Reliable Secret-key Binding for Physical Unclonable Functions with Transform Coding

Onur Günlü, Onurcan İşcan, Vladimir Sidorenko, and Gerhard Kramer
{onur.gunlu, vladimir.sidorenko, gerhard.kramer}@tum.de, onurcan.iscan@huawei.com

Motivation

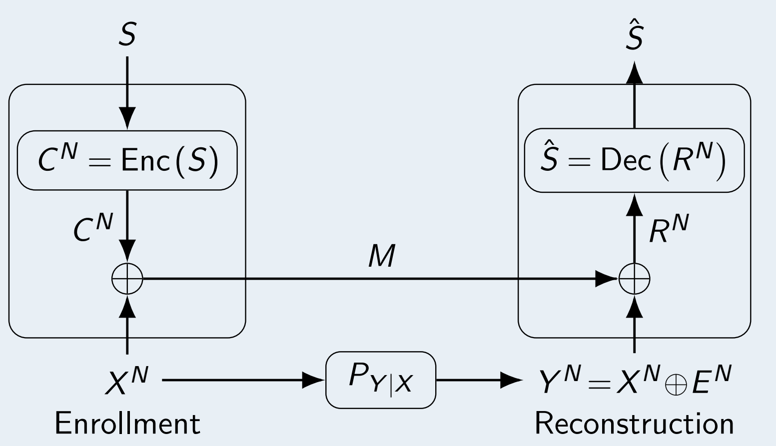
- Physical identifiers are secure and cheap alternatives to storing secret keys in non-volatile memory.
- Fine variations of ring oscillator (RO) outputs are used as a random stationary ergodic source with high entropy.
- Information-theoretic limits for a "key-binding" (chosen-secret) scheme, which uses identifier outputs to hide a secret key from an attacker, are used to evaluate our proposed approaches.
- The discrete cosine transform (DCT) based transform-coding approach is shown in [1] to improve RO reliability under varying environmental conditions.

Main Contributions

- Our **extended transform-coding** approach jointly improves
  - Decorrelation efficiency,
  - Maximum secret-key length,
  - Reliability and security of the extracted sequence,
  - Hardware cost performance.
- Design the **transform-coding** approach and **channel codes** for the *fuzzy commitment scheme* with realistic assumptions, i.e.,
  - Highly correlated RO outputs,
  - Maximum block-error probability of $P_B \leq 10^{-9}$.
- The (secret-key, privacy-leakage) rate pairs for our codes
  - $(0.1473, 0.8527)$ and $(0.1719, 0.8281)$ bits/source-symbol

  are better than all previously suggested codes, e.g.,
  - $(0.0782, 0.9218)$ [2], $(0.115, 0.885)$ [3], and $(0.1260, 0.8740)$ [3] bits/source-symbol.

System Model and Fuzzy Commitment Scheme



Consider **before transform coding**

- A two-dimensional RO array of size $L = r \times c$ and the output vector random variable $\widetilde{X}^L \sim p_{\widetilde{X}^L}$,
- Additive white Gaussian noise components $\widetilde{Z}^L \sim p_{\widetilde{Z}^L}$,
- Noisy RO outputs $\widetilde{Y}^L = \widetilde{X}^L + \widetilde{Z}^L$

so that **after transform coding** we obtain

- independent and identically distributed binary and uniformly distributed random vectors (X^N, Y^N),
- a binary error vector as $E^N = X^N \oplus Y^N$, where $E_i \sim Bern(p)$ for $i = 1, 2, \ldots, N$.

Capacity Region for Fuzzy Commitment Scheme

Definition

A secret-key vs. privacy-leakage rate pair (R_s, R_l) is achievable by the fuzzy commitment scheme with zero secrecy leakage if, given any $\varepsilon > 0$, there is some $N \geq 1$ and an encoder and decoder for which $R_s = \frac{\log|\mathcal{S}|}{N}$ and

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

$$I(S; M) = 0 \qquad \textit{(secrecy)} \qquad (2)$$

$$\frac{1}{N} I\left(X^N; M\right) \leq R_l + \varepsilon \qquad \textit{(privacy)}. \qquad (3)$$

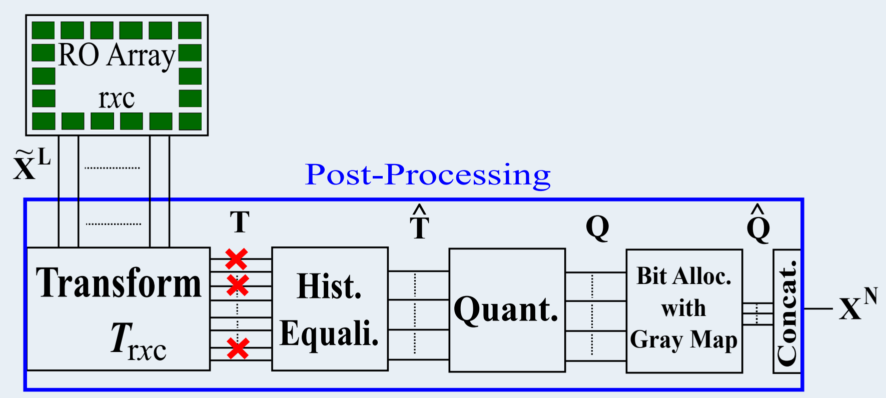
Theorem [4]

The achievable secret-key vs. privacy-leakage rate region for the fuzzy commitment scheme with a channel $P_{Y|X}$ that is a BSC with crossover probability p, uniformly distributed X and Y, and zero secrecy leakage is

$$\mathcal{R} = \{(R_s, R_l) : 0 \leq R_s \leq 1 - H_b(p), \quad R_l \geq 1 - R_s\} \qquad (4)$$

where $H_b(p) = -p\log p - (1-p)\log(1-p)$ is the binary entropy function. This region is optimal only if $R_s = 1 - H_b(p)$.

Transform Coding Steps



1. A **transform** $T_{r\times c}(\cdot)$ (e.g., *DCT, discrete Walsh-Hadamard transform (DWHT), discrete Haar transform (DHT), and Karhunen-Loeve transform (KLT)*) is applied to an array of RO outputs to reduce correlations.
2. Gaussian distributions are fitted to each transform coefficient obtained from the RO-output dataset in [5].
3. **Histogram equalization** converts the probability density of each coefficient into a standard normal distribution, i.e., $\hat{t} = \frac{t-\mu}{\sigma}$, where μ is the mean and σ is the standard deviation.
4. Use the **quantizer** $Q(\cdot)$ for all $k = 1, 2, \cdots, 2^K$ when extracting K bits such that $Q(\hat{t}) = k$ if $b_{k-1} < \hat{t} \leq b_k$, where $b_k = \Phi^{-1}\left(\frac{k}{2^K}\right)$ and $\Phi^{-1}(\cdot)$ is the quantile function of the standard normal distribution.
5. Apply **Gray mapping** and then **concatenate** the extracted bit sequences from each coefficient.

Quantizer Selection

- Define and fix a p_b as the crossover probability of the binary symmetric channel (BSC) $P_{Y|X}$.
- Define

$$D(K) = \frac{1}{K} \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} \left(\sum_{k=1}^{2^K} \Pr[Q(\hat{t}+\hat{n}) = k] \mathrm{HD}_k(\hat{t}) \right) \cdot p_{\hat{T}}(\hat{t}) p_{\hat{N}}(\hat{n}) \mathrm{d}\hat{t}\mathrm{d}\hat{n}$$

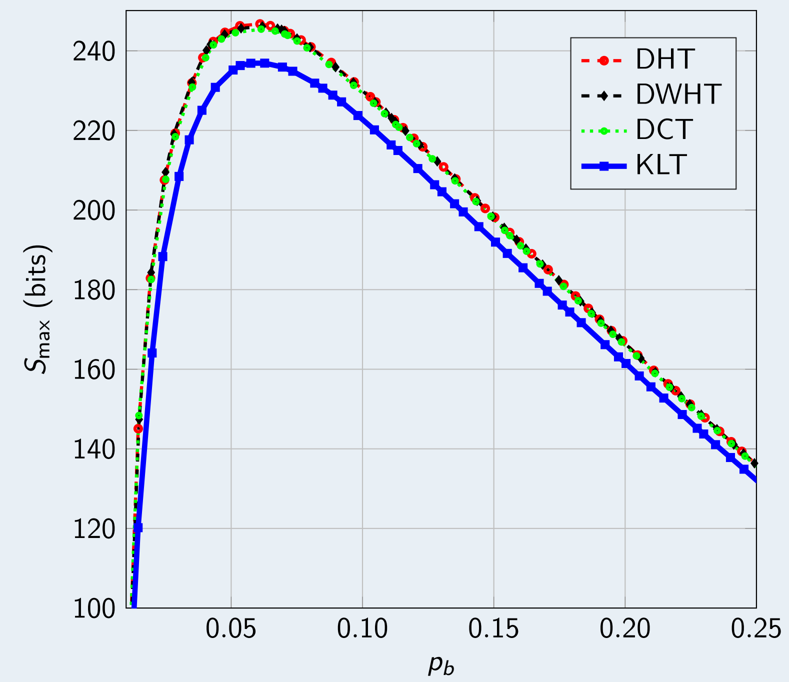
  - $\mathrm{HD}_k(\hat{t})$: the Hamming distance (HD) between the bit sequences assigned to the k-th interval and to the interval $Q(\hat{t})$.
  - $\hat{N}$: the Gaussian noise in the coefficient after equalization.
- Determine the number of bits $K(p_b)$ extracted from each coefficient as the maximum K such that $D(K) \leq p_b$.
- Do not use the DC coefficient, known by the attacker.
- The total number of extracted bits is $N(p_b) = \sum_{i=2}^{L} K_i(p_b)$.
- The maximum secret-key length is $S_{\max} = (1 - H_b(p_b)) \cdot N(p_b)$.

Performance Evaluations

1. Decorrelation Efficiency

	DCT	DWHT	DHT
η_c for 8×8 ROs	0.9978	0.9977	0.9978
η_c for 16×16 ROs	0.9987	0.9988	0.9986

2. Maximum Secret-key Length



3. Complexity

KLT	DCT	DWHT	DHT
$\mathcal{O}(N^3)$	$\mathcal{O}(N^2 \log N)$	$\mathcal{O}(N^2 \log N)$	$\mathcal{O}(N^2)$

4. Uniqueness and Security: *Uniqueness* is 0.500 and HD variance is approximately 7×10^{-4} for all transforms. They also pass the NIST randomness tests.

Proposed Error Correction Codes

- Fix $p_b = 0.06$, where $S_{\max}$ is at its maximum.
- The block-error probability constraint: $P_B \leq 10^{-9}$.
- The code-dimension constraint: $k \geq 128$.

Proposed Codes

1. The **Reed-Muller** code $\mathcal{C}(32, 6, 16)$ as the inner code and a **Reed-Solomon** code $\mathcal{RS}(2^6; 28, 22, 7)$ as the outer code.
   - The majority logic decoder of the inner code transforms the $BSC(0.06)$ into a channel with the erasure probability of 6.57×10^{-5} and the error probability of 4.54×10^{-6}.
   - The bounded minimum distance decoder (BMDD) of the outer code results in the block-error probability of $P_B = 1.37\times 10^{-11}$.
   - $(\mathbf{R_s}, \mathbf{R_l}) = (\mathbf{0.1473}, \mathbf{0.8527})$ bits/source-bit.
2. A **repetition** code with block length $n_i = 3$ as the inner code and a **binary extended Bose-Chaudhuri-Hocquenghem** code with parameters $(256, 132, 36)$ as the outer code.
   - The maximum-likelihood decoder of the inner code transforms the $BSC(0.06)$ into a $BSC(0.0104)$.
   - The BMDD of the outer code results in the block-error probability of $P_B = 3.48\times 10^{-10}$.
   - $(\mathbf{R_s}, \mathbf{R_l}) = (\mathbf{0.1719}, \mathbf{0.8281})$ bits/source-bit.

- Both channel codes provide better (secret-key, privacy-leakage) rate pairs than previously suggested codes (e.g., in [2, 3]).

- The **best possible** $(\mathbf{R_s}, \mathbf{R_l})$ **pair** achievable by the fuzzy commitment scheme from (4) for a $BSC(0.06)$ is $(\mathbf{0.6726}, \mathbf{0.3274})$ bits/source-bit.
- Better key-leakage rate pairs are thus possible, but these constructions would result in increased hardware complexity, which is not desired for ***internet of things*** applications.

Discussion

- It would be natural to use iterative decoders in combination with low density parity check or turbo codes. Hardware complexity would then increase due to iterations and it is a difficult task to simulate these codes for $P_B \leq 10^{-9}$.

References

[1] O. Günlü, O. İşcan, and G. Kramer, "Reliable secret key generation from physical unclonable functions under varying environmental conditions," in *IEEE Int. Workshop Inf. Forensics and Security*, Rome, Italy, Nov. 2015, pp. 1–6.

[2] R. Maes, A. V. Herrewege, and I. Verbauwhede, "PUFKY: A fully functional PUF-based cryptographic key generator," in *Cryptographic Hardware and Embedded Sys.* Berlin Heidelberg, Germany: Springer-Verlag, Sep. 2012, pp. 302–319.

[3] S. Puchinger *et al.*, "On error correction for physical unclonable functions," in *VDE Int. ITG Conf. Systems, Comm. and Coding*, Hamburg, Germany, Feb. 2015, pp. 1–6.

[4] T. Ignatenko and F. M. Willems, "Information leakage in fuzzy commitment schemes," *IEEE Trans. Inf. Forensics and Sec.*, vol. 5, no. 2, pp. 2337–348, 2010.

[5] A. Maiti *et al.*, "A large scale characterization of RO-PUF," in *IEEE Int. Symp. Hardware-Orient. Sec. and Trust*, Anaheim, CA, Jun. 2010, pp. 94–99.

German Research Foundation

Unterstützt von / Supported by
Alexander von Humboldt
Stiftung / Foundation

Technical University of Munich