Abstract:

The incorporation of reliable and robust security features in electronic devices have seen a burgeoning demand in recent times starting from banking infrastructure to critical communication links. For setting up trustworthy communication links as well as data-privacy hardware-level security features have become extremely important. Specifically, the IoT devices that are plentiful in many households and institutions often strive for low power consumption and handle sensitive information. Physical Unclonable Functions (PUFs) are popular low-cost hardware primitives largely utilized for hardware-security applications. The operations that PUFs are capable of performing have historically required larger, more power-hungry, crypto processors and many clock cycles; PUFs are able to provide low-power solutions perfect for IoT applications. A PUF acts like a device “finger print” which leverages the manufacturing variation of integrated circuits to produce initially unpredictable, yet consistent, unique responses to given challenges, known as a challenge-response pair (CRP). Depending on the possible number of CRPs and type of applications, PUFs are broadly classified as “weak” and “strong”. A strong PUF can produce a huge number of CRPs and it is typically used for device authentication [1][2]. On the other hand, weak PUFs show only few feasible CRPs and are mainly utilized for secure key generation [3][4]. A PUF core can be based on bi-stable circuits such as SRAMs [2], custom bi-stable circuits [1][3][4] and also circuits employing delay variability such as ring oscillators [5], arbiters [6-8] etc. PUF circuits are often vulnerable to either invasive or non-invasive attacks trying to predict and/or modify the PUF responses to challenges. These attacks can be machine learning based modelling attacks, side-channel attacks, etc. Many techniques have been developed in recent years to make the PUFs resilient to these attacks [1-2]. Typically, a non-linear response generation mechanism enhances the resiliency of PUFs by making the machine-learning predictions more difficult. Another major issue with the PUF circuits is that the PUF responses are prone to errors or variations due to environmental changes (such as voltage, temperature etc.). These variations can be classified as intra-PUF and inter-PUF variations. Whereas the inter-PUF variation is a desired phenomenon to ensure the uniqueness of a PUF, the intra-PUF variations are unwanted and can cause significantly large bit error rate (BER). Several error-correction techniques have been demonstrated in literature including use of 2-D Hamming codes [9], BCH codes [10], temporal-majority voting (TMV), soft dark-bits masking[4] etc. Although for device authentication (i.e. strong PUF) the BER requirement can be somewhat relaxed due to finite allowable detection tolerance, the requirement is much more stringent in case of weak-PUFs for key generation application. For our project, with the importance of PUF's application to IoT devices, we will aim to improve PUF stability and power consumption by working to evaluate and design a state-of-the-art PUF core. We will also work on designing and implementing efficient digital logic with error correction and detection to decrease the BER and allow the PUF to be integrated into an SoC.

References:

[1] V. Suresh, R. Kumar, M. Anders, H. Kaul, V. De and S. Mathew, "A 0.26% BER, 1028 Challenge-Response Machine-Learning Resistant Strong-PUF in 14nm CMOS Featuring Stability-Aware Adversarial Challenge Selection," 2020 IEEE Symposium on VLSI Circuits, Honolulu, HI, USA, 2020.

[2] S. Jeloka, K. Yang, M. Orshansky, D. Sylvester and D. Blaauw, "A sequence dependent challenge-response PUF using 28nm SRAM 6T bit cell," *2017 Symposium on VLSI Circuits*, Kyoto, 2017.

[3] S. K. Mathew *et al*., "16.2 A 0.19pJ/b PVT-variation-tolerant hybrid physically unclonable function circuit for 100% stable secure key generation in 22nm CMOS," *2014 IEEE International Solid-State Circuits Conference Digest of Technical Papers (ISSCC)*, San Francisco, CA, USA, 2014.

[4] S. Satpathy *et al*., "A 4-fJ/b Delay-Hardened Physically Unclonable Function Circuit With Selective Bit Destabilization in 14-nm Trigate CMOS," in *IEEE Journal of Solid-State Circuits*, vol. 52, no. 4, pp. 940-949.

[5] K. Yang, Q. Dong, D. Blaauw and D. Sylvester, "14.2 A physically unclonable function with BER <10−8 for robust chip authentication using oscillator collapse in 40nm CMOS," *2015 IEEE International Solid-State Circuits Conference - (ISSCC) Digest of Technical Papers*, San Francisco, CA, USA, 2015.

[6] J. W. Lee, Daihyun Lim, B. Gassend, G. E. Suh, M. van Dijk and S. Devadas, "A technique to build a secret key in integrated circuits for identification and authentication applications," *2004 Symposium on VLSI Circuits. Digest of Technical Papers (IEEE Cat. No.04CH37525)*, Honolulu, HI, USA, 2004.

[7] M. Majzoobi, F. Koushanfar, and M. Potkonjak, ‘‘Lightweight secure PUFs,’’ in Proc. ACM/IEEE Int. Conf. Comput.-Aided Design, 2008, pp. 670–673.

[8] G. E. Suh and S. Devadas, ‘‘Physical unclonable functions for device authentication and secret key generation,’’ in Proc. ACM/IEEE Design Autom. Conf., 2007, pp. 9–14.

[9] B. Gassend, ‘‘Physical random functions,’’ M.S. thesis, Dept. Electr. Eng. Comput. Sci., Massachusetts Inst. Technol., Cambridge, MA, USA, Jan. 2003.

[10] G. E. Suh, ‘‘AEGIS: A single-chip secure processor,’’ Ph.D. dissertation, Dept. Electr. Eng. Comput. Sci., Massachusetts Inst. Technol., Cambridge, MA, USA, Aug. 2005.