THE UNIVERSITY OF
ALABAMA IN HUNTSVILLE

Office of Sponsored Programs

May 15, 2018

Southeastern Center for Electrical Engineering Education (SCEEE)
SCEEE Development Fund Grants Program
Attn: Dr. Nicolas Younan

Subject: UAH Research Proposal No. 2018-523

Dear Dr. Younan:

The University of Alabama in Huntsville (UAH) a state funded institution of higher education is pleased to submit the subject proposal on behalf of the Principal Investigator, Dr. Tauhidur Rahman, in response to the RFP entitled: "LDHSP: Exploiting DRAM Latency Variations for Generating Hardware-based Security Primitives." The estimated total proposed project cost for a one year period is $51,000 (SCEEE $25,500; UAH $25,500).

Dr. Rahman's proposal may contain information and/or data that are proprietary and/or confidential to UAH. This information is submitted for purposes of review and evaluation either to the specific request for proposal denoted herein or as an unsolicited proposal. No other disclosure or use of this information or data contained herein is permitted without written permission of UAH and the Principal Investigator.

Please direct all technical questions to Dr. Rahman at (256) 824-6678 or email: mtr0011@uah.edu. For contractual assistance please contact Ms. Jescia Sigh at (256) 824-5834 or email: jrs0044@uah.edu.

Sincerely,

Gloria W. Greene

Gloria W. Greene, MA, CRA
Director, Office of Sponsored Programs

LDHSP: Exploiting DRAM Latency Variations for Generating Hardware-based Security Primitives

Tauhidur Rahman

1. Problem Statement: Integrated circuits (ICs) play an increasingly important role in our day-to-day lives. On the one hand, ICs form the foundation of critical military and commercial systems. On the other hand, the rapid growth of information technology has enabled development of more and more emerging products and application that require communication with server/cloud databases to access high-quality services. Electronic devices (laptops, tablets, smartphones, GPS, medical devices, etc.) have become more pervasive in our daily lives, maintaining a high level of security and reliability has become a significant societal challenge. To this end, central tasks include realizing secure and reliable identification, authentication, and integrity checking of the underlying hardware (e.g., integrated circuits) in these devices. More recently, the hardware security community has helped to shift industry's attention towards the design of hardware-based security primitives to replace the more expensive and vulnerable software-based primitives. Hardware-based security primitives play important roles in protecting and securing the assets of an electronic system. Identification, authentication, secure communication, IC obfuscation to prevent IC piracy in semiconductor supply chain, detection of counterfeit ICs, etc. are some common use of hardware-based security primitives. The three major primitives under investigation in this proposal are further elaborated in the following: (i) **Physical Unclonable Functions (PUFs)** have been proposed as a more secure alternative to secret key storage because of their unclonability and built-in tamper evidence [1-3]. (ii) A **True Random Number Generator (TRNG)** translates a physical entropy source such as thermal noise, atmospheric noise, shot noise, radio noise, flicker noise, chaos, etc. into a non-deterministic random bitstream [1-3]. An ideal TRNG has uniform statistical characteristics at any operating conditions, workload, and degradation in the field. TRNG is used in cryptography and secure communication [2]. (iii) **Anti-Counterfeit (AC) Technology** commonly in the form of **certified object authenticators (COAs)** is essential for improving supply chain security and assurance. As the consumer electronics market continues to expand, counterfeiting of electronic components is becoming more profitable and difficult to contain. Recycled chips, remarked chips, out-of-spec chips, and chips from a fake manufacturer are the major types of counterfeit chips [2]. It has been reported that memory contributes ~20% of total counterfeit chips [1-3]. Therefore, it's essential to develop a technology that prevents counterfeiting.

Memory-based security primitives have been gaining popularity because they are the cheapest and don't need any additional hardware [2-3]. In previous work, the PI has mainly focused on SRAM and Flash based security primitives [3, 6, biosketch]. But SRAM is very expensive, and flash-based security primitives are very slow [2-3]. Therefore, DRAM can be the most suitable for major applications. However, existing DRAM-based security primitives have major limitations (see Section 2). In this work, the PI proposes novel latency-based DRAM signature generation which can be used for creating security primitives and make them applicable to real and run-time commodity applications.

2. Motivations, Objectives, and Novelty: DRAM is ubiquitous but suffers several limitations which make it almost impossible to use DRAM for security primitives in electronic commodities. The objective of this project is to propose novel DRAM-based security primitives by exploiting the timing latency variations [4]. We summarize the motivations, objectives, and novelty of our proposed work below.

- **Waste of DRAM Power Cycle:** Start-up based key/random number (RN) generation requires a DRAM power cycle to obtain device signatures. As a result, the whole system needs a turn-off and a turn-on to evaluate the PUF /TRNG operation. Therefore, this type of DPUF/DTRNG (DRAM-based PUF/TRNG) cannot be evaluated while the system is in operation (i.e., during run-time). **Our proposed technique does not require power ON/OFF.**
- **Destructive:** Retention-based key/RN generation is destructive (data is lost). A dedicated memory might need to be used which contradicts the original no-hardware purpose. Like retention-based DPUF/DTRNG, the start-up based DPUF/DTRNG is also destructive. **Our proposed DRAM-based security primitives are not destructive.**
- **Disruptive to System Operation:** The granularity of DRAM chip is the channel. An already busy channel cannot be used for key generation. Similarly, we cannot use the DRAM cells to perform other services if they are active in generating a key/RN. **Our proposed technology will not disrupt the system operation.**
- **Weak PUF:** Like SRAM-PUF, most of the existing DRAM-based PUFs are weak. We will propose a strong PUF that **does not require any modification of DRAM architecture**.

- **Quality of Key/RN:** The quality of existing methodology of generating key/RN is limited because of limited entropy. We will propose **algorithms for generating high-quality security primitives**. We will also show experimental comparison to present the superiority of our proposed methodology.
- **Large Evaluation Time:** Retention-based key/RN generation requires a large amount of time, order of minutes, to generate a key/RN. Existing technology is not suitable for mass-volume detection of counterfeit DRAM chips [2]. **Our goal is to make the evaluation time from the order of minutes to order of milliseconds.**

3. Novel Latency-based Signature Generation from DRAM with Preliminary Results (under review [5]): The DRAM is periodically refreshed each 32ms or 64ms (vendor to vendor) to ensure the data integrity [3]. With the increased refresh interval, some of the DRAM cells lose the original data and get flipped to opposite values. This is used for a signature generation but requires the order of seconds to generate enough errors for PUF/TRNG. Therefore, the retention based PUF is not suitable for PUF/TRNG. In this project, we propose latency-based key generation which is at least 1000X faster than retention-based PUF. Fig. 1 (left) shows the DRAM timing latency. Latency is the required time to move charge between row buffer and a DRAM row, and they suffer significant variations for each of the above operations among cells across the entire chips. Some of the cells are very slow, and some of the cells are very fast. For reliable operation, the minimum required latency has to be larger than the latency of the slowest cell [4]. We read or write the faulty data when the vendor recommended minimum timing latency is not maintained (i.e., the latency is reduced). In our proposed project, we reduce the timing latency to cause unreliable operation. The introduced error pattern at the reduced timing latency parameter is unique from device to device and can be used to generate device signatures. We plan to reduce two crucial DRAM latency parameters: ***activation*** latency and ***precharge*** latency (Fig. 1, left). Fig. 1 (right) shows that the memory contents are flipped at the reduced ***precharge*** latency. This pattern can be used to generate device signatures. The results also show that the erroneous pattern is random and unique from chip to chip. The timing latency in the millisecond range. In the proposed approach, the signature can be generated in only several milliseconds (>1000X faster than retention-based security primitives).

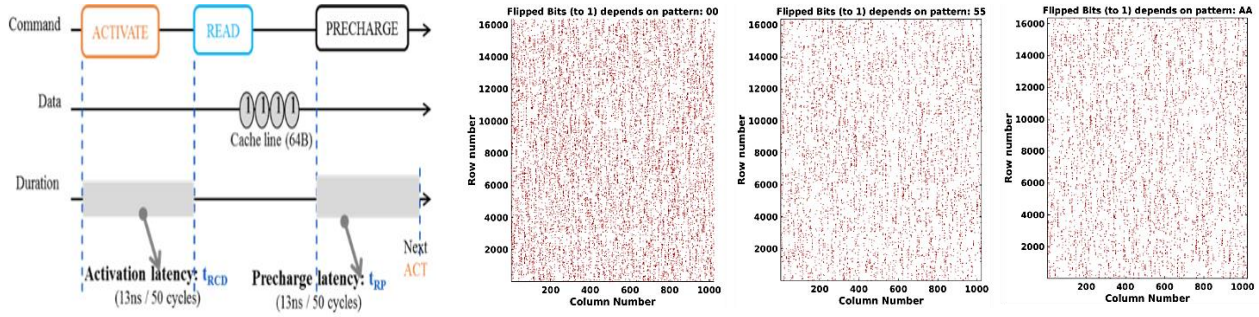

Fig 1. ***Left:*** DRAM latency parameters. ***Right:*** The unique erroneous pattern (**red** presents 'error') at the reduced ***precharge*** latency with different input patterns written into the memory [5].

4. Proposed Approach (Process):

Task 1: Characterizing DRAM cells with the reduced DRAM latency- The preliminary data shows that not all cells can be used to generate PUF (or TRNG). Some of the cells are suitable for PUF, and some of the cells are suitable for TRNG (or AC technology). In this task, we will characterize the DRAM cells to find the right candidates for the right security primitives. We will characterize the cells based on the input patterns: (i) pattern insensitive: the output does not depend on the DRAM contents (ii) Pattern sensitive: the erroneous pattern depends on the input patterns written into the memory. The pattern sensitive cells are good candidates for the strong-PUF. Primary results show that the number of pattern-insensitive DRAM cells is few. The primary results also show that some of the cells are sensitive to noise and good for the RN. On the other hand, the robust DRAM cells can be used for generating a key. Pattern sensitive DRAM cells can be ideal candidates for strong PUF.

Task 2: Developing metrics and cell Selection algorithm for the right and quality DPUF/DTRNG- Reliability (how often a PUF can generate the same outputs over different environmental conditions through entire chip lifetime), uniqueness (how well a single PUF is differentiated from other PUFs), and randomness (the unpredictability of the PUF/TRNG outputs) are the standard metrics to quantify the quality of security primitives. Our goal is to obtain a good quality of PUF/TRNG. The primary results show that the pattern sensitive (useful for randomness and uniqueness) DRAM cells are few (less than 3% of total DRAM cells). Therefore, a proper algorithm is required for

generating quality DPUF/DTRNG with the limited resource. At first, we will propose new metrics (that will show statistical dependency) that will rely on (i) data dependency and (ii) spatial correlation for extracting better signatures from the device. The metrics will help us to choose a specific data pattern to the particular DRAM cells for making a good quality DPUF/DTRNG. The erroneous pattern does not depend only on the input of a row but also depends on the neighbor cells because of coupling effect. However, most manufacturers don't share the physical layout. Therefore, we need a strong algorithm to select the best candidates for the right security primitives.

Task 3: Foundry and OCM identification- Foundry identification is essential for many tasks including intellectual property protection, trust, and preventing counterfeiting. There are several DRAM manufacturers such as Micron, Samsung, Hynix, etc. The manufacturing and layout variations are unavoidable and can be helpful to distinguish from one technology node to another technology node of a particular vendor or from one vendor to another vendor for a given specification (technology node for example). Our holistic approach will identify the origin of DRAM chips in a low-cost manner. The primary results from two major vendors show that the erroneous pattern is sensitive to manufacturers. The proposed metrics in ***Task 2*** will be used to identify the best latency parameters to identify the origin of OCM or foundry with very high accuracy.

Task 4: Recycled, remarked, and out-of-spec IC (DRAM) detection- accurate and low-cost D-ACs (DRAM-based ACs) for recycled IC, remarked IC, and out-of-spec IC detection. We assume that PUFs can detect cloned ICs as it provides a unique ID for each chip. From the preliminary latency-based aging data, we observed that there is the difference between the erroneous patterns at the reduced latency for the fresh chip and aged one. Note that the counterfeit electronic system might contain counterfeit DRAM chips. Therefore, detection of counterfeit chips can help us detecting counterfeit electronic system as well.

5. Project Outcomes and Deliverable (IPs):

- A novel latency-based DRAM signature. The proposed approach >1000X faster than existing approach.
- High-quality LDPUFs (latency-based DRAM PUFs) that utilize innovative bit selection metrics and algorithms to generate a unique key that is reliable in the presence of extreme conditions in the field require a low testing methodology to the manufacturer and reduce the need for error correcting code.
- Robust LD-TRNGs (latency-based DRAM TRNGs) that remain strong in hostile environments and under different attacks, while generating true random numbers quickly. Our approaches will identify the most unstable bits in the memory (i.e., opposite of PUF objective) and take advantage of distribution of stable and unstable bits in the memory to make LD-TRNGs that are less sensitive to tampering.
- Accurate and low-cost LD-ACs (latency-based DRAM AC) for recycled IC, remarked IC, and out-of-spec IC detection.
- A novel methodology of identifying the original OCM. There is no such technique to validate the authenticity of the OCM for any DRAM.
- The proposed four tasks are connected to each other. The data collected from DRAM chips can be used in all 4 tasks in parallel. **We are hopeful that we will be able to deliver findings from all 4 tasks within the specified time (one year).**

6. Technology Transfer: We plan to publish our research findings to major IEEE/ACM conferences and journals.

7. References

[1] Guin, Ujjwal, et al. "Counterfeit integrated circuits: A rising threat in the global semiconductor supply chain."

[2] Anagnostopoulos et al. "An Overview of DRAM-Based Security Primitives." *Cryptography* 2.2 (2018): 7.

[3] **M. Tauhidur Rahman** "Hardware-Based Security Primitives and Their Applications to Supply Chain Integrity" PhD thesis. Available [online]: http://ufdc.ufl.edu/UFE0051419/00001

[4] Chang, Kevin K., et al. "Understanding latency variation in modern DRAM chips: Experimental characterization, analysis, and optimization." *ACM SIGMETRICS Performance Evaluation Review*. Vol. 44. No. 1. ACM, 2016.

[5] B. M. S. B. Talukder, B. Ray, D. Forte, and **M. T. Rahman**, "LDPUF: Exploiting DRAM Latency Variations to Generate Robust Device Signatures," ACM Transactions on Embedded Computing Systems (TECS) (under review).

[6] P. Kumari, B. M. S. Bahar Talukder, S. Sakib, B. Ray and **M. T. Rahman**, "Independent Detection of Recycled Flash Memory: Challenges and Solutions," in IEEE Hardware-Oriented Security and Trust Symposium, 2018.

Md Tauhidur Rahman
Assistant Professor, Electrical and Computer Engineering
University of Alabama in Huntsville, 301 Sparkman Dr. Huntsville, AL 35899
Phone: (256) 824-6678 Email: tauhidur.rahman@uah.edu

Professional Preparation

University of Connecticut, Storrs, CT	Computer Engineering	M.S., 2015
University of Florida, FL	Computer Engineering	Ph.D., 2017

Professional Appointments

2017- Assistant Professor, Electrical and Computer Engineering, University of Alabama in Huntsville

Publications

(i) Five products most closely related

1. M. T. Rahman, A. Hosey, J. Carrol, D. Forte, and M. Tehranipoor, "Systematic Correlation and Cell Neighborhood Analysis of SRAM-PUF for Robust and Unique Key Generation," Journal of Hardware and Systems Security 1 (2), 137-155, 2017.

2. M. Tauhidur Rahman "Hardware-Based Security Primitives and Their Applications to Supply Chain Integrity" PhD thesis. Available [online]: http://ufdc.ufl.edu/UFE0051419/00001

3. M. T. Rahman, K. Xiao, D. Forte, X. Zhang, J. Shi and M. Tehranipoor, "TI-TRNG: Technology independent true random number generator," 2014 51st ACM/EDAC/IEEE Design Automation Conference (DAC), San Francisco, CA, 2014, pp. 1-6. doi: 10.1145/2593069.2593236

4. M. T. Rahman, F. Rahman, D. Forte and M. Tehranipoor, "An Aging-Resistant RO-PUF for Reliable Key Generation," in IEEE Transactions on Emerging Topics in Computing, vol. 4, no. 3, pp. 335-348, July-Sept. 2016. doi: 10.1109/TETC.2015.2474741

5. K. Xiao, M. T. Rahman, D. Forte, Y. Huang, M. Su and M. Tehranipoor, "Bit selection algorithm suitable for high-volume production of SRAM-PUF," 2014 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), Arlington, VA, 2014, pp. 101-106. doi: 0.1109/HST.2014.6855578

(ii) Five other significant products

1. M. T. Rahman, D. Forte, F. Rahman and M. Tehranipoor, "A pair selection algorithm for robust RO-PUF against environmental variations and aging," 2015 33rd IEEE International Conference on Computer Design (ICCD), New York, NY, 2015, pp. 415-418. doi: 10.1109/ICCD.2015.7357137

2. M. T. Rahman, D. Forte, Xiaoxiao Wang and M. Tehranipoor, "Enhancing noise sensitivity of embedded SRAMs for robust true random number generation in SoCs," 2016 IEEE Asian Hardware-Oriented Security and Trust (AsianHOST), Yilan, 2016, pp. 1-6. doi: 10.1109/AsianHOST.2016.7835559

3. P. Kumari, B. M. S. Bahar Talukder, S. Sakib, B. Ray and M. T. Rahman, "Independent Detection of Recycled Flash Memory: Challenges and Solutions," in IEEE Hardware-Oriented Security and Trust Symposium (HOST), 2018. (In press)

4. Md Tauhidur Rahman, Domenic Forte, Quihang Shi, G. K. Contreras and Mark Tehranipoor, "CSST: Preventing distribution of unlicensed and rejected ICs by untrusted foundry and assembly," 2014 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT), Amsterdam, 2014, pp. 46-51. DOI: 10.1109/DFT.2014.6962096.

5. Z. Guo, X. Xu, M. T. Rahman, M. M. Tehranipoor and D. Forte, "SCARe: An SRAM-Based Countermeasure Against IC Recycling," in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 26, no. 4, pp. 744-755, April 2018. doi: 10.1109/TVLSI.2017.2777262

Synergistic Activities

1. Session Chair and Moderator, International Conference on Computer Aided Design, 2017.
2. Technical Committee Member of IEEE International Conference on Consumer Electronics (ICCE), 2017, 2018.
3. Technical Committee Member of International Symposium for Testing and Failure Analysis in Phoenix, Arizona, 2018.
4. Reviewer of hardware security articles for IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, IEEE Transactions on Dependable and Secure Computing, and few more.
5. One NSF review panel, Last week of May, 2018.

SCEEE DEVELOPMENT FUND GRANTS
Budget Sheet

DEPT./ORGANIZATION Electrical & Computer Engineering The University of Alabama in Huntsville	TITLE LDHSP: Exploiting DRAM Latency Variations for Generating Hardware-based Security Primitives	PROPOSED START DATE **July 1, 2018**
PRINCIPAL INVESTIGATOR Dr. Tauhidur Rahman	SPONSOR Southeastern Center For Electrical Engineering Education (SCEEE)	PROPOSED DURATION 12 months

ITEM	AMOUNT REQUESTED FROM SCEEE	INSTITUTION COST SHARING
SALARIES: LIST BY PERSON MONTHS FACULTY PRINCIPAL INVESTIGATOR Dr. Tauhidur Rahman FY/AY (0.17) months $1,000 amount SUM (0.59) months $ 21,600 amount	$730	$15,766
GRADUATE ASSISTANT TBD FY/AY(50%) months $ 15,541 amount SUM (50%) months $_____ amount	$12,951	$2,590
STUDENT LABOR	$0	$0
TRAVEL	$2,000	$0
EQUIPMENT	$0	$0
MATERIALS AND SUPPLIES	$3,000	$0
OTHER CHARGES (specify)	$0	$0
FRINGE BENEFITS % of	$6,819	$7,144
INDIRECT COSTS (not allowed)		
TOTAL PROJECT COST	$25,500	$25,500

P.I. SIGNATURE	DIRECTOR SIGNATURE (IF APPLICABLE)	DATE
05/15/2018		05/15/2018
DEPT. CHAIR SIGNATURE	DEAN SIGNATURE	DATE
		05/15/2018

REV. 01/01

THE UNIVERSITY OF
ALABAMA IN HUNTSVILLE

May 9, 2018

Dr. N. H. Younan

Re: SCEEE Development Fund Grant – Dr. Tauhidur Rahman

Dear Dr. Younan:

I wish to confirm that Dr. Tauhidur Rahman, Assistant Professor on a tenure-track in the Electrical and Computer Engineering Department at the University of Alabama in Huntsville has less than five years of academic experience and has not received a federal grant of $100K or more.

Sincerely,

Ravi Gorur
Professor and Chair

Department of Electrical and Computer Engineering
272 Engineering Building
Huntsville, AL 35899
t 256-824-6316
f 256-824-6803
www.ece.uah.edu
eceinfo@ece.uah.edu

THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

Jescia Sigh <jrs0044@uah.edu>

Re: SCEEE proposal

1 message

Ravi Gorur <ravi.gorur@uah.edu> Tue, May 15, 2018 at 10:10 AM
To: Tauhidur Rahman <mtr0011@uah.edu>
Cc: jrs0044@uah.edu

Dear Tauhid,

If your SCEEE proposal gets funded, the ECE department will be able to provide you 1:1 matching funds in the amount of $25,500 to meet the agency's required cost share.

Best,
Ravi

Dr. Ravi S. Gorur, Professor and Chair
Department of Electrical and Computer Engineering
The University of Alabama in Huntsville
Huntsville, AL 35899
Tel: (256) 824-5621
email: ravi.gorur@uah.edu