DCT BASED RING OSCILLATOR PHYSICAL UNCLONABLE FUNCTIONS

Onur Günlü and Onurcan İşcan

Technische Universität München
Institute for Communications Engineering
onur.gunlu@tum.de, onurcan.iscan@tum.de

ABSTRACT

A new post-processing scheme is proposed for Physical Unclonable Functions (PUFs) based on Ring Oscillators (ROs). The scheme uses the Discrete Cosine Transform (DCT) to decorrelate the RO outputs and improves on existing RO PUFs in terms of uniqueness and the number of extracted bits.

Index Terms— Physical Unclonable Function, Ring Oscillator, Discrete Cosine Transform, Key Generation

1. INTRODUCTION

One way to provide cryptographic security is to generate secret keys and store them using Integrated Circuits (ICs), traditionally in non-volatile memory. An important task is to ensure that the keys are not revealed to adversaries. However, storing keys safely in ICs is usually costly and unreliable [1]. An alternative and promising technique called *Physical Unclonable Function* (PUF) was proposed in [2] as an improved version of the technique called Physical One-Way Function, proposed in [3]. PUFs are challenge-response mappings that depend on random physical variations. The secret keys are derived from the mappings. Two important features of PUFs are that the keys need not be stored and that they can be generated on demand. PUFs provide cheap (no requirement for memory to store the key) and safe (complex mapping) alternatives to other secret key generation and storage techniques [1]. PUFs are also used for chip authentication, Intellectual Property (IP) protection and remote IC enabling/disabling [4], [5].

We focus on secret key generation via Ring Oscillator (RO) PUFs and consider the requirements of cryptographic primitives as quality measures [6], [7]. We propose the Discrete Cosine Transform (DCT) as a post-processing step to extract bits from PUFs. We show that the DCT reduces undesired systematic variations in RO outputs and increases the number of extracted bits.

This paper is organized as follows. In Section 2, the basic RO logic circuit and classic RO PUFs are reviewed. The new approach, called *DCT-based RO PUFs*, is explained in Section 3. Comparisons with previous approaches are given in Section 4. Section 5 concludes the paper.

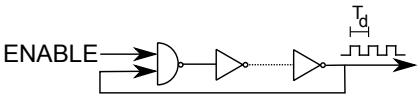

Fig. 1. Single ended ring oscillator logic circuit [8].

2. RING OSCILLATOR PUF

The logic circuit of ROs has an odd number m of inverters connected in serial and the output of the last inverter is fed back to the first inverter [8]. To avoid self-heating, a NAND gate can replace the first inverter as shown in Figure 1. The ring must provide a 2π phase shift and have unity voltage gain at the oscillation frequency to sustain oscillation. A propagation delay of τ_d seconds per inverter gives the oscillation frequency of $f_c = 1/(2m\tau_d)$ [8].

The propagation delay τ_d is sensitive to circuit nonlinearities and parasitics. In addition, noise sources like the simultaneous switching of multiple gates to the same state, cross-talk between adjacent signal traces, or noise sources like thermal noise and shot noise make it difficult to perfectly predict f_c. Moreover, with decreasing semiconductor size, it becomes more difficult to predict these important effects. There have been efforts to improve reproducibility but every ring oscillator tends to have a unique response [8]. This is a drawback for most applications but [1] suggests to use such effects to store secrets. For example, Figure 2 shows the first RO PUF approach [1]. There are N ROs and the idea is that the multiplexers are challenged by a bit sequence of length $\lceil \log_2 N \rceil$ so that two different ROs are selected among N of them. The counters put out the number of rising edges in the analog square waves from the two selected ROs for a certain period of time. The counter values are compared and a logic bit 1/0 is obtained when the upper/lower RO counter has a larger value than the other RO. Assuming that the oscillators are laid out identically, the difference in the RO frequencies is determined mainly by manufacturing variations [1]. The number of independent bits that can be generated by choosing RO pairs is less than the number of distinct pairs since the bits from these pairs are correlated. Thus, different grouping

978-1-4799-2893-4/14/$31.00 ©2014 IEEE

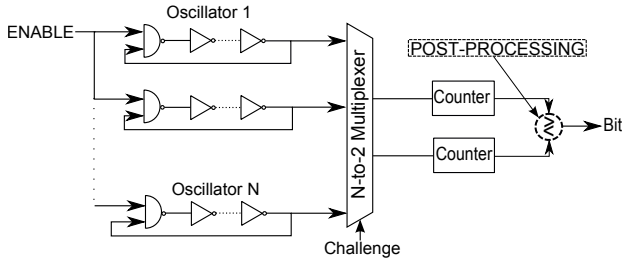

Fig. 2. First RO PUF design and its components.

and pairing approaches have been proposed. One proposal uses adjacent pairs of ROs [6] and a better proposal uses non-overlapping RO pairs [1] so that correlations are reduced, but there are systematic variations in RO outputs that depend on the surrounding logic. Thus, using non-overlapping RO pairs cannot ensure uncorrelatedness [9].

Temperature and voltage changes can cause the same PUF to give different outputs than the nominal condition, which reduces the reliability of the PUF. To avoid this problem, the authors of [1] proposed a *1-out-of-k masking* scheme. This scheme uses the RO pair that gives the maximum frequency difference for a range of temperatures among k RO pairs (e.g., $k = 8$) and only one bit is generated for each challenge input.

Another RO PUF proposed in [9] uses regression-based distillers to eliminate systematic variations. Two different types of sequences are grouped in this scheme to increase randomness and reliability.

We will compare PUFs by considering ROs of 32×16 and 16×16 arrays. There has been some work on such arrays that uses the public dataset [6] consisting of measurements from 193 different Xilinx Spartan (XC3S500E) FPGAs with 32×16 RO arrays for test and comparison.

3. DCT BASED RO PUFS

Three challenges for RO PUFs are error correction for the secret key (see [10] and [11]), the number of required ROs, and the secret key randomness [4], [9]. These challenges are relevant to the quality measures reliability, cost and attack resiliency, respectively. We apply a DCT-based post-processing to deal with these challenges. The steps of the new approach are shown in Figure 3 and are as follows:

1. Apply a two-dimensional DCT to the RO outputs ($\mathrm{F}_{32\times16}$) to generate the DCT coefficients ($\mathrm{C}_{32\times16}$).
2. Select L of the 512 DCT coefficients and quantize them to the variable Q_L. The selection and quantization routines are determined by the chip manufacturer for a family of chips.
3. Represent the quantized values by bit sequences and concatenate them to construct the output bit sequence.

3.1. Two Benefits of the DCT

Two benefits of the DCT are that it decorrelates the RO outputs (this does not mean that the resulting outputs are independent) and localizes the effect of temperature variations (to eliminate it) in the DCT-domain. These features decrease the systematic variations and increase the randomness within the output sequence [12]. Localizing the effect of temperature variations is also beneficial for efficient error correction [13].

3.2. Quantizer Design and Bit Assignment

The manufacturer must select the DCT coefficients and the number of bits extracted from them. Thus, one must use the same RO PUF design in all chips and one should gather statistical information about the DCT coefficients. We determine the empirical probability distribution functions (pdfs) of the DCT coefficients across different chips. Quantization and bit assignment algorithms are then determined according to the pdf of each coefficient. In addition, the number of bits extracted from a particular coefficient is determined by calculating distortion values for bit lengths in the range of 1 to 12 (a broad range of bit lengths that is selected according to predetermined configurable target bit error probability values p_b). After selecting the DCT coefficients, the number of extracted bits from each coefficient, the quantization steps and the bit assignment algorithm, the manufacturer stores these parameters as public data. The secret key of predetermined length T is generated by each user via DCT-based RO PUFs as shown in Figure 3.

The pdf of each DCT coefficient can be found by applying distribution fitting to the samples of each coefficient [14]. We use the public dataset in [6] to obtain the distributions. When this dataset is used for fitting distributions to 32×16 and 16×16 RO arrays, the highest match from the Kolmogorov-Smirnov tests [14] is observed from Cauchy distributions (rather than generalized-Gaussian or Laplace distributions, often used in the literature [15]). The pdf parameters are estimated via maximum-likelihood estimation [12].

We choose the quantization algorithm that makes the probability of each quantization interval the same (similar to [16]), i.e., the area between neighboring quantization steps under the fitted pdf of a DCT coefficient is $1/2^L$ when ex-

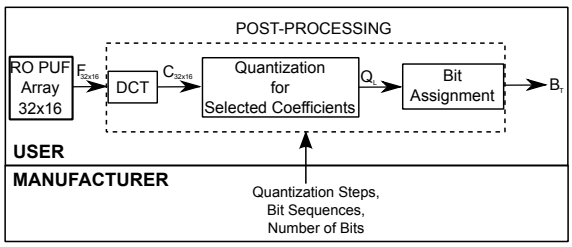

Fig. 3. DCT based RO PUF steps.

tracting L bits. Each quantization interval is represented by a Gray-coded bit sequence (as, e.g., in [17]). Gray encoding ensures that neighboring quantization intervals are represented by bit sequences that differ by only one bit. Thus, the most probable error event causes only one bit error.

Similar to the DCT coefficients, the noise in the DCT-domain (assumed to be additive) for each coefficient is fitted to a Cauchy distribution (rather than generalized-Gaussian, Laplace, or log-normal distributions) since it has the best match according to Kolmogorov-Smirnov tests. By using the estimated parameters of the coefficients and noise, the distortion $D(L)$ is calculated for each coefficient as follows:

$$D(L) = \frac{1}{L} \int_{-\infty}^{\infty} \left(\sum_{k=1}^{2^L} P_k(c,n) \mathrm{H}_{L,k}(c) \right) f(c) \mathrm{d}c \quad (1)$$

where c represents the value of a particular DCT coefficient with the pdf $f(c)$, $P_k(c,n)$ is the probability that the output is quantized to the k-th interval due to noise with the pdf $f(n)$, and $\mathrm{H}_{L,k}(c)$ is the Hamming distance between the bit sequences assigned to the kth interval and to quantized value of c. This distortion value corresponds to the mean number of errors due to noise for a single bit extracted from a particular coefficient. It is used to determine the number of bits extracted from each coefficient. In addition, this distortion also affects the requirements for the helper data generation algorithm which is used to correct errors in the generated bits due to noise, e.g., [10].

The distortion values are shown in Figure 4 when (1) is calculated numerically for each coefficient. To determine which coefficients to select, the following steps are performed:

- Determine the target bit error probability p_b according to the error correction requirements.
- Find the bit length L_i that minimizes the absolute difference $|D(L_i) - p_b|$ for each DCT coefficient and assign it as the number of bits extracted from a particular coefficient. This can be done by looking at the crossing points of $D(L)$ and p_b.
- Select the coefficients with the largest bit values (L_i) until the total number T of bits are gathered. This corresponds to selecting the coefficients belonging to the rightmost curves in Figure 4, which minimizes the number of coefficients used [12].

Empirical results show that the selected coefficients are mostly in the low frequency bands of the DCT .

4. DISCUSSION

We next analyze the DCT-based approach in terms of the number of extracted bits and the Hamming distances between different PUF outputs. Moreover, we compare the results with previous approaches in the literature.

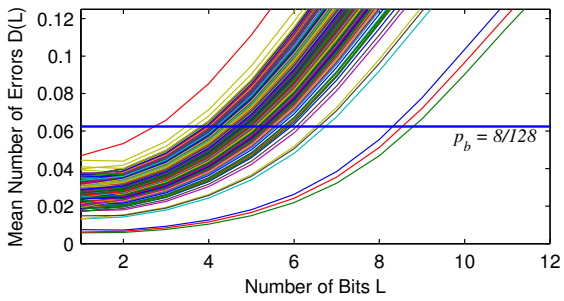

Fig. 4. Mean number of errors per bit. Each curve corresponds to a coefficient and the horizontal line to a p_b value.

4.1. Number of Extracted Bits

The maximum number T_{max} of extractable bits from a PUF can be regarded as a design metric since it gives the mean cost for generating one bit in terms of the number of ROs. In Table 1, T_{max} values for different approaches are listed for 32×16 and 16×16 two-dimensional RO arrays. For the DCT-based approach, T_{max} is the total number of extracted bits if all DCT coefficients are selected for a predetermined p_b. The results for the previous approaches are taken from [1] and [9], and they are independent of p_b. According to these results, the DCT-based approach outperforms the previous approaches in terms of T_{max}, meaning that the required number of ROs per bit is less than in previous work. In addition, our approach gives a trade-off between p_b and T_{max}. If p_b increases, one must improve the error correcting capability but more bits are extracted. The p_b level can thus be optimized for particular error correction schemes.

Approach	$\mathbf{32 \times 16}$	$\mathbf{16 \times 16}$
1-out-of-8 Masking	128	64
Non-overlapping RO pairs	256	128
Regression-based Distillers for RO PUFs	512	256
DCT-based RO PUFs ($p_b = 0.05$)	1930	1516
DCT-based RO PUFs ($p_b = 0.10$)	3171	1966
DCT-based RO PUFs ($p_b = 0.15$)	4003	2668

Table 1. Maximum number of extracted bits. The results of the reference approaches are taken from [1] and [9].

4.2. Uniqueness

Uniqueness refers to the difference between the secret keys generated by different chips with the same PUF design [6] and is often measured using the Hamming distance d_{H} between two generated bit sequences. For analyses in nominal environmental conditions, we use the public dataset in [6]. Figure 5 depicts the histogram of d_{H} when bit sequences of length 1275 are generated via our DCT-based approach. The average is 0.498 that is close to the desired value 0.500, and

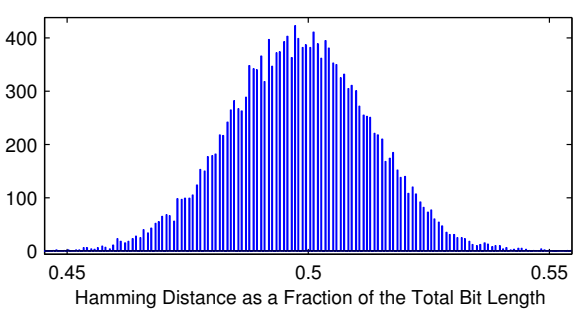

Fig. 5. Histogram of d_{H} from DCT-based RO PUF outputs.

its variance is 2.08×10^{-4}. By comparing these results with the results of comparison of adjacent pair of ROs (average 0.473) [6], 1-out-of-8 masking (average 0.462) [1] and other variants of these approaches, e.g., [7] (the best average 0.455), we conclude that our approach outperforms the previous approaches in terms of uniqueness since it has a mean closer to 0.500 with an acceptable deviation from the mean.

5. CONCLUSIONS

A new secret key generation method based on RO PUFs was presented. The DCT-based post-processing steps for the RO PUFs are optimized according to certain quality measures. The results are analyzed and compared with the previous approaches. In terms of the required number of ROs per bit and uniqueness, our approach outperforms reference approaches.

Acknowledgment

The authors were supported by the German Ministry of Education and Research in the framework of the Alexander von Humboldt-Professorship. The authors thank Prof. Gerhard Kramer for suggesting the use of the DCT and for his contributions to this work.

6. REFERENCES

[1] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *Proc. 44th Design Automation Conf.*, San Diego, CA, USA, Jun. 2007, ACM, pp. 9–14.

[2] B. Gassend, "Physical random functions," M.S. thesis, M.I.T., Jan. 2003.

[3] R. Pappu, *Physical one-way functions*, Ph.D. thesis, M.I.T., Oct. 2001.

[4] C. Böhm and M. Hofer, *Physical Unclonable Functions in Theory and Practice*, Springer, 2013.

[5] J. Guajardo, S. S. Kumar, G.-J. Schrijen, and P. Tuyls, "FPGA intrinsic PUFs and their use for IP protection," in *Cryptographic Hardware and Embedded Systems*, pp. 63–80. Springer, 2007.

[6] 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, Jun. 2010, pp. 94–99.

[7] A. Maiti and P. Schaumont, "Improving the quality of a physical unclonable function using configurable ring oscillators," in *IEEE Int. Conf. on Field Programmable Logic and Appl.*, Aug. 2009.

[8] M. K. Mandal and B. C. Sarkar, "Ring oscillators: Characteristics and applications," *Indian J. of Pure & Appl. Physics*, vol. 48, pp. 136–145, Feb. 2010.

[9] C.-E. Yin and G. Qu, "A regression-based entropy distiller for RO PUFs," Tech. Rep., The Inst. for Sys. Research, A. James Mark School of Eng., Univ. of Maryland, 2011.

[10] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," *Soc. for Ind. and Appl. Math. J. on Comp.*, vol. 38, pp. 97–139, Mar. 2008.

[11] M. D. M. Yu and S. Devadas, "Secure and robust error correction for physical unclonable functions," *IEEE Design and Test of Comp.*, vol. 27, pp. 48–65, Feb. 2010.

[12] O. Günlü, "Design and analysis of discrete cosine transform based ring oscillator physical unclonable functions," M.S. thesis, Techn. Univ. München, Oct. 2013.

[13] G. Kramer, "Information theory models/ideas for ring oscillator PUFs," Presented in SFB Transregio Meeting, Mar. 2013.

[14] J. Durbin, *Distribution Theory for Tests Based on the Sample Distribution Function*, Regional Conf. Series in Appl. Math. Soc. for Ind. and Appl. Math., 2001.

[15] N. Kamaci, Y. Altunbasak, and R. M. Mersereau, "Frame bit allocation for the H. 264/AVC video coder via Cauchy-density-based rate and distortion models," *IEEE Trans. Circuits and Sys. for Video Techn.*, vol. 15, no. 8, pp. 994–1006, 2005.

[16] E. Verbitskiy, P. Tuyls, C. Obi, B. Schoenmakers, and B. Skoric, "Key extraction from general non-discrete signals," *IEEE Trans. on Inf. Forensics and Security*, vol. 5, no. 2, pp. 269–279, 2010.

[17] P. Tuyls, B. Skoric, T. Kevenaar, et al., *Security with Noisy Data: On Private Biometrics, Secure Key Storage and Anti-Counterfeiting*, Springerverlag London, 2007.