcal{F}_1 \subset \mathcal{F}$ that results in an average distortion of $E[q]$ with a minimum possible amount of helper data. Use $\mathcal{F}_1$ as the frozen set of $\mathcal{C}_1$.

WZ Polar Code Construction (Cont'd)

1. Step 1 is a conventional polar code design task.

2. Step 2 is applied by Monte-Carlo simulations.

3. For step 3, we start with $\mathcal{F}_1^{'} = \mathcal{F}$ and compute the resulting average distortion $E[q']$ via Monte-Carlo simulations. If $E[q']$ is not less than $E[q]$, we remove elements from $\mathcal{F}_1^{'}$ according to the reliabilities of the polarized bit channels and repeat the procedure until we obtain the desired average distortion $E[q]$.

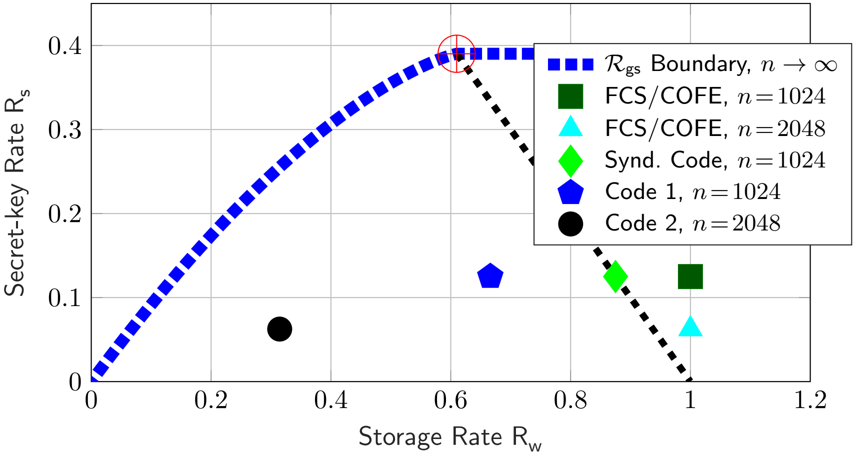
Rate-tuple Comparisons

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

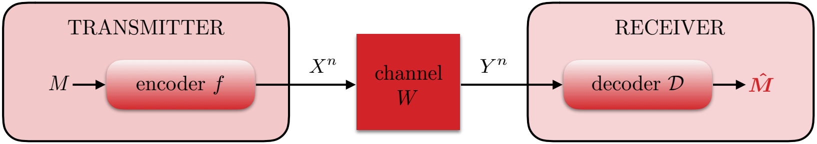
Rate-tuple Comparisons (Cont'd)



Part IV

Secure Identification with PUFs

Traditional Communication (Shannon Picture)



- Transmit a message $m \in \mathcal{M} := \{1, 2, ..., M_n\}$
- Block code with input alphabet $\mathcal{X} := \{0, 1, ..., q-1\}^n$
- Channel $W = \{W(y|x) : x \in \mathcal{X}, y \in \mathcal{Y}\}$ is a stochastic matrix
- Probability for receiving a sequence $y^n \in \mathcal{Y}^n$ when $x^n \in \mathcal{X}^n$ has been transmitted:

$$W^n(y^n|x^n) = \prod_{i=1}^{n} W(y_i|x_i)$$

- Recover the *exact message* $m \in \mathcal{M}$ with small decoding error

➠ Find the correct answer to *"What was the transmitted message?"*

Message Transmission Capacity

- Rate of the code is: $R = \frac{1}{n} \log |\mathcal{M}|$
- **Question:** What is the largest rate of (almost) error free message transmission?

The *message transmission capacity* $C(W)$ of a discrete memoryless channel (DMC) W is

$$\boldsymbol{C(W) = \max_{X} I(X;Y)}$$

➠ Size of message set is $|\mathcal{M}| = 2^{nC(W)}$ (exponential)

The Shannon picture is the theoretical framework for all existing communication, storage, and information processing systems!

Local Randomness

Deterministic code

A (deterministic) (n, M_n)-code for W is a set of pairs $\{(x_i^n, \mathcal{D}_i) : i \in \mathcal{M}\}$ with

- Codewords $x_i^n \in \mathcal{X}^n$ for all $i \in \mathcal{M}$
- Disjoint decoding sets $\mathcal{D} \subset \mathcal{Y}^n$ with $\mathcal{D}_i \cap \mathcal{D}_j = \emptyset$ for all $i, j \in \mathcal{M}$, $i \neq j$
- Probability of error $W^n(\mathcal{D}_i | x_i^n) \geq 1 - \lambda$ for all $i \in \mathcal{M}$

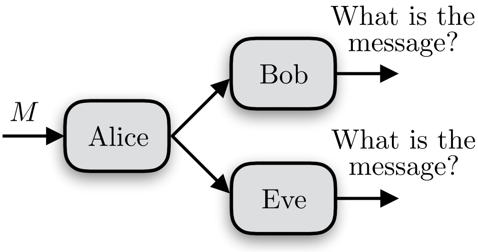
Randomized code

A randomized (n, M_n)-code for W is a set of pairs $\{(Q(\cdot|i)^n, \mathcal{D}_i) : i \in \mathcal{M}\}$ with

- Probability distributions $Q(\cdot|i) \in \mathcal{P}(\mathcal{X}^n)$ for all $i \in \mathcal{M}$
- Disjoint decoding sets $\mathcal{D} \subset \mathcal{Y}^n$ with $\mathcal{D}_i \cap \mathcal{D}_j = \emptyset$ for all $i, j \in \mathcal{M}$, $i \neq j$
- Probability of error $\sum_{x^n \in \mathcal{X}^n} W^n(\mathcal{D}_i | x^n) Q(x^n | i) \geq 1 - \lambda$ for all $i \in \mathcal{M}$

➠ **No** gain in performance with local randomness for traditional message transmission!

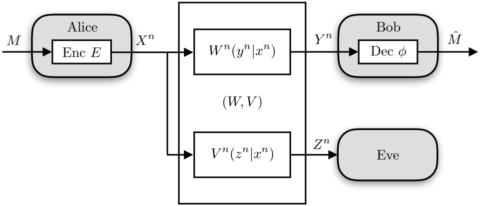
Physical Layer Security



Goal:

- Alice has to transmit a message to the legitimate receiver Bob
- Bob has to decode the correct message with small decoding error
- on legitimate receiver Eve is not able to decode the message

Secrecy Capacity



- What is the largest rate of (almost) error free secure message transmission?

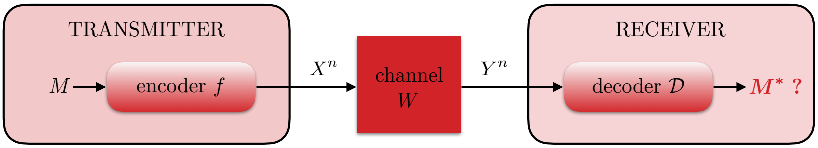
The *secure message transmission capacity* $C_S(W,V)$ of a discrete memoryless channel (DMC) W is

$$\boldsymbol{C_S(W,V) = \max_{U - X - (Y,Z)} [I(U;Y) - I(U;Z)]}$$

➠ Size of message set is $|\mathcal{M}| = 2^{nC_S(W)}$ (exponential)

Here randomized encoding is necessary and, accordingly, local randomness is crucial!

A New Communication Paradigm



- New applications are practical use-driven, e.g., Industry 4.0, V2X, V2V, ...
  $\Rightarrow$ *Identification task*
- Transmit a message $m \in \mathcal{N}$ (transmitter has no knowledge about the message of interest m^*)

➠ Identify if a *particular message* $m^* \in \mathcal{N}$ *of interest* has been sent

➠ Find the correct answer to *"Was the transmitted message m^* or not?"*

Identification Capacity

- **Question:** What is the largest rate of (almost) error free identification?

The *identification capacity* $C_{\mathsf{ID}}(W)$ of a discrete memoryless channel (DMC) W is

$$\boldsymbol{C_{\mathsf{ID}} = \max_{X} I(X;Y) = \max_{P_X} I(P_X, W) = C(W)}$$

➠ **Size of message set is $|\mathcal{N}| = 2^{2^{nC(W)}}$ (double-exponential)**

- Randomized encoding / local randomness is necessary

➠ Otherwise, $|\mathcal{N}| = 2^{nC(W)}$ only

Identification Code

Identification Code

A randomized (n, N_n)-identification code for W is a set of pairs $\{(Q_i^n, \mathcal{D}_i) : i \in \mathcal{N}\}$ with

- Probability distributions $Q_i \in \mathcal{P}(\mathcal{X}^n)$ for all $i \in \mathcal{N}$
- Decoding sets $\mathcal{D} \subset \mathcal{Y}^n$ for all $i \in \mathcal{N}$ (not necessarily disjoint!)

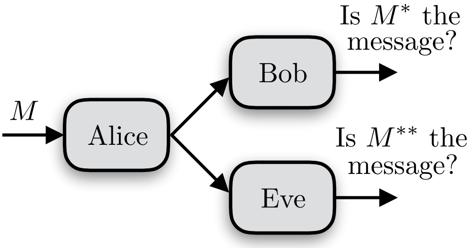
and with errors of first and second kind as

$$\sum_{x^n \in \mathcal{X}^n} Q_i(x^n) W^n(\mathcal{D}_i | x^n) \geq 1 - \lambda_1 \quad \text{for all } i \in \mathcal{N}$$

$$\sum_{x^n \in \mathcal{X}^n} Q_j(x^n) W^n(\mathcal{D}_i | x^n) \leq \lambda_2 \quad \text{for all } i, j \in \mathcal{N} \text{ with } i \neq j$$

➠ The receiver who is interested in message i will decide that his message was transmitted if and only if the received channel output y^n is in $\mathcal{D}_i$, otherwise he will deny that message i was sent

Physical Layer Security and Identification



- New approach: embedded security and identification

Goal:

- Alice has to transmit a message to the legitimate receiver Bob
- Bob is interested in message m', and he has to decide "m' is transmitted or not?"
- Alice has no knowledge about m'
- Non-legitimate receiver Eve is not able to identify any message

Secure Identification

The *secure identification capacity* $C_{S,\text{ID}}(W,V)$ of a discrete memoryless channel (DMC) W is

$$C_{S,\text{ID}}(W,V) = \begin{cases} C(W) & \text{if } C_S(W,V) > 0 \\ 0 & \text{otherwise} \end{cases}$$

with $C(W)$ the traditional message transmission capacity and $C_S(W,V)$ the traditional secure message transmission capacity.

➠ **Size of message set is $|\mathcal{N}| = 2^{2^{nC(W)}}$ (double-exponential)**

Here randomized encoding is necessary and, accordingly, local randomness is crucial!

Secure Identification Code

Secure Identification Code

A randomized (n, N_n)-secure identification code for (W, V) is a set of pairs $\{(Q_i^n, \mathcal{D}_i) : i \in \mathcal{N}\}$ with

- Probability distributions $Q_i \in \mathcal{P}(\mathcal{X}^n)$ for all $i \in \mathcal{N}$
- Decoding sets $\mathcal{D} \subset \mathcal{Y}^n$ for all $i \in \mathcal{N}$ (not necessarily disjoint!)

and with errors of first and second kind as

$$\sum_{x^n \in \mathcal{X}^n} Q_i(x^n) W^n(\mathcal{D}_i | x^n) \geq 1 - \lambda_1 \quad \text{for all } i \in \mathcal{N}$$

$$\sum_{x^n \in \mathcal{X}^n} Q_j(x^n) W^n(\mathcal{D}_i | x^n) \leq \lambda_2 \quad \text{for all } i, j \in \mathcal{N} \text{ with } i \neq j$$

and secrecy

$$\sum_{x^n \in \mathcal{X}^n} Q_j(x^n) V^n(\mathcal{E} | x^n) + \sum_{x^n \in \mathcal{X}^n} Q_i(x^n) V^n(\mathcal{E}^c | x^n) \geq 1 - \lambda_E$$

for any pair (i, j) with $i \neq j$ and any $\mathcal{E} \subset \mathcal{Z}^n$.

Comparison

Transmission – Shannon Picture

Sender chooses and sends
$m \in \mathcal{M} = \{1, 2, \dots, 2^{nC}\}$

channel

Receiver's goal:
What was the message?

Identification – New Paradigm

Sender chooses and sends
$m \in \mathcal{N} = \{1, 2, \dots, \mathbf{2^{2^{nC}}}\}$
local randomness

channel

Receiver's goal:
Was the message m^* or not?

➠ **Exponential performance increase!**

Security - New Quality

Transmission – Shannon Picture

Sender chooses and sends
$m \in \mathcal{M} = \{1, 2, \dots, 2^{nC_S}\}$
$C_S = \max I(U;Y) - I(U;Z)$
local randomness

channel

Wiretapper's goal:
What was the message?

Receiver's goal:
What was the message?

Identification – New Paradigm

Sender chooses and sends
$m \in \mathcal{N} = \{1, 2, \dots, \mathbf{2^{2^{nC}}}\}$
$C = \max I(X;Y)$, if $C_S > 0$
local randomness

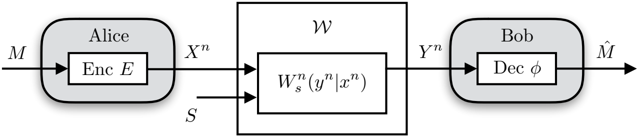
channel

Wiretapper's goal:
Was the message m^{**} or not?

Receiver's goal:
Was the message m^{*} or not?

➠ **Exponential performance increase and we pay no price for security!**

Detour: Robust Message Transmission



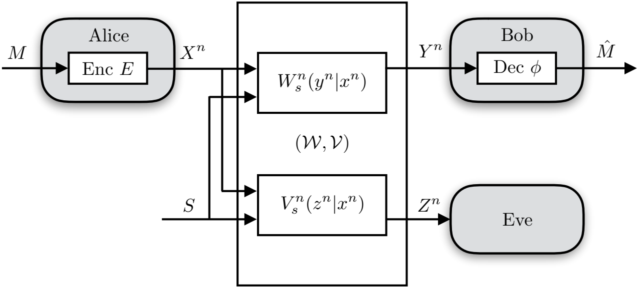
- Uncertainty is modeled by a set of channels $\mathcal{S}$
- Set $\mathcal{S}$ is known, but not the actual realization $s \in \mathcal{S}$
- Channel realization remains constant

➠ Concept of *compound channels*

The *message transmission capacity* $C(\mathcal{W})$ of a compound channel (CC) $\mathcal{W}$ is

$$C(\mathcal{W}) = \max_{X} \min_{s \in \mathcal{S}} I(X; Y_s)$$

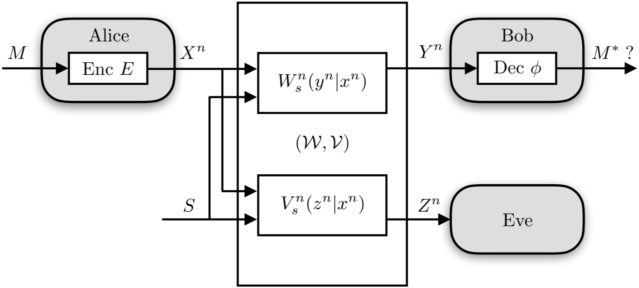
Robust and Secure Message Transmission



The *secure message transmission capacity* $C_S(\mathcal{W},\mathcal{V})$ of a compound wiretap channel (CWC) $(\mathcal{W},\mathcal{V})$ is

$$C_S(\mathcal{W},\mathcal{V}) = \lim_{n\to\infty} \frac{1}{n} \max_{U - X^n - (Y_s^n, Z_s^n)} \Big[\min_{s\in\mathcal{S}} I(U;Y_s^n) - \max_{s\in\mathcal{S}} I(U;Z_s^n) \Big]$$

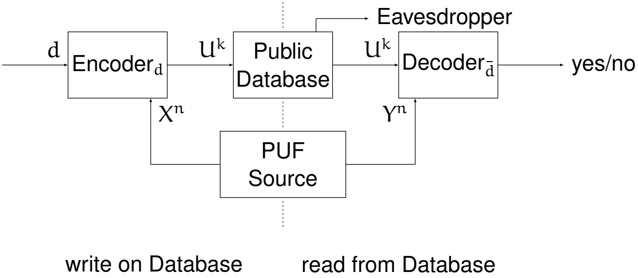
Secure and Robust Identification



The *secure identification capacity* $C_{S,\text{ID}}(\mathcal{W},\mathcal{V})$ of a compound wiretap channel (CWC) $(\mathcal{W},\mathcal{V})$ is

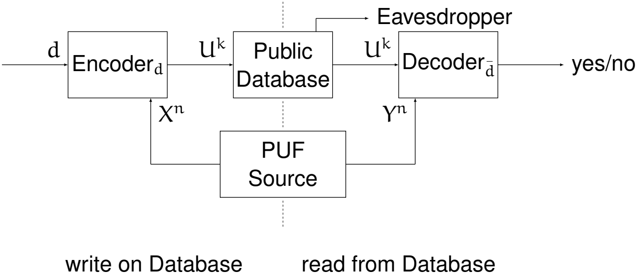
$$C_{S,\text{ID}}(\mathcal{W},\mathcal{V}) = \begin{cases} 0 & \text{if } C_S(\mathcal{W},\mathcal{V}) = 0 \\ C(\mathcal{W}) & \text{if } C_S(\mathcal{W},\mathcal{V}) > 0 \end{cases}$$

Secure Storage for Identification



- Store messages in a public database for identification
- A PUF source is available as additional resource

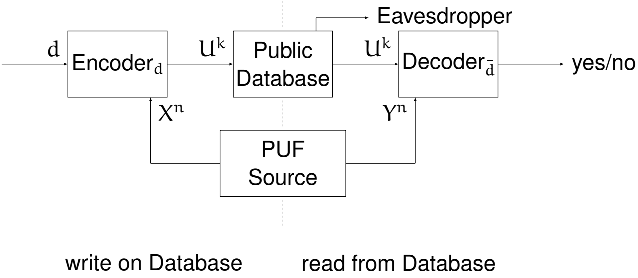
Secure Storage Protocol



We require

- $\mathbb{P}\{\mathsf{Dec}_d(\mathsf{Enc}_d(X^n), Y^n) = 0\} \leq \delta$
- $\mathbb{P}\{\mathsf{Dec}_d(\mathsf{Enc}_{\bar{d}}(X^n), Y^n) = 1\} \leq \delta$
- $\mathbb{P}\{\mathsf{Dec}_d^E(\mathsf{Enc}_d(X^n)) = 0\} + \mathbb{P}\{\mathsf{Dec}_d^E(\mathsf{Enc}_{\bar{d}}(X^n)) = 1\} \geq 1 - \delta$
- $\dfrac{1}{n} I(\mathsf{Enc}_d(X^n); X^n) \leq R_{PL} + \delta$

Achievable Rate Region



Achievable rate region for secure storage protocols is given by

$$\mathcal{R} = \bigcup_{V-X-Y} \Big\{ (R_{ID}, R_{PL}) : 0 \leq R_{ID} \leq I(V;X), R_{PL} \geq I(V;X) - I(V;Y) \Big\}$$

Thank you for your attention!

Bundesministerium
für Bildung
und Forschung

supported by "*NewCom - Post Shannon Communication*"

Main References

- **B. Gassend**, “Physical random functions,” *Master’s thesis*, M.I.T., Cambridge, MA, Jan. 2003.
- **R. Pappu**, “Physical one-way functions,” *Ph.D. dissertation*, M.I.T., Cambridge, MA, Oct. 2001.
- **R. Ahlswede and I. Csiszar**, “Common randomness in information theory and cryptography - Part I: Secret sharing,” *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121-1132, July 1993.
- **U. M. Maurer**, “Secret key agreement by public discussion from common information,” *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 2733-742, May 1993.
- **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.
- **T. Ignatenko and F. M. J. Willems**, “Biometric systems: Privacy and secrecy aspects,” *IEEE Trans. Inf. Forensics Security*, vol. 4, no. 4, pp. 956–973, Dec. 2009.
- **O. Günlü, T. Kernetzky, O. Iscan, V. Sidorenko, G. Kramer, and R. F. Schaefer**, “Secure and reliable key agreement with physical unclonable functions,” Entropy, vol. 20, no. 5, May 2018.
- **I. Csiszar and P. Narayan**, “Common randomness and secret key generation with a helper,” *IEEE Trans. Inf. Theory*, vol. 46, no. 2, pp. 344-366, Mar. 2000.
- **A. E. Gamal and Y.-H. Kim**, *Network Information Theory*. Cambridge, U.K.: Cambridge Uni. Press, 2011.
- **A. D. Wyner and J. Ziv**, “A theorem on the entropy of certain binary sequences and applications: Part I” *IEEE Trans. Inf. Theory*, vol. 19, no. 6, pp. 769–772, Nov. 1973.
- **O. Günlü, O. Iscan, and G.Kramer**, “Reliable secret key generation from physical unclonable functions under varying environmental conditions,” in *IEEE Int. Workshop Inf. Forensics Security*, Rome, Italy, Nov. 2015, pp. 1–6.
- **A. Maiti, J. Casarona, L. McHale, and P. Schaumont**, “A large scale characterization of RO-PUF,” in *IEEE Int. Symp. Hardware-Oriented Security Trust*, Anaheim, CA, June 2010, pp. 94-99.
- **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.
- **M. H. Yassaee, M. R. Aref, and A. Gohari**, “Achievability proof via output statistics of random binning,” *IEEE Trans. Inf. Theory*, vol. 60, no. 11, pp. 6760-6786, Nov. 2014.

Main References (2)

- **M. Bloch**, *Lecture Notes in Information-Theoretic Security*. Atlanta, GA: Georgia Inst. Technol., July 2018.
- **D. Slepian and J. Wolf**, "Noiseless coding of correlated information sources," *IEEE Trans. Inf. Theory*, vol. 19, no. 4, pp. 471-480, July 1973.
- **O. Günlü, O. Iscan, V. Sidorenko, and G. Kramer**, "Code constructions for physical unclonable functions and biometric secrecy systems," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 11, pp. 2848–2858, Nov. 2019.
- **S. Shamai, S. Verdu, and R. Zamir**, "Systematic lossy source/channel coding," *IEEE Trans. Inf. Theory*, vol. 44, no. 2, pp. 564-579, Mar. 1998.
- **A. Juels and M. Wattenberg**, "A fuzzy commitment scheme," in *ACM Conf. Comp. Commun. Security*, New York, NY, Nov. 1999, pp. 28-36.
- **T. Ignatenko and F. M. J. Willems**, "Information leakage in fuzzy commitment schemes," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 2, pp. 337–348, Mar. 2010.
- **U. Maurer and S. Wolf**, "Information-theoretic key agreement: From weak to strong secrecy for free," in *Int. Conf. Theory Appl. Cryptographic Techn.*, Bruges, Belgium, May 2000, pp. 351–368.
- **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.
- **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.
- **S. Lin and D. J. Costello**, *Error control coding*. Englewood Cliffs, NJ, USA: Prentice- Hall, May 2004.
- **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.
- **R. G. Gallager**, *Low-Density Parity-Check Codes*. Cambridge, MA, USA: M.I.T. Press, 1963.
- **B. Chen, T. Ignatenko, F. M. Willems, R. Maes, E. van der Sluis, and G. Selimis**, "A robust SRAM-PUF key generation scheme based on polar codes," in *IEEE Global Commun. Conf.*, Singapore, Dec. 2017, pp. 1-6.

Main References (3)

- **R. Ahlswede and G. Dueck**, "Identification via channels," *IEEE Trans. Inf. Theory*, vol. 35, no. 1, pp. 15-29, Jan. 1989.
- **H. Boche and C. Deppe**, "Secure identification for wiretap channels; robustness, super-additivity and continuity," *IEEE Trans. Forensics Security*, vol. 13, no. 7, pp. 1641-1655, Jul. 2018.
- **R. Ahlswede and Z. Zhang**, "New directions in the theory of identification via channels," *IEEE Trans. Inf. Theory*, vol. 41, no. 4, pp. 1040-1050, Jul. 1995.
- **D. Blackwell, L. Breiman, and A. J. Thomasian**, "The capacity of a class of channels," *Ann. Math. Stat.*, vol. 30, no. 4, pp. 1229–1241, Dec. 1959.
- **I. Bjelakovic, H. Boche, and J. Sommerfeld**, "Secrecy results for compound wiretap channels," *Probl. Inf. Transmission*, vol. 49, no. 1, pp. 73–98, Mar. 2013.
- **I. Csiszar and P. Narayan**, "The capacity of the arbitrarily varying channel revisited: Positivity, constraints," *IEEE Trans. Inf. Theory*, vol. 34, no. 2, pp. 181–193, Mar. 1988.
- **H. Boche and C. Deppe**, "Secure identification under passive eavesdroppers and active jamming attacks," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 2, pp. 472–485, Feb. 2019.
- **S. Baur, C. Deppe, and H. Boche**, "Secure Storage for Identification; Random Resources and Privacy Leakage," *IEEE Trans. Forensics Security*, vol. 14, no. 8, pp. 2013-2027, Aug. 2019.