Low-complexity and Reliable Transforms for Physical Unclonable Functions

Onur Günlü and Rafael F. Schaefer
Information Theory and Applications Chair, TU Berlin
{guenlue, rafael.schaefer}@tu-berlin.de

IEEE ICASSP, May 2020
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.
Alternative: Physical unclonable functions (PUFs) such as fine variations in the oscillation frequency of ring oscillators (ROs) for on-demand key generation so that

- invasive attacks permanently change the identifier output,
- randomness is provided by uncontrollable manufacturing variations,
- new identifiers can be inserted when there is leakage.
• Encryption/Decryption with Physical Unclonable Functions (PUFs)

NVM = Non-Volatile Memory
• **PUF Outputs Used As a Local Key for a Digital Device**
Fuzzy Commitment Scheme (FCS)

- Secret key $S$ and helper data $W$ have to be independent,
- Block error probability should satisfy $P_B = \Pr[S \neq \hat{S}] \leq 10^{-9}$,
- $S$ should be uniformly random with entropy of 128 bits.
Main Contributions

\[ C^n = \text{Enc}(S) \]

\[ \tilde{Y}^L = \tilde{X}^L + \tilde{E}^L \]

Signal Processing

\[ W = X^n \oplus C^n \]

\[ Y^n = X^n \oplus E^n \]

\[ \hat{S} = \text{Dec}(R^n) \]

\[ \tilde{X}^L \]

\[ \hat{S} \]

\[ S \]
Main Contributions (Cont’d)

➤ Propose a new set of 2D orthogonal transforms that simultaneously

➤ provide high decorrelation efficiency
  (i.e., small secrecy and privacy leakage);

➤ increase reliability significantly (i.e., smaller bit error probability);

➤ decrease hardware complexity
  (i.e., smaller hardware area due to No Multiplications);

➤ obtain significantly smaller block-error probability $P_B << 10^{-9}$ than previous FCS designs with the same or smaller channel code rate.
Apply a transform $T_{rxc}(\cdot)$ to decorrelate $\tilde{X}^L/\tilde{Y}^L$,

Each scalar quantizer satisfies the uniformity property
$$\Pr[\text{Quant}(\hat{T}_i) = (q_1, q_2, \ldots, q_{K_i})] = \frac{1}{2^{K_i}} \text{ for } i = 1, 2, \ldots, L,$$
The noise components have zero mean, so use Gray mapping,

Concenate 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 (i.i.d.).
New Set of Transforms

Consider an orthogonal matrix $A$ with elements 1 or $-1$ and of size $k \times k$, i.e., $AA^T = I$.

The following matrices are also orthogonal:

$$\begin{bmatrix} A & A \\ A & -A \end{bmatrix}, \begin{bmatrix} A & A \\ -A & A \end{bmatrix}, \begin{bmatrix} A & -A \\ A & A \end{bmatrix}, \begin{bmatrix} -A & A \\ A & A \end{bmatrix}. \tag{1}$$

Choose $k = 4$ for exhaustive search of matrices $A$ and apply the matrix extension methods in (1) twice to obtain 12288 unique orthogonal transforms of size $16 \times 16$ with elements 1 or $-1$.  

Onur Günülü and Rafael F. Schaefer: Low-complexity and Reliable Transforms for Physical Unclonable Functions 10
We use a public dataset\textsuperscript{1} with ring oscillator (RO) outputs.

The dataset contains multiple measurements of $16 \times 16$ arrays of ROs, e.g., $L = 255$, with identical circuit designs.

Measurements are taken from multiple devices from the same chip family under ideal temperature and voltage conditions.

We compare bit error probabilities of the transform coefficients for the selected transform (ST) from the new set, the discrete cosine transform (DCT), and the discrete Walsh-Hadamard transform (DWHT).
New transforms, including the DWHT, do not require multiplications (because their transform matrix elements are 1 and -1), unlike other transforms, so the hardware cost is significantly decreased;

Reliability of the ST is considerably higher than all other transforms;

All transforms perform well in terms of the decorrelation efficiency and pass most of the national institute of standards and technology (NIST) randomness tests.
Take advantage of STs’ higher reliability by combining them with binary linear block codes with bounded minimum distance decoders (BMDD) for low complexity.

A BMDD for a block code can correct all error patterns with at most 
\[ e = \left\lfloor \frac{d_{\text{min}} - 1}{2} \right\rfloor \] errors.

We use a Bose-Chaudhuri-Hocquenghem (BCH) code with blocklength 
\[ n = 255 = L \] bits, code dimension 
\[ k = 131 > 128 \] bits, and minimum distance 
\[ d_{\text{min}} = 37 \] in the FCS.

This BCH code achieves a block error probability of 
\[ P_B \approx 2.860 \times 10^{-12} << 10^{-9}, \] which is the smallest \( P_B \) in the literature achieved by codes with the same or smaller code rates.
Conclusion

- Proposed a new set of 2D orthogonal transforms that simultaneously satisfy
  - negligible secrecy leakage;
  - small privacy leakage;
  - large secret key size;
  - small block error probability;
  - low hardware complexity constraints.

- In combination with a BCH code in the FCS, the ST provides the smallest block error probability in the PUF literature.
THANK YOU!

guenlue@tu-berlin.de