2015

Integrating emerging cryptographic engineering research and security education

Mehran Mozaffari Kermani

Reza Azarderakhsh

122nd ASEE Annual Conference & Exposition
June 14 - 17, 2015
Seattle, WA
Paper ID #11880

Integrating Emerging Cryptographic Engineering Research and Security Education

Prof. Mehran Mozaffari Kermani, Rochester Institute of Technology (COE)

Mehran Mozaffari Kermani received the B.Sc. degree in electrical and computer engineering from the University of Tehran, Tehran, Iran, in 2005, and the M.E.Sc. and Ph.D. degrees from the Department of Electrical and Computer Engineering, University of Western Ontario, London, Canada, in 2007 and 2011, respectively. He joined the Advanced Micro Devices as a senior ASIC/layout designer, integrating sophisticated security/cryptographic capabilities into a single accelerated processing unit.

In 2012, he joined the Electrical Engineering Department, Princeton University, New Jersey, as an NSERC post-doctoral research fellow. Currently, he is with the Department of Electrical and Microelectronic Engineering, Rochester Institute of Technology, Rochester, NY. His current research interests include emerging security/privacy measures for deeply embedded systems, cryptographic hardware systems, fault diagnosis and tolerance in cryptographic hardware, VLSI reliability, and low-power secure and efficient FPGA and ASIC designs.

Currently, he is serving as an Associate Editor for the ACM Transactions on Embedded Computing Systems and the lead Guest Editor for the IEEE Transactions on Computational Biology and Bioinformatics for the special issue of Emerging Security Trends for Biomedical Computations, Devices, and Infrastructures (2015 and 2016). Moreover, he has served as the lead Guest Editor of the IEEE Transactions on Emerging Topics in Computing for the special issue of Emerging Security Trends for Deeply-Embedded Computing Systems (2014 and 2015). He is currently serving as the technical committee member for a number of related conferences including DFT, FDTC, RFIDsec, LightSEC, and WAIFI.

He was a recipient of the prestigious Natural Sciences and Engineering Research Council of Canada Post-Doctoral Research Fellowship in 2011 and the Texas Instruments Faculty Award (Douglas Harvey) in 2014.

Prof. Reza Azarderakhsh, Rochester Institute of technology

Reza Azarderakhsh received the BSc degree in electrical and electronic engineering in 2002, the MSc degree in computer engineering from the Sharif University of Technology in 2005, and the PhD degree in electrical and computer engineering from the University of Western Ontario in 2011. He was with the Department of Electrical and Computer Engineering, University of Western Ontario, as a Limited Duties Instructor, in 2011. He was a recipient of the Natural Sciences and Engineering Research Council of Canada (NSERC) Post-Doctoral Research Fellowship in 2012. He has been an NSERC post-doctoral research fellow with the Center for Applied Cryptographic Research at the Department of Combinatorics and Optimization, University of Waterloo. Currently, he is a faculty member with the Department of Computer Engineering at Rochester Institute of Technology. His current research interests include finite field and its application, high-performance computation, elliptic curve cryptography, and pairing based cryptography. He is a member of the IEEE.

Integrating Emerging Cryptographic Engineering Research and Security Education

Abstract

Unlike traditional embedded systems such as secure smart cards, emerging secure deeply-embedded systems, e.g., implantable and wearable medical devices, have larger "attack surface". A security breach in such systems which are embedded deeply in human bodies or objects would be life-threatening, for which adopting traditional solutions might not be practical due to tight constraints of these often-battery-powered systems. Unfortunately, although emerging cryptographic engineering research mechanisms have started solving this critical problem, university education (at both graduate and undergraduate level) lags comparably. One of the pivotal reasons for such a lag is the multi-disciplinary nature of the emerging security bottlenecks (mathematics, engineering, science, and medicine, to name a few). Based on the aforementioned motivation, in this paper, we present an effective research and education integration strategy to overcome this issue at Rochester Institute of Technology. Moreover, we present the results of more than one year implementation of the presented strategy at graduate-level through "side-channel analysis attacks" case studies. The results of the presented work show the success of the presented methodology while pinpointing the challenges encountered compared to traditional embedded system security research/teaching integration.

Introduction

Embedded system security is one of the main concerns of any nation with direct organizational, societal, and economical effects. The growing number of instances of security breaches in the last few years has created a compelling case for efforts towards securing such systems[1], and refining new research and teaching trends[2, 3]. It is known that the number of embedded devices in use, currently, is about two orders of magnitude higher than that of desktops and it is envisioned that deeply-embedded systems follow such trend as well.

Unlike traditional embedded systems, deeply-embedded systems which are deployed in human bodies and objects have two distinct characteristics, differentiating them from the traditional ones. First, such systems are embedded into very sensitive environments, e.g., cardiovascular defibrillators embedded into human bodies which perform therapeutic tasks or insulin pump/glucose monitoring pairs which are used for diagnosis and therapy[4, 5]. A security breach here is life-threatening and unlike traditional embedded systems such as smart cards in which financial loss is the result of the breach, here, catastrophic and vitally-adverse problems are inevitable.

The other pivotal concern in deploying traditional cryptographic architectures into deeply-embedded systems [both hardware through application-specific integrated circuits (ASICs) and field-programmable gate arrays (FPGAs), and software through microcontrollers] is the potential, unacceptable degradation of performance and implementation metrics[5]. For instance, if the security protection schemes for a pacemaker (typically battery-powered to perform medical tasks for roughly 10 years) lead to its battery depletion in 6 months, the resulting (now secure) device would be unacceptable, life-threatening, and impractical to use.

In this paper, we present integrating emerging cryptographic engineering (used for protecting the aforementioned deeply-embedded systems) research with security education. This project is addressing the respective tradeoffs between the security levels (noting the larger attack surface for deeply-embedded systems) and affording the overheads applicably, which are the two main facets of the proposed integration. To meet this objective, we have used such methodology for more than a year in educating graduate students at Rochester Institute of Technology and brought them very well up to speed which resulted in successful research (publications in top-tier electrical and computer engineering *IEEE Transactions* journals for the case study of side-channel analysis attacks and reliability).

We have had the following goals in such integration:

(a) Exposing the challenges of deeply-embedded system security education;
(b) Hardware and software secure system co-design teaching and research integration (in previous work, theory and practice are combined for such purpose: A co-design course applying symmetric key ciphers has been presented[6], a helicopter-like robot motion control has been implemented[7], and co-design as an emerging discipline in education has been discussed[8]);
(c) Developing a respective multi-disciplinary laboratory for both research and teaching of hardware/software security; and
(d) Advancing education through inter- and intra-university research collaborations (it is noted that the authors of this work are from different and diverse backgrounds).

We note that a cryptographic system was chosen for deeply-embedded security integration of research and teaching for a number of reasons: (a) efficient and practical use of cryptography will be one of the major schemes in providing security in future deeply-embedded systems and (b) the cryptographic architectures are modular thus dividing the tasks in performing research or instructing in multiple independent sessions is possible.

The rest of the paper is organized as follows. First, we present select topics and sub-topics essentially needed for cryptographic engineering research and teaching integration. Next, the integration methodology is explained through a case study. This includes the challenges for the experimented studies. The paper is concluded by summarizing the project's results.

Research/Teaching Topic Essentials

Although there are few resources very specific to embedded systems security education (not typically designed for undergraduate or college/university level education[9, 10]), deeply-embedded systems security challenges and mechanisms have not been subject of specific readings/books for teaching and educational purposes, to the best of authors' knowledge. As such, in order to provide select topics and sub-topics essentially needed for cryptographic engineering research/teaching integration, we need to differentiate the materials used in embedded security courses[11, 12] and the ones specific to deeply-embedded security for the purpose of integration in this paper. Table 1 presents select topics we have considered in the integration process. We note that the topics presented can be extended to a larger, more comprehensive list. Nonetheless, because the presented work is scalable, such extension is acceptable and possible (based on the security requirements, the overheads that can be tolerated, and the usage models).

Table 1. Select topics essentially needed for cryptographic engineering research/teaching integration

Select topics	Select sub-topics
Cryptographic implementations	• Hardware architectures for deeply-embedded systems • Cryptographic embedded processors and co-processors • Hardware accelerators • Physical unclonable functions (PUFs) • Efficient embedded software implementations
Implementation attacks	• Side-channel attacks and countermeasures targeting deeply-embedded systems • Fault attacks and countermeasures (considering practical attacks for deeply-embedded hardware)
Tools and methodologies	• Computer aided cryptographic engineering • Metrics for the security of embedded systems • Secure programming techniques • FPGA design security (embedded hardware) • Topics related to post-quantum cryptography • Topics related to machine learning security
Applications	• Cryptography for deeply-embedded systems • Reconfigurable hardware for cryptography (embedded hardware) • Technologies and hardware for content protection • Trusted computing platforms deeply-embedded into human body or objects

As the main objective of this paper is integration of research and teaching, we refrain from presenting the topics used for education purposes only and are not the results of our prior research work. However, it is useful to note that a specific course in deeply-embedded systems security (and as such, a potential textbook) may have four main readings/chapters, i.e., the select topics in Table 1 in addition to, typically, an Introduction and a Discussion. Moreover, we note that such course/reading needs to take into account the level of readers (undergraduate- or graduate-level, for instance) and, accordingly, needs to be tailored noting different considerations including real-world examples (to encourage the students and give them the context), references to the state-of-the-art (for undergraduate students, specifically, to encourage graduate-level studies), platforms for hardware and software (free-of-charge platform tools for simulations/syntheses/implementations, for instance), to name a few.

Integration of Side-Channel Analysis Research/Teaching

To present the results of our teaching and research integration, we have used “side-channel analysis attacks” as our topic at Rochester Institute of Technology. Any attack based on information gained from the physical implementation of a cryptosystem (on hardware or

software), rather than brute force or theoretical weaknesses in the algorithms is denoted as side-channel analysis. For example, timing information or power consumption can provide an extra source of information which can be exploited to break the system. There are two main reasons for such a choice: (a) this topic is related to many other topics in Table 1 and, thus, allows us to cover a large number of topics/sub-topics used for cryptographic engineering research/teaching integration. These related topics and sub-topics include "hardware architectures for deeply-embedded systems", "side-channel attacks and countermeasures targeting deeply-embedded systems", "fault attacks and countermeasures (considering practical attacks for deeply-embedded hardware)", "FPGA design security (embedded hardware)", "cryptography for deeply-embedded systems", "reconfigurable hardware for cryptography (embedded hardware)", "technologies and hardware for content protection", and "trusted computing platforms deeply-embedded into human body or objects", and (b) the authors have extensive experience with the topic, making it suitable to analyze and elaborate.

Phase 1. Identifying the Challenges of Education for Initiating Research: A group of five students who perform research under the supervision of the authors of this work was chosen (we note that although the focus has been on the aforementioned topic, some students were directed to work on general "reliability" approaches to broaden the focus beyond cryptography). Active side-channel attacks topic through fault injection has been selected as it combines simulations and implementations for which the students acquired knowledge through choosing three textbooks and instruction of the authors: "Error Control Coding"[13], "Fault-Tolerant Systems"[14], and "Cryptography Engineering"[15]. The objective of this phase was to familiarize the students through education-based instruction with the topic of the research. The outcome was satisfactory although the third textbook, i.e., "Cryptography Engineering", was mainly used as reference.

One of the main goals of this phase was to expose the challenges of deeply-embedded systems security education. The aforementioned textbooks were fit resources for the research; yet, they were not sufficient for the topics covered in this project. Thus, the first challenge was to find resources directly related to deeply-embedded systems security education. As this is an emerging topic and includes studying emerging cryptographic engineering, in addition to these three books, students were directed to read select articles from three conferences in the field: Cryptographic Hardware and Embedded Systems (CHES)[16], Fault Diagnosis and Tolerance in Cryptography (FDTC)[17], and Hardware-Oriented Security and Trust (HOST)[18]. The second challenge was the multi-disciplinary nature of the topic chosen (electrical engineering, computer engineering, mathematics, computer science, and the like). Although this challenge necessities having students with diverse backgrounds, the expertise of authors in these topics helped filling the gap in cases where students were not acquainted with the field of study. Moreover, knowing such gap, the instructors (authors of this work) consulted with faculty members from other departments (especially computer science and mathematics) to meet the teaching objectives.

Phase 2. Research and Development: Differential fault analysis is a variant of side-channel analysis attacks in the field of cryptography (active sub-variant). The principle in such attacks is to induce faults maliciously (intentionally injecting faults into the architectures of crypto-systems) to reveal their internal states.

With respect to deeply-embedded systems, for instance, a pacemaker containing an embedded processor might be subjected to a number of conditions, e.g., high temperature, unsupported supply voltage or current, excessively high overclocking, strong electric or magnetic fields, or

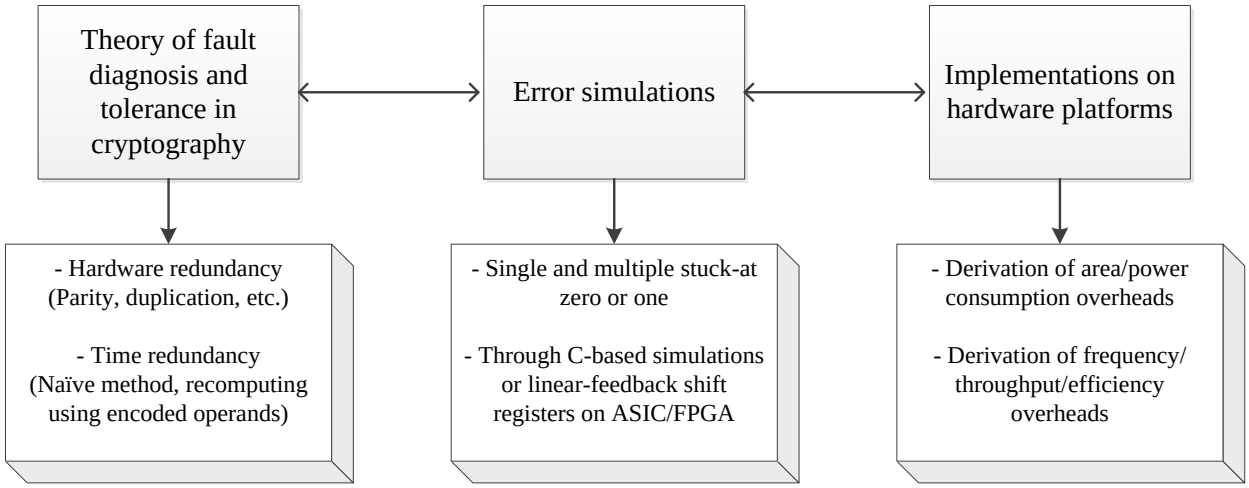

Figure 1. Sub-parts of the presented research scheme for integrating with teaching in this work.

ionizing radiation, to influence the operation of the processor (here the processor is an ASIC architecture typically; yet, FPGAs containing the designs of cryptographic algorithms can very similarly be attacked). After such fault attack, the processor on the pacemaker may begin to output incorrect results due to physical data corruption. Such erroneous output may help a cryptanalyst deduce the instructions that the processor is running.

Many countermeasures (typically based on error detection schemes) have been proposed to defend from this attack. Therefore, using the previous experience of the authors, a group of students were instructed the background topics[13-18], and the teaching tasks were followed as seen in the flowchart of Fig. 1, including three sub-parts: (a) theory of fault diagnosis and tolerance in cryptography, (b) simulation steps for error coverage derivation for single/multiple stuck-at zero/one faults, and (c) implementation on hardware platforms, i.e., ASIC (Synopsys tools) and FPGA (Xilinx tools), to derive the overheads induced.

Finally, we have given three sub-cases to the students: (a) low-complexity block ciphers which are more lightweight than the Advanced Encryption Standard (AES), (b) public-key cryptography with the case elliptic-curve cryptography (ECC), and (c) non-cryptography computer arithmetic architectures (e.g., complex division) whose reliability assurance is critical. These sub-cases have been selected carefully to cover a wide-range of applications. It is worth mentioning that the authors of this work have extensive background on fault detection and tolerance in many fields including cryptography[19-34].

Phase 3. Integration of Research and Teaching: The last phase included integrating the research on emerging cryptographic engineering with teaching. For this objective, we have built on the research of a group of graduate students in the second phase during the academic year of 2013-2014 and used the lessons learnt in the integration process.

The first note here is engaging students in non-traditional learning activities for understanding the deeply-embedded system security topics shown in Table 1. This included (a) asking them to read research papers and explain the core of research on deeply-embedded system security, (b) contacting the authors of research papers through email to broaden the understating, and (c) having discussion sessions among themselves and share the learning materials including but not limited to simulation and implementation environment, typesetting details, and the like.

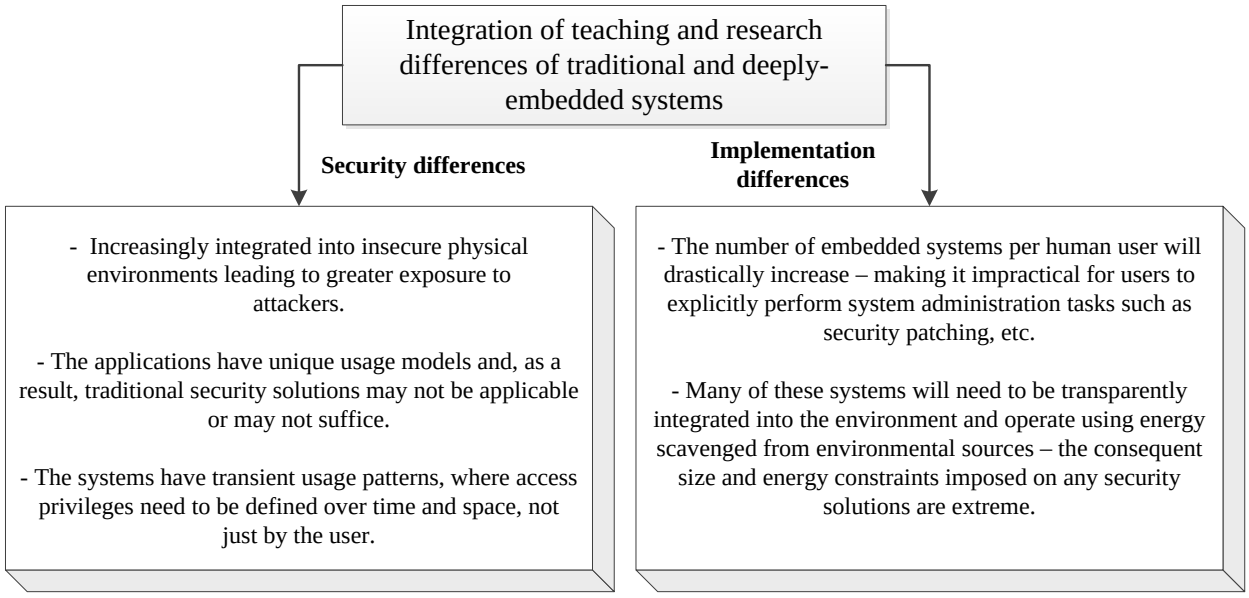

Figure 2. Traditional *vs.* deeply-embedded security teaching and research integration.

The second step was to contrast traditional embedded security and deeply-embedded security based on the differences between these two. Fig. 2 shows the major differences taught to the students which were partly results of prior research work in 2013-2014 academic year at Rochester Institute of Technology; thus, a step-forward towards integration of emerging cryptographic engineering teaching and research.

The third step is to identify the modularity of different cryptographic algorithms such as AES and ECC to apply fault diagnosis and tolerance techniques specified for deeply-embedded systems. Fig. 3 shows such modularity for ECC which was instructed to the students and noted that in order to have applicable fault diagnosis methods for ECC for deeply-embedded systems (for instance, processors of pacemakers), we need to have low overhead and high error coverage. In Fig. 3, the hierarchy of computation of ECC is depicted which is known as ECC Pyramid (this was explained in detailed to the students, which is not elaborated here for the sake of brevity). As one can see, on the top of the pyramid, security establishment protocols such as elliptic curve Diffie-Hellman (ECDH), digital signature algorithm (ECDSA), and integrated encryption scheme (ECIES) are placed. In all of these security protocols which are standardized by several national and international organizations, the main computation is point multiplication. The elliptic curve point multiplication is defined as $Q = k.P$, where k is a positive integer, and Q and P are two points on the elliptic curve. The efficiency of computing point multiplication depends on finding the minimum number of steps to reach Q from a given point P.

Some of the *educational goals* in this step were (a) understanding the implementation platforms (commonly referred to as hardware [ASIC/FPGA] or software platforms [microcontrollers]) through which the overheads were derived, (b) soft skills including presentation of the results of deeply-embedded security research orally or in writing, team-work, decision-making, and the like, and (c) hard technical skills for simulations and implementations of the fault diagnosis schemes for crypto-systems including those based on AES and ECC.

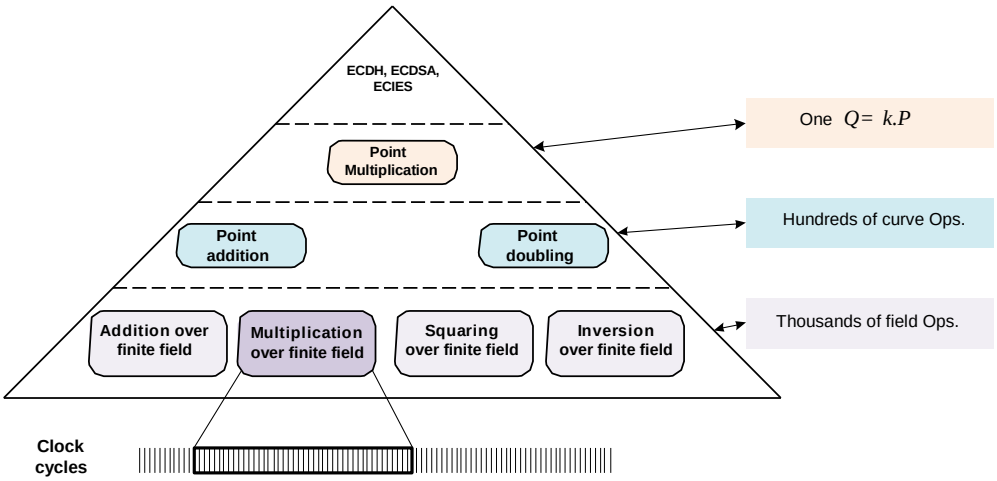

Figure 3. Hierarchy of the ECC operations used in differentiating traditional and embedded system security for integrating research/teaching.

The security assessment is based on the resources in the already-developed "Applied Cryptography" laboratory; the research is conducted by the graduate students. The experiments will be part of two relevant graduate/undergraduate courses taught by the authors. The form of outcome of the assessment will be mostly in programming languages specially hardware description languages of cryptographic algorithms developed in the courses as final projects.

Teaching and Research Integration Complications

In what follows, we present through three instances, the complications we had in the integration process for three steps of theory, simulation, and implementation.

Theory: The theory of fault detection and tolerance with respect to cryptography is broad and includes different methods with redundancy of hardware and time. Such methods were instructed to the students through the aforementioned books. Nevertheless, a major complication here was that the reliability approaches taught might not be suitable for fault attack immunity. Specifically, the attackers might use entropy-aware injections to bypass the solutions. Through the research work done in 2013-2014 academic year, we had identified very carefully different reliability approaches; yet, we refined them to have specific applicability to fault attacks in the second round and during the integration phase.

Simulation: Single stuck-at fault injection in ASIC and FPGA platforms are usually done for assessing the effectiveness of the proposed fault diagnose methods. Nevertheless, the injection locations depend on the specific problem to solve, e.g., AES or ECC architectures. Thus, a challenge here is that the integration of research and teaching becomes very application-specific and dynamic with respect to simulations. A second challenge here is the choice of hardware or software based injections through C++ or LFSRs. This is again very dependent on the nature of research, for instance, a simple reason to choose one method over another would be the availability of source codes in hardware or software. These two and several other environment and application specific choices make the integration of "simulation" step as a number of general guidelines rather than specific schemes.

Implementation: Finally, the complications in the implementation step usually relate to the resources available (ASIC and FPGA tools and hardware, for instance). Therefore, for such a choice, general guidelines are preferred. We note that such a choice affects the implementation and performance metrics as well; thus, the integration need to be tailored based on the usage models.

Discussions and Lessons Learnt

High level research is seen as driver of economic growth. Increasing the number of students pursuing research towards graduate studies is also important for economic and social growth. As such, one of the main objectives of this paper is to focus on an extremely-sensitive research area and perform pedagogical developments and drive to improve student experience of research-led teaching and integration of research/teaching.

After integrating the research performed in 2013-2014 by authors (and select previous research work), the integration of the results into teaching led to a number of useful lessons. We observed increased student engagement and deeper understanding through inquiry-led learning of fundamentals of deeply-embedded systems security (measured through project-based assessments). Such integration provided students with additional skills such as critical enquiry and evaluation of knowledge. We also believe that linkage of research and teaching in academic work makes university education distinctive (it was beneficial for the two departments the authors are affiliated with). Moreover, it certainly helped generating additional research output/knowledge creation and strengthened pathways to postgraduate research (we are currently working on two *IEEE Transactions* journal papers as a result of such creation). Finally, we believe our deeply-embedded security research and teaching integration helps develop student as *knowledge worker,* and engages them in concept of the provisionality of existing knowledge.

Deeply-embedded systems methodology, hard skill, and soft skill teaching goals were evaluated for graduate students working in the related research area (through the assessment of the research papers they were involved in and theory/simulation/implementation-based question asked). We also note that a comprehensive assessment later was done by the peer-review methodology of the authors' peers. Feedback was collected in the form of oral questions and discussions. The students were satisfied with the integration outcome and also their publications progress (typically both academia and industry value top-tier journal publications). The students also improved their understanding of the general areas of (a) cryptography, (b) security, (c) resource-constrained digital design, and (d) fault detection and tolerance in cryptography.

We note that the evaluation of success of integration of research and teaching has been performed by a group of research/teaching faculty members from diverse departments (electrical/computer engineering, security, and computer science). Data management has been a pivotal part of this integration, noting that the results are useful for advancing global education and with the aim of possible improvement from both research and education communities. Such results are possible through a closely-monitored data management plan for quality assurance of data which could be possibly modified by engineering industry and academia. The eventual outcome of this integration is a step-forward to fill the current gap of research in and education of emerging security mechanisms.

Let us discuss and present the lessons learnt from two the variants of the presented integration. First, in the teacher-focused variant of integration of emerging cryptographic engineering research and teaching, security research outcome was transmitted (see Fig. 4). This could include the results of, for instance, fault diagnosis and tolerance approaches in cryptography (AES or ECC) transmitted to the learners including but not limited to simulation results and implementation overhead. Then, the process through which such results are obtained was transmitted to the students, e.g., how to inject faults through C++ error simulations and/or LFSRs in hardware description languages, or how to implement and derive area/delay/power consumption overheads.

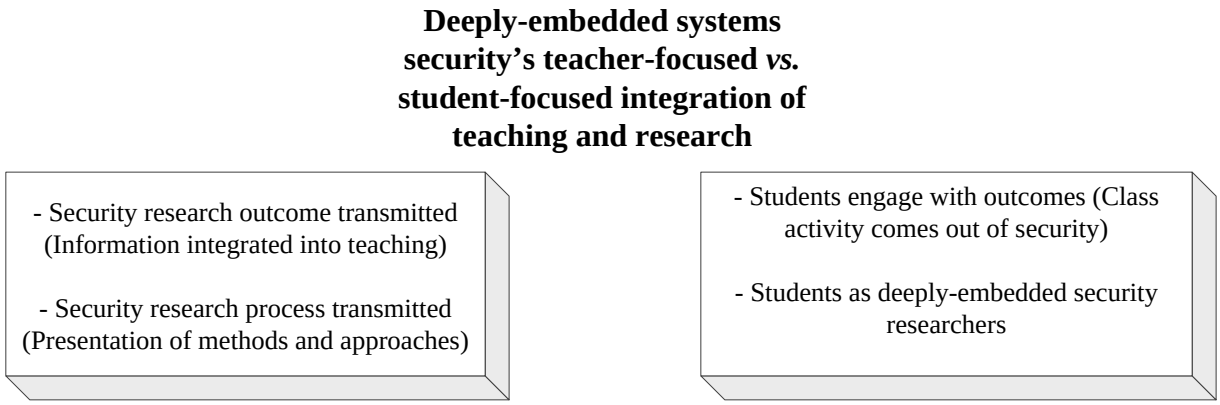

Figure 4. Comparison of the integration variants.

Second, in the student-focused variant of integration of emerging cryptographic engineering research and teaching, engagement is a must. Thus, students have been engaged in the outcomes and learnt to scrutinize the results and refine them through activities including discussions and re-simulation/re-implementation of the fault detection methods on ASIC and FPGA hardware platforms. Then, new problems were identified and students were engaged in performing the research process from literature review to final polishing for publications.

Conclusions

Computing platforms are expected to be deeply-embedded within physical objects and people (objects and human body are among two instances of sensitive environments), creating an Internet of Things (nano-Things). These sensitive embedded computing platforms will enable a wide spectrum of applications, including implantable medical devices, physical infrastructure monitoring, and intelligent transportation systems. Unfortunately, the explosion in devices and connectivity creates a much larger attack surface (opportunity for attackers to succeed.

In this paper, we have presented research and education integration of deeply-embedded systems security through emerging cryptography mechanisms. Moreover, we have presented the results of more than one year implementation of the presented strategy at graduate-level through "side-channel analysis attacks" case studies. The results of the presented work show the success of the presented work while pinpointing the challenges encountered compared to traditional embedded system security research/teaching integration.

Finally, we present the outcome of our work as follows:

(a) We were successful in exposing the challenges of deeply-embedded system security education through working closely with a number of students in the areas of cryptographic engineering and general reliability;
(b) Teaching and research integration was quite successful with respect to educational goals, assessments, and research outcome;
(c) We tested and evaluated the possibility of hardware and software secure system co-design teaching and research integration;
(d) Using the experience gained, lessons learnt for developing a respective multi-disciplinary laboratory for both research and teaching of hardware/software security (this is partly done and will be a future-work as step-forward for hands-on experiments); and
(e) Inter- and intra-university research collaborations were initiated and will be pursued to ensure delivering an expanded set of outcomes for the integration.

References

[1] S. Ravi, P. C. Kocher, R. B. Lee, G. McGraw, and A. Raghunathan, "Security as a new dimension in embedded system design," in *Proc. Design Automation Conference*, 2004, pp. 753-760.

[2] J. Zalewski, A. J. Kornecki, B. Denny Czejdo, F. Garcia Gonzalez, N. Subramanian, and D. Trawczynski, "Curriculum development for embedded systems security," in *Proc. ASEE Conf.*, 2014, pp. 1-7.

[3] L. Uhsadel, M. Ullrich, A. Das, D. Karaklajic, J. Balasch, I. Verbauwhede, and W. Dehaene, "Teaching HW/SW co-design with a public key cryptography application," *IEEE Trans. Education*, vol. 56, no. 4, pp.478-483, 2013.

[4] M. Zhang, A. Raghunathan, and N. K. Jha, "Trustworthiness of medical devices and body area networks," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1174-1188, 2014.

[5] M. Mozaffari-Kermani, M. Zhang, A. Raghunathan, and N. K. Jha, "Emerging frontiers in embedded security," in *Proc. VLSI Design*, 2013, pp. 203-208.

[6] P. Schaumont, "A senior-level course in hardware/software co-design," *IEEE Trans. Education*, vol. 51, no. 3, pp. 306-311, 2008.

[7] R. H. Klenke, J. H. Tucker, and J. M. Blevins, "A new hardware/software codesign environment and senior capstone design project for computer engineering," in *Proc. IEEE MSE*, Jun. 2003, pp. 66-67.

[8] W. Wolf, "A decade of hardware/software codesign," *Computer Journal*, vol. 36, no. 4, pp. 38-43, Apr. 2003.

[9] C. H. Gebotys, "Security in embedded devices," Springer-Verlag, New York, 2010.

[10] T. Stapko, "Practical embedded security," Elsevier/Newnes, Amsterdam, 2008.

[11] Cyber Security and Embedded Systems, https://pe.gatech.edu/courses/cyber-security-and-embedded-systems.

[12] Security of Hardware Embedded Systems, http://www.ece.rice.edu/~fk1/classes/ELEC528.htm.

[13] S. Lin and D. J. Costello, Error Control Coding, Prentice Hall, 2004.

[14] I. Koren and C. M. Krishna, Fault-Tolerant Systems, Elsevier Science, 2007.

[15] N. Ferguson, B. Schneier, and T. Kohno, Cryptography Engineering, Wiley, 2010.

[16] CHES Workshop, http://www.chesworkshop.org/.

[17] FDTC Workshop, http://conferenze.dei.polimi.it/FDTC15/.

[18] HOST Symposium, http://www.hostsymposium.org/.

[19] M. Mozaffari Kermani, N. Manoharan, and R. Azarderakhsh, "Reliable radix-4 complex division for fault-sensitive applications," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, Accepted and to be published in 2015.

[20] M. Mozaffari Kermani, R. Azarderakhsh, and A. Aghaie, "Reliable and error detection architectures of Pomaranch for false-alarm-sensitive cryptographic applications," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, Accepted and to be published in 2015.

[21] M. Mozaffari Kermani, K. Tian, R. Azarderakhsh, and S. Bayat-Sarmadi, "Fault-resilient lightweight cryptographic block ciphers for secure embedded systems," *IEEE Embedded Sys.*, vol. 6, no. 4, pp. 89-92, Dec. 2014.

[22] S. Bayat-Sarmadi, M. Mozaffari Kermani, and A. Reyhani-Masoleh, "Efficient and concurrent reliable realization of the secure cryptographic SHA-3 algorithm," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 33, no. 7, pp. 1105-1109, Jul. 2014.

[23] M. Mozaffari Kermani, R. Azarderakhsh, C. Lee, and S. Bayat-Sarmadi, "Reliable concurrent error detection architectures for extended Euclidean-based division over GF(2^m)," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 22, no. 5, pp. 995-1003, May 2014.

[24] Mozaffari Kermani and R. Azarderakhsh, "Efficient Fault Diagnosis Schemes for Reliable Lightweight Cryptographic ISO/IEC Standard CLEFIA Benchmarked on ASIC and FPGA," *IEEE Trans. Ind. Electron.*, vol. 60, no. 12, pp. 5925-5932, Dec. 2013.

[25] M. Mozaffari Kermani and A. Reyhani-Masoleh, "A Low-Power High-Performance Concurrent Fault Detection Approach for the Composite Field S-box and Inverse S-box," *IEEE Trans. Comput.*, vol. 60, no. 9, pp. 1327-1340, Sep. 2011.

[26] M. Mozaffari Kermani and A. Reyhani-Masoleh, "A Lightweight High-Performance Fault Detection Scheme for the Advanced Encryption Standard Using Composite Fields," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 19, no. 1, pp. 85-91, Jan. 2011.

[27]. M. Mozaffari Kermani and A. Reyhani-Masoleh, "Concurrent Structure-Independent Fault Detection Schemes for the Advanced Encryption Standard," *IEEE Trans. Comput.*, vol. 59, no. 5, pp. 608-622, May 2010.

[28]. M. Mozaffari Kermani and A. Reyhani-Masoleh, "Fault Detection Structures of the S-boxes and the Inverse S-boxes for the Advanced Encryption Standard," *J. Electronic Testing: Theory and Applications (JETTA)*, vol. 25, no. 4, pp. 225-245, Aug. 2009.

[29] M. Mozaffari Kermani and A. Reyhani-Masoleh, "Reliable hardware architectures for the third-round SHA-3 finalist Grostl benchmarked on FPGA platform," in *Proc. IEEE Int. Symp. Defect and Fault Tolerance in VLSI Systems (DFT)*, pp. 325-331, Vancouver, Canada, Oct. 2011.

[30]. M. Mozaffari Kermani and A. Reyhani-Masoleh, "A high-performance fault diagnosis approach for the AES SubBytes utilizing mixed bases," in *Proc. IEEE Workshop Fault Diagnosis and Tolerance in Cryptography (FDTC)*, pp. 80-87, Nara, Japan, Sep. 2011.

[31]. M. Mozaffari Kermani and A. Reyhani-Masoleh, "A lightweight concurrent fault detection scheme for the AES S-Boxes using normal basis," in *Proc. LNCS Cryptographic Hardware and Embedded Systems (CHES)*, pp. 113-129, Washington, D.C., USA, Aug. 2008.

[32]. M. Mozaffari Kermani and A. Reyhani-Masoleh, "A structure-independent approach for fault detection hardware implementations of the Advanced Encryption Standard," in *Proc. IEEE Workshop Fault Diagnosis and Tolerance in Cryptography (FDTC)*, pp. 47-53, Vienna, Austria, Sep. 2007.

[33]. M. Mozaffari Kermani and A. Reyhani-Masoleh, "Parity-based fault detection architecture of S-box for Advanced Encryption Standard," in *Proc. IEEE Int. Symp. Defect and Fault Tolerance in VLSI Systems (DFT)*, pp. 572-580, Washington, D.C., USA, Oct. 2006.

[34]. M. Mozaffari Kermani and A. Reyhani-Masoleh, "Parity prediction of S-box for AES," in *Proc. IEEE Canadian Conference on Electrical and Computer Engineering (CCECE)*, pp. 2357-2360, Ottawa, Canada, May 2006.