Key Agreement with Physical Unclonable Functions

Onur Günlü
Joint work with Bernhard Geiger and Gerhard Kramer

onur.gunlu@tum.de

July 2018
TUM-Eurecom Workshop on Secure Communications

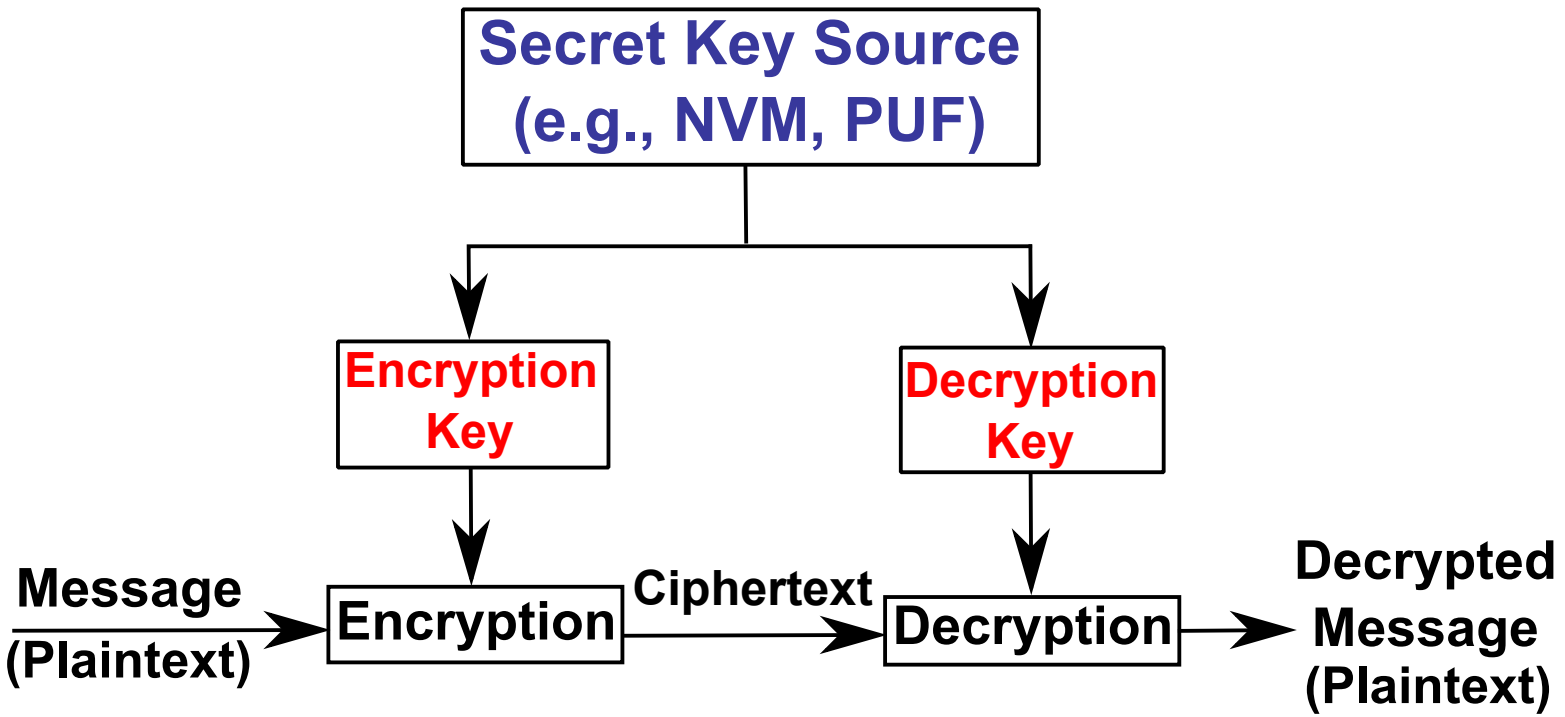
Motivation

- Secure secret-key storage and execution in hardware are not trivial due to
  - non-random key generation,
  - possible physical access to the storage medium,
  - information leakage via side channels.
- Alternative: physical identifiers 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.

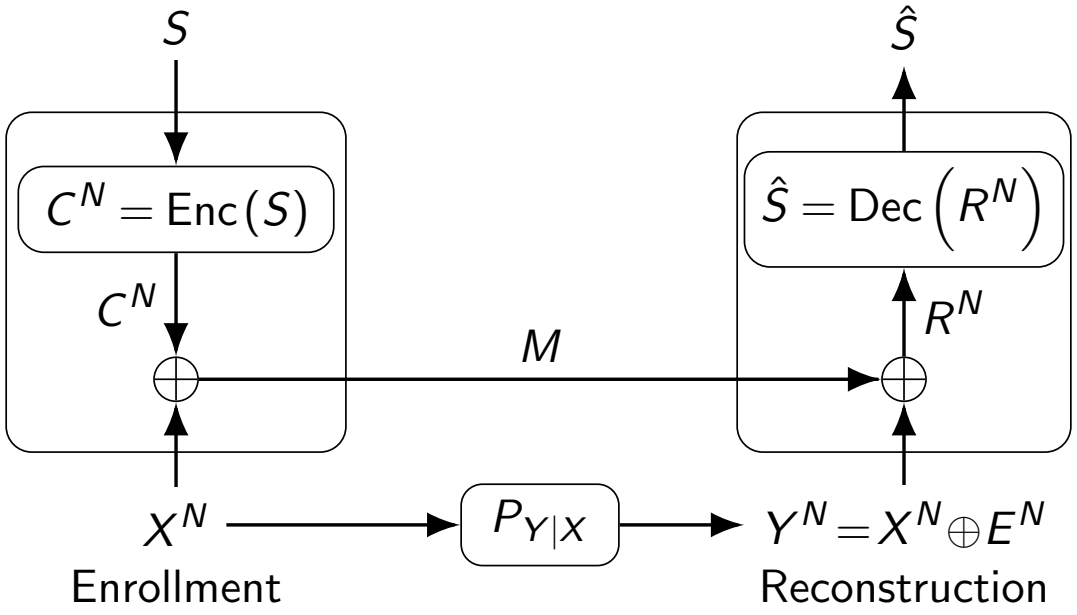
Motivation (cont'd)

- **Physical Unclonable Functions (PUF)**

NVM= Non-Volatile Memory

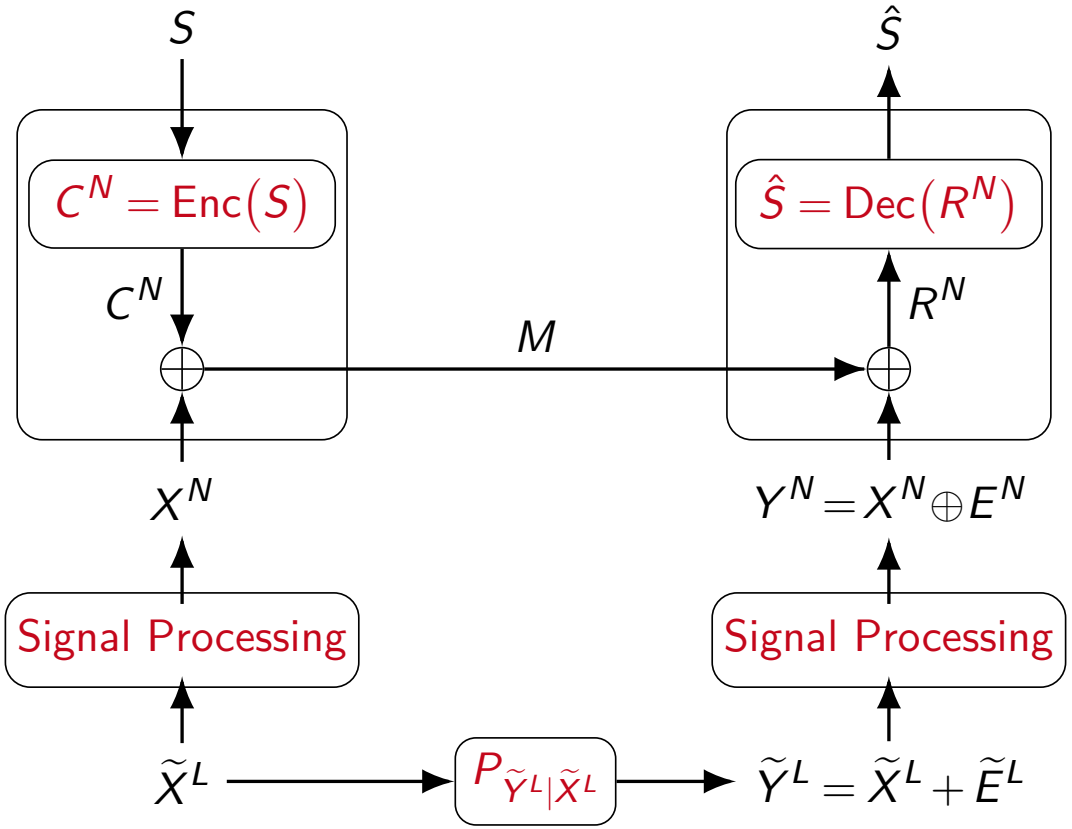


Fuzzy Commitment Scheme



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

Main Contributions

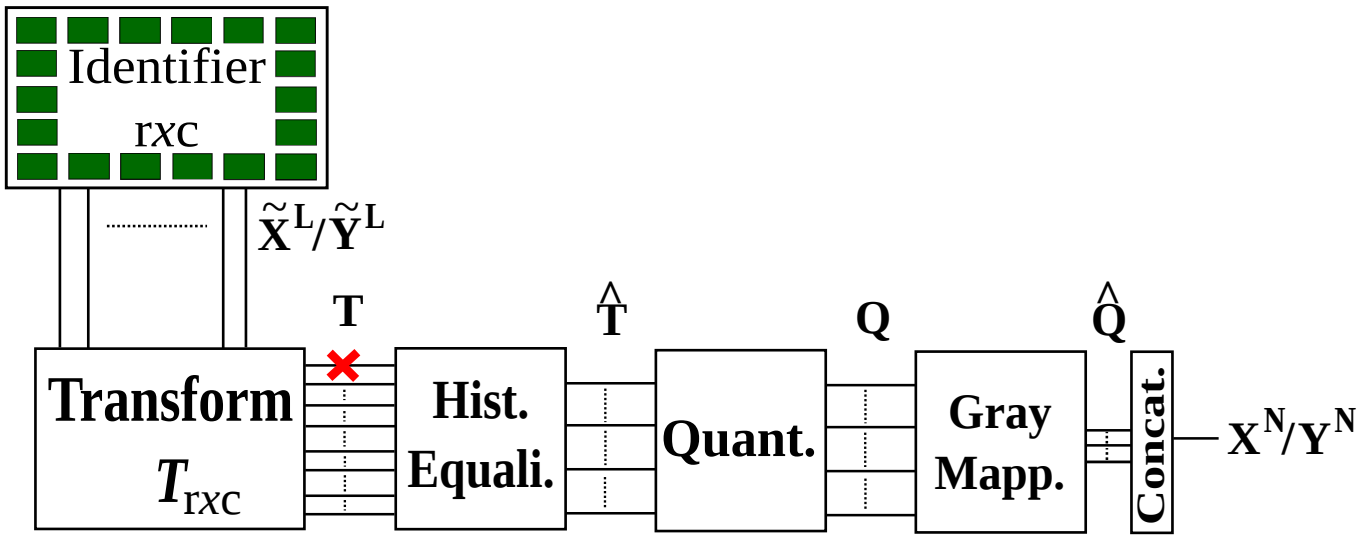


- *Block error probability* should satisfy $P_B \leq 10^{-9}$.

Enc and Dec

- 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 $e = \left\lfloor \frac{d-1}{2} \right\rfloor$ errors.

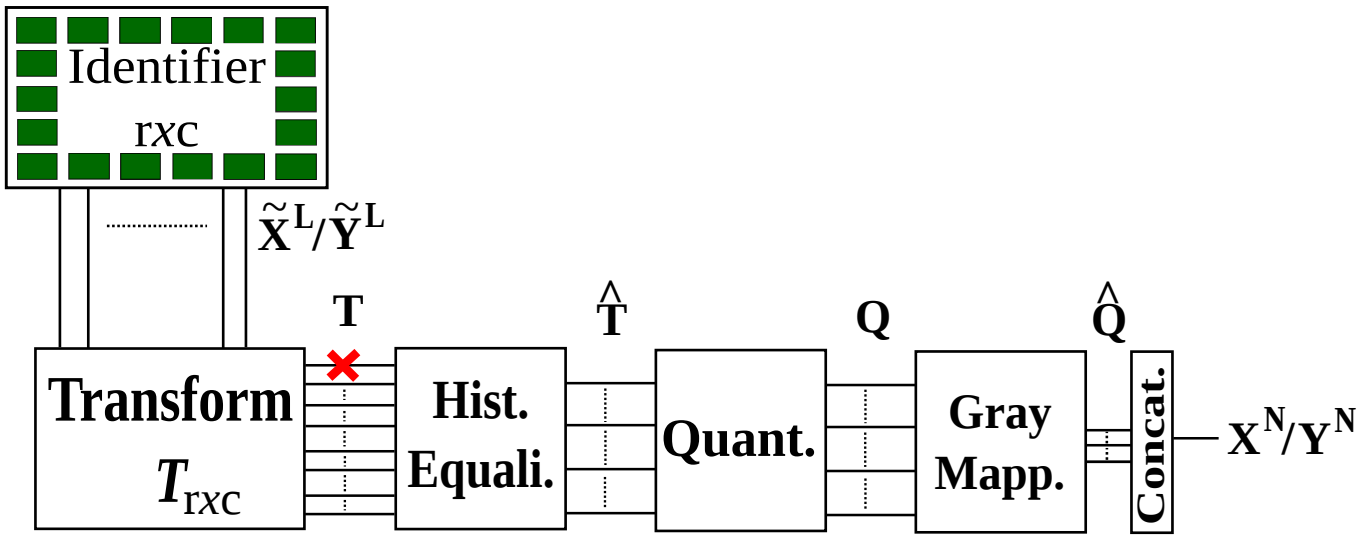
Signal Processing Steps



- Apply a transform $T_{r\times c}(\cdot)$ to decorrelate $\tilde{X}^L$,
- 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

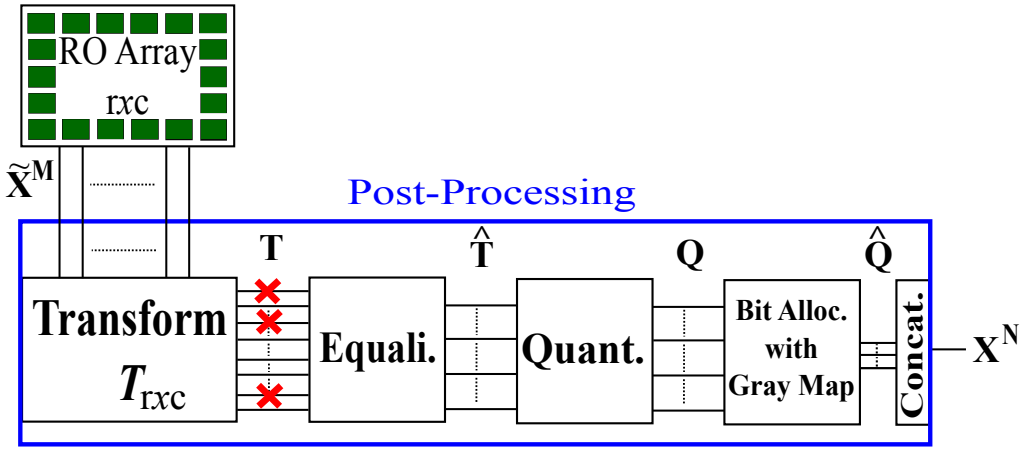
$$D_i(L) = \frac{1}{L} \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} \left(\sum_{l=1}^{2^L} \Pr[Q(\hat{t}+\hat{n}) = l] \mathrm{HD}_l(\hat{t}) \right) \cdot p_{\widehat{T}_i}(\hat{t}) p_{\widehat{N}_i}(\hat{n}) \mathrm{d}\hat{t} \mathrm{d}\hat{n}$$

- 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 $k \geq 128$ bits;
  - Code rate is at its maximum;
  - Extracted bit sequence X^N is independent and identically distributed (i.i.d.) according to $Ber(\frac{1}{2})$;
  - 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**!)

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

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

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

Code-based Quantizer Design (cont'd)

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

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

- 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 $d \geq 2e+1 \geq 2\left(\sum_{i=1}^{C_{\max}} K_i\right)+1$.

Ring Oscillator Dataset

- We use a public dataset[1] 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.

[1] A. Maiti, J. Casarona, L. McHale, and P. Schaumont, A large scale characterization of RO-PUF, in *IEEE Int. Symp. on Hardware-Oriented Security and Trust*, Anaheim, CA, USA, June 2010, pp. 94-99.

Code-based Quantizer Design for Ring Oscillators

C_{max}	16	17	18	19	20
$\bar{P}_c$					
K_{max}					
N					
e					

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

Code-based Quantizer Design for Ring Oscillators

C_{max}	16	17	18	19	20
$\bar{P}_c$	0.9902				
K_{max}					
N					
e					

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

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

Code-based Quantizer Design for Ring Oscillators

$\mathbf{C_{max}}$	**16**	**17**	**18**	**19**	**20**
$\bar{P}_c$	0.9902				
$K_{\max}$	3				
N					
e					

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

Code-based Quantizer Design for Ring Oscillators

$\mathbf{C_{max}}$	**16**	**17**	**18**	**19**	**20**
$\bar{P}_c$	0.9902				
$K_{\max}$	3				
N	144				
e					

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

Code-based Quantizer Design for Ring Oscillators

C_{max}	16	17	18	19	20
$\bar{P}_c$	0.9902				
K_{max}	3				
N	144				
e	18				

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

Code-based Quantizer Design for Ring Oscillators

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 $[N(C_{max}), e(C_{max})]$ 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 $\mathbf{e = C_{max} = 20}$!
- Choose the binary BCH code with
  - blocklength $n = 255$,
  - dimension $k = 131$,
  - minimum distance $d = 2e_{\mathrm{BCH}} + 1 = 2 \times 18 + 1$.
- $e_{\mathrm{BCH}} = 18$ 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

- We 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*.

Outlook

- 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 have separately proposed **the first optimal code construction** for PUFs and biometrics with privacy preservation. This construction improves on all previous schemes.

Outlook

- 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 have separately proposed **the first optimal code construction** for PUFs and biometrics with privacy preservation. This construction improves on all previous schemes.

THANK YOU