9-2016

Education and Research Integration of Emerging Multidisciplinary Medical Devices Security

Mehran Mozaffari Kermani
mmkeme@rit.edu

Reza Azarderakhsh
rxaeec@rit.edu

Mehdi Mirakhorli
mxmvse@rit.edu

Education and Research Integration of Emerging Multidisciplinary Medical Devices Security

Abstract

Traditional embedded systems such as secure smart cards and nano-sensor networks have been utilized in various usage models. Nevertheless, emerging secure deeply-embedded systems, e.g., implantable and wearable medical devices, have comparably larger "attack surface". Specifically, with respect to medical devices, a security breach can be life-threatening (for which adopting traditional solutions might not be practical due to tight constraints of these often-battery-powered systems), and unlike traditional embedded systems, it is not only a matter of financial loss. Unfortunately, although emerging cryptographic engineering research mechanisms for such deeply-embedded systems have started solving this critical, vital 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. Based on the aforementioned motivation, in this work, at Rochester Institute of Technology, we present an effective research and education integration strategy to overcome this issue in one of the most critical deeply-embedded systems, i.e., medical devices. Moreover, we present the results of two years of implementation of the presented strategy at graduate-level through fault analysis attacks, a variant of side-channel attacks. We note that the authors also supervise an undergraduate student and the outcome of the presented work has been assessed for that student as well; however, the emphasis is on graduate-level integration. 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 of medical devices security. We would like to emphasize that our integration approaches are general and scalable to other critical infrastructures as well.

Introduction

Security and privacy of embedded systems have been center of attention in research and teaching whose compromise has direct organizational, societal, and economical adverse effects. Embedded systems in critical infrastructures, smart homes, smart fabrics, and similar smart platforms need to be secure to transfer data in private manner. Medical devices, e.g., implantable and wearable medical devices (IWMDs) which are commonly used for diagnosing, monitoring, and treating various medical conditions, are among the most critical smart platforms. Similar to other emerging usage models, a general trend is toward increased functional complexity and connectivity, resulting in larger attack surface. The growing number of instances of security breaches in the last few years in such extremely sensitive usage models has created a compelling case for efforts towards securing such systems[1,2,3,4,5,6], and refining new research and teaching trends[7, 8]. Deeply-embedded systems such as medical devices will dominate the future of traditional embedded systems and will likely get wide-spread adoption about 100 times more compared to traditional desktops.

IWMDs are generally categorized into 16 groups by the U.S. Food and Drug Administration (FDA): anesthesiology; cardiovascular; clinical chemistry and clinical toxicology; dental; ear, nose, and throat; gastroenterology and urology; general and plastic surgery; general hospital and personal use; hematology and pathology; immunology and microbiology; neurology; obstetric

and gynaecologic; opthalmic; orthopedic; physical medicine; and radiology[9]. Many of such devices are able to communicate through wireless means. These, unlike traditional embedded systems, have three distinct characteristics, differentiating them from the traditional ones. First, such IWMDs are embedded deeply into human bodies, e.g., cardiovascular defibrillators embedded into human bodies which perform therapeutic tasks or Glucose Monitor and Insulin Pump monitoring pairs which are used for diagnosis and therapy. 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. Second, they are already developed and in wide-spread use and any change to provide security would require tremendous efforts. Third, the area/delay/power consumption and, in general, the implementation and performance metrics of these devices cannot, in most of the cases, tolerate the burden of the cryptographic algorithms used for traditional embedded systems. Specifically, for both hardware through application-specific integrated circuits (ASICs) and field-programmable gate arrays (FPGAs), and software through microcontrollers, the potential unacceptable degradation of performance and implementation metrics is a meaningful concern for medical devices security. For instance, if the security protection schemes for a pacemaker (typically battery-powered to perform medical tasks for years) lead to its battery depletion in months instead of years, the resulting secure device would be life-threatening and impractical.

Contributions

There have been previous efforts for integrating research and teaching in traditional systems; nonetheless, to the best of our knowledge, a practical solution and an effective assessment strategy have not been adopted for emerging usage models integration such as IWMDs. Our pedagogical hypothesis is that emerging security research (through cryptographic solutions) can be integrated in university education considering three teaching and learning approaches; (a). Developing a respective multi-disciplinary laboratory (engineering, mathematics, and biomedicine in particular) for both research and teaching, (b). Advancing education through inter- and intra-university research collaborations in the aforementioned fields, and (c). Assessing the outcome through detailed benchmarks. The authors of this work are from different and diverse backgrounds and have prior expertise in the topic proposed (both teaching and research) and have been with world-known security and cryptography groups. This project is addressing the respective tradeoffs between the IWMDs security levels and affording the overheads. To meet this objective, we have used such methodology for two years in educating graduate students 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 fault analysis attacks).

The assessment strategy for the proposed integration is two-fold. A pilot project is developed (through work of undergraduate and graduate students) for testing the pedagogy in three phases: (a) education, (b) research, and (c) integration. The education phase takes into account the multi-disciplinary aspects of the project and in the research phase, publishing through the outcomes of the education phase is the priority. Security integration assessment is based on the resources in the already-developed laboratory.

Programming languages, especially hardware description languages of cryptographic algorithms developed in the courses, are used as final projects. The evaluation of success of integration of

research and teaching is performed by a group of research/teaching faculty members with diverse departments. The results will be placed on the world-wide web for advancing global education and with the aim of possible improvement from both research and education communities. The eventual outcome of this integration is a step-forward to fill the current gap of emerging security teaching/research integration for IWMDs.

We have had the following goals in such integration:

(a) Assess and benchmark the complications in IWMDs security and privacy;
(b) Evaluate co-design for hardware and software platforms teaching and research integration. Indeed, in previous work, co-design architectures through symmetric key block ciphers have been evaluated[10], motion control robots have been implemented[11], and co-design education has been researched[12]);
(c) IWMDs, and in general, deeply-embedded systems security teaching and research challenges and complications benchmark in practice through developing a respective multi-disciplinary laboratory; and
(d) Rochester Institute of Technology-based collaboration as well as inter-university research work for advancing education with respect to IWMDs security and privacy.

The rest of the paper is organized as follows. Related to IWMDs, we present topics needed for cryptographic engineering research and teaching integration. Furthermore, the methodology for integration is explained through a case study, covering both the challenges for the experimented studies and the routes to dissolve them. Finally, we summarize the paper.

Essential (Sub)-Topics for Research/Teaching

It is known that there exist select resources specifically suitable for embedded systems security education[13, 14], nevertheless, medical devices (IWMDs) security challenges have not been subject of specific readings for educational purposes, to the best of authors' knowledge. To provide select topics and sub-topics (the list includes select items but it does not confine the approach and can be broadened) required for cryptographic engineering used for IWMDs security research/teaching integration, we would like to first differentiate the materials used in embedded security courses[15, 16] and the ones specific to IWMDs. Table 1 presents select topics considered in the integration process.

Because the main objective of this paper is integration of research and teaching related to IWMDs security, we exclude 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 graduate or undergraduate level course in IWMDs systems security (and thus a potential textbook) may have a number of readings/chapters, i.e., the select topics in Table 1 in addition to, typically, an Introduction and a Discussion. Level of readers in such course/reading needs to be taken into account (undergraduate- or graduate-level, for instance) and, accordingly, needs to be tailored noting different considerations including real-world examples for IWMDs (to encourage the students and give them the context within different medical fields), references to the state-of-the-art IWMDs security mechanisms and respective solutions (for undergraduate students, specifically, to encourage graduate-level studies), platforms for hardware [ASIC/FPGA from different vendors such as Xilinx/Altera/Synopsys tools, to name a few] and software (free-of-charge platform tools for simulations/syntheses/implementations, for instance), to name a few.

Table 1. IWMDs security through cryptographic engineering research/teaching integration topics

Select topics	Select sub-topics
Reliable design of IWMDs	• Hardware and software architectures for IWMDs • Fault tolerance of IWMDs architectures • Design for test and reliability • Battery-power preservation • Dependability requirements
Cryptographic solutions for IWMDs	• Cryptographic embedded processors and co-processors • Hardware accelerators for secure IWMDs • Efficient embedded software implementations
Side-channels and countermeasures	• Side-channel attacks and countermeasures targeting IWMDs • Fault attacks and countermeasures (considering practical attacks for IWMDs hardware implementations) • Power analysis and cache timing attacks
Case studies	• Implantable Cardioverter-Defibrillators • Microprocessor-Based Pacemaker Design
Risk assessment	• Battery power • Overhead tolerance • Efficiency measurement • Verification and safety
Cryptographic tools and methodologies	• Metrics for the security of embedded systems • Secure programming techniques • FPGA design security (embedded hardware)
Applications	• The Framework of Contextual Integrity • Trusted computing platforms deeply-embedded into human body • Economics of IWMDs security and privacy • FDA-relevant policies, solutions, and benchmark

Fault Analysis Attacks: Integration of Research and Teaching

Implementation attacks which are based on retrieving secret information from an implemented secure cryptographic algorithm are one of the major threats for such devices. In general, such attacks could be based on active measures (in which the device is modified, i.e., through active attacks, such as fault attacks; or through passive listening to the side-channels, such as power analysis attacks. Specifically, in fault analysis attacks, faults are injected and information is derived whereas in power analysis attacks, one would only listen to what is leaked, for example power traces. To present the results of our IWMDs security teaching and research integration, we have used "side-channel analysis attacks" as our topic. As mentioned, these are based on information gained from the physical implementation of a cryptosystem (on hardware or software), rather than brute force or theoretical weaknesses. As another example, cache timing information can provide an extra source of information which can be exploited to break the system.

The reason for selecting fault analysis attacks for providing our methodology is that, as seen in Table 1, this topic is related to many other topics, allowing us to cover a large number of sub-topics used for integration. Table 2 lists this relation (sub-topics are directly related whereas related other topics are related indirectly).

Table 2. Related topics to side-channels.

Topic	Sub-topics	Related other topics
Side-channels and countermeasures	- Side-channel attacks and countermeasures targeting IWMDs - Fault attacks and countermeasures (considering practical attacks for IWMDs hardware implementations) - Power analysis and cache timing attacks	- Hardware architectures for IWMDs - FPGA design security (embedded hardware) - Cryptography for IWMDs - Reconfigurable hardware for cryptography (embedded hardware) - Trusted computing platforms deeply-embedded into human body

Main Step 1. Identifying the Education Challenges: Two of the authors supervise students whose research focus is security and reliability (specifically fault diagnosis and tolerance in hardware). Fault analysis attacks (active side-channel attacks) topic through fault injection has been selected.

One of the main goals of this phase was to expose the challenges of IWMDs systems security education as follows:

- The first challenge was to find resources directly related to IWMDs security education which is an emerging topic. Some important resources are: USENIX Enigma conference (a new conference on emerging threats and novel attacks),

TROOPERS IT Security conference, U.S. House Cybersecurity Caucus, Health Privacy & Security Forum, U.S. Senate Hearing on IRS Breach, FDA Cybersecurity Workshop, NIST Information Security and Privacy Advisory Board on medical device security, Association for the Advancement of Medical Instrumentation Standards Week: Medical Device Security working group, Healthcare Technology Research and Advisory Council Secure Health, and Archimedes Medical Device Security Workshop.

- The second challenge was that the topic chosen is, in nature, multi-disciplinary. The expertise of authors in these topics helped filling the gap in cases where students were not acquainted with the field of study. The instructors (authors of this work) also consulted with faculty members from other departments (especially computer science and mathematics) to meet the teaching objectives.

Main Step 2. Research and Development: Fault analysis is an active sub-variant for side-channel attacks. In such implementation attacks, faults are injected maliciously (attackers want to inject transient faults not to break the system, so their plan is intentionally injecting faults into the architectures of crypto-systems to retrieve as much leaked sensitive information as possible).

With respect to IWMDs, for instance, a pacemaker containing an embedded hard processor, high temperature, unsupported supply voltage or current, excessively high overclocking, strong electric or magnetic fields, or ionizing radiation, are all the ways to assert faults 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).

Let us divide the research and development into two parts. Fig. 1 presents different topics in IWMDs security.

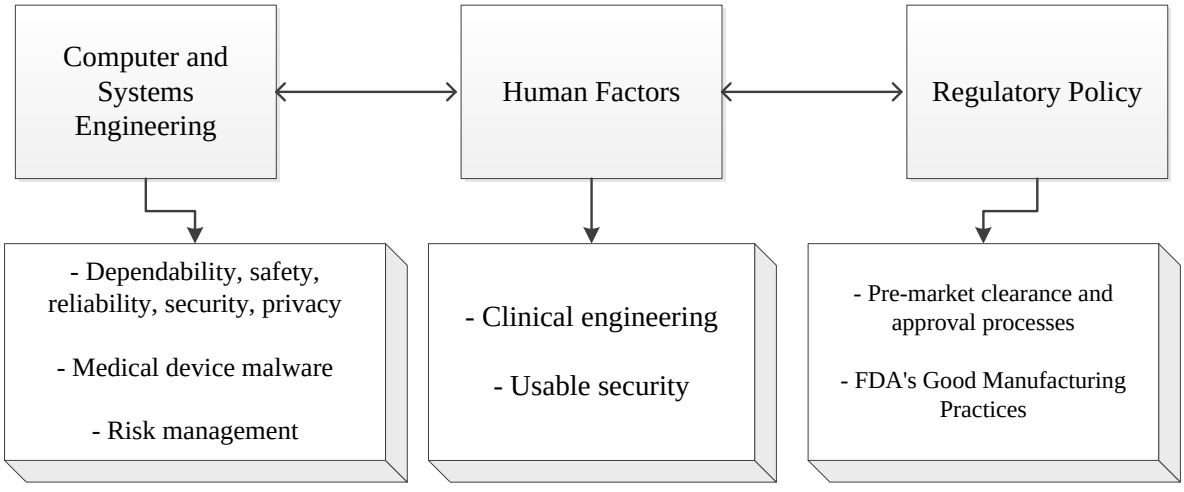

Figure 1. Different topics in IWMDs security.

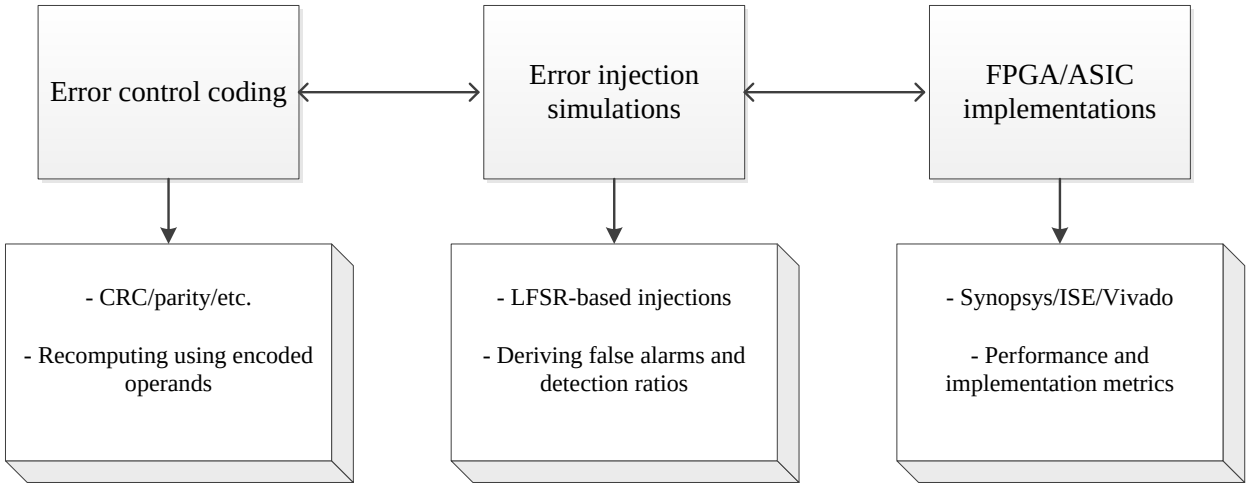

Figure 2. Sub-parts of the presented research scheme for integrating with teaching in this work.

Many error detection schemes have been proposed to defend against fault analysis attacks. We have followed the teaching tasks as seen in the flowchart of Fig. 2, including three sub-parts: (a) error control coding, (b) error injection simulations for error coverage derivation for single/multiple stuck-at zero/one, and (c) FPGA/ASIC implementations to derive the overheads.

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., CORDIC and Viterbi algorithms) whose reliability assurance is critical.

Main Step 3. Integration of Research and Teaching: For this step, we have built on the research of a group of graduate students in the second phase during the academic years of 2013-2014 and 2014-2015.

Engaging students in non-traditional learning activities: For understanding the IWMDs security, this step is pivotal. There are a number of sub-steps needed for this main step:

- Asking students to read research papers (venues include both security and medical domains) to explain the core of research on IWMDs security,
- Contacting the authors of research papers, when needed, and
- Conducting discussion sessions to share the learning materials and hard/soft skills

Comparison of traditional embedded security and IWMDs security: The second sub-step was to contrast traditional embedded security and IWMDs security based on the differences between these two. Fig. 3 shows the major differences taught to the students (IWMDs *vs.* traditional embedded systems security). This is a step-forward towards integration of emerging cryptographic engineering teaching and research.

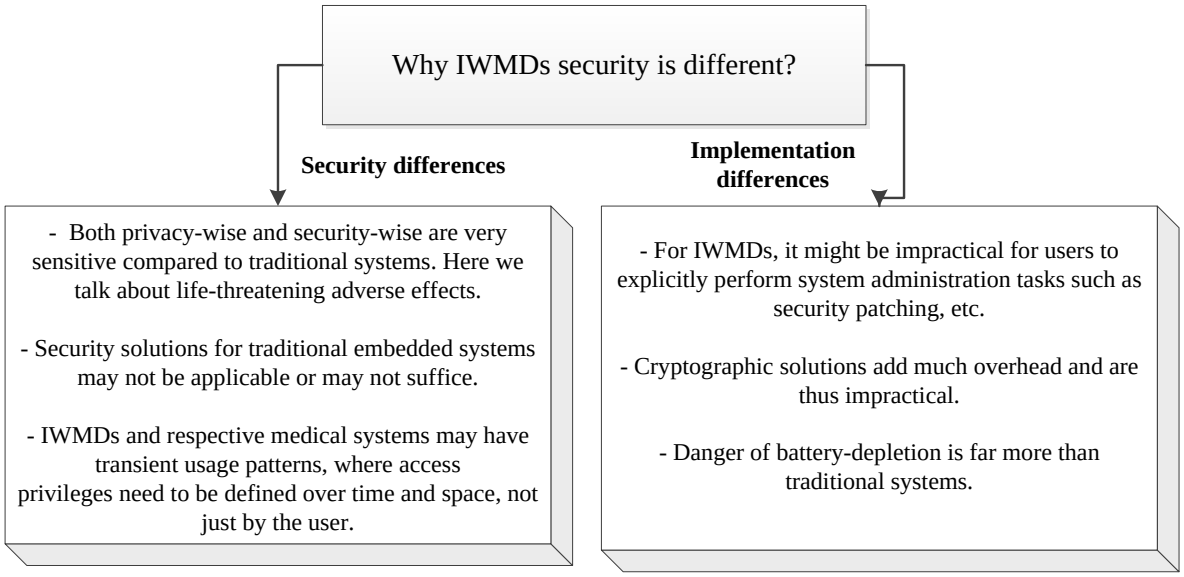

Figure 3. Traditional *vs.* IWMDs security (comparison for teaching and research integration).

Identifying the modularity of different cryptographic algorithms: These include algorithms such as SHA3 and the Advanced Encryption Standard (AES). The sub-step includes applying fault diagnosis and tolerance techniques specified for IWMDs.

Fig. 4 shows the first part of an S-box structure for the Pomaranch cipher. The structure of Pomaranch is based on linear feedback shift registers (LFSRs) which allow fast implementation and produce sequences with large period if the feedback polynomial is chosen appropriately (often clock controlled for complexity induction and used in conjunction with "jumping" to increase the efficiency and reach a CJCSG structure). The operations used in composite fields include addition, multiplication (including multiplication with constant), squaring, cubing, and inversion in GF(2^3). The architecture of the substitution box in Fig. 4 includes a first sub-part which contains the transformation matrix **M** whose input is shown by **X** in GF(2^9) to get an output of **A** in GF((2^3)^3).

Composite fields can be utilized to realize the substitution box to achieve low-complexity architectures. In Pomaranch, the two most and least significant bits are discarded to get to the uneven structure of the substitution box of Pomaranch.

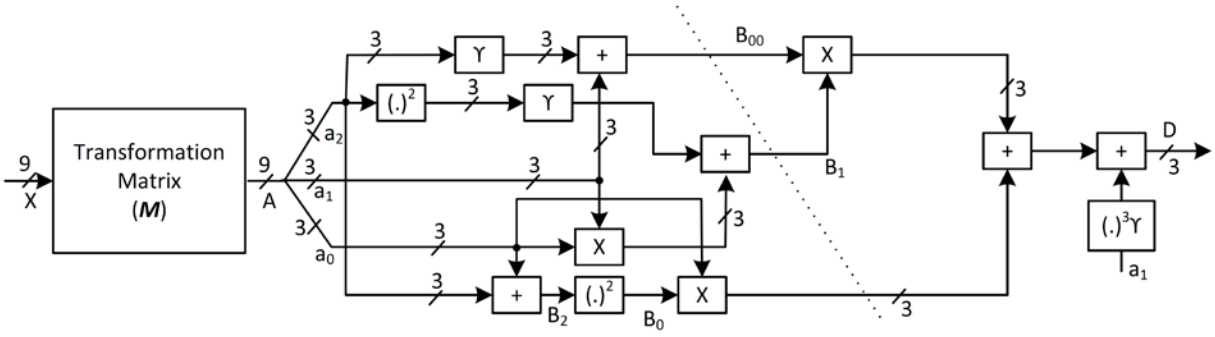

Figure 4. Hierarchy of the first part of an S-box structure for the Pomaranch cipher.

Educational Objectives:

- Understanding the implementation platforms (hardware [ASIC/FPGA] or software [microcontrollers]) through which the overheads were derived, this objective is fulfilled by implementing the original and fault detection designs and deriving the metrics overheads.
- Refining soft skills including presentation of the results of IWMDs security research (a) orally or (b) in writing, and decision-making.
- Evaluating hard technical skills for simulations and implementations of the fault diagnosis schemes for crypto-systems.

We already have a security laboratory and the security assessment is based on the resources in the already-developed "Applied Cryptography" laboratory. The form of outcome of the assessment will be mostly in programming languages specially hardware description languages of cryptographic algorithms developed as final projects. It is worth mentioning that the authors of this work have extensive background on fault detection and tolerance in many fields including cryptography[17-35]. Moreover, in the fields of computer arithmetic and cryptographic engineering, they have prior expertise[36-50], as well as prior editorials of related special issues[51-52.]

Integration Problems for Teaching and Research of IWMDs

The problems, challenges, and complications during the course of the integration have been resolved. In what follows, through three instances, we present some of them.

IWMDs and fault detection and tolerance with respect to cryptography have broad theory. This includes time/hardware/hybrid redundancies. Books and readings as well as conference/journal papers have been used for instruction of students. Nevertheless, we note that just trying random faults will not be helpful in breaking most ciphers. As such, error detection approaches based on recomputing with encoded operands for both transient and permanent faults can be used, for instance, as a remedy. The attackers might use entropy-aware injections to bypass the solutions. Through the research work done in 2013-2015, we refined the approaches to have specific applicability to fault attacks.

Simulation-based assessments through single/multiple stuck-at zero/one, transient and permanent faults are a major part of fault diagnosis and tolerance in cryptography. Single stuck-at fault injection is 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., Pomaranch, Sha-3, or ECC architectures.

A challenge here is that the integration of research and teaching becomes very application-specific and dynamic with respect to error simulations. There are two methods, in general, for assessing the fault coverage of the designs. The choice of hardware or software based injections through C++ or LFSRs is an important step to take. These application specific choices make the integration of "simulation" step as a number of general guidelines rather than specific schemes.

The complications in the implementation step usually relate to the ASIC and FPGA tools and hardware. Specifically, for IWMDs, if ASIC is used as the hardware platform, Synopsys tools

are used for implementations to derive the metrics (Design Compiler, PrimeTime PX, and the like). For FPGAs, Xilinx Vivado and Altera Quartus II are utilized.

Discussions and Conclusions

We have observed increased student engagement and deeper understanding through inquiry-led learning of fundamentals of IWMDs security. Moreover, it certainly helped generating additional research output/knowledge creation and strengthened pathways to postgraduate research (we are currently working on a number of *IEEE Transactions* journal papers and related conference papers as a result of such creation).

We also believe that linkage of research and teaching in academic work is beneficial for the departments the authors are affiliated with. Students become *knowledge workers* and are engaged in concept of the provisionality of existing knowledge. Overall, the students were satisfied with the integration outcome and also their publications progress.

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.

In this paper, for IWMDs security research and teaching integration, new methods considering their complications are presented. We have presented the results of two years of implementing the presented strategy at graduate-level through fault attacks of Pomaranch case study. 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. We were successful in exposing the challenges of IWMDs security education through working closely with a number of students in the areas of cryptographic engineering and general reliability. Finally, inter- and intra-university research collaborations were initiated. These help us towards future directions of such integration, e.g., post-quantum cryptography.

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] 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.

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

[4] C. Li, A. Raghunathan, and N. K. Jha, “Improving the trustworthiness of medical device software with formal verification methods,” *Embedded Systems Letters*, vol. 5, no. 3, pp. 50-53, 2013.

[5] M. Zhang, A. Raghunathan, and N. K. Jha, “MedMon: Securing medical devices through wireless monitoring and anomaly detection,” *IEEE Trans. Biomed. Circuits and Systems*, vol. 7, no. 6, pp. 871-881, 2013.

[6] M. Shoaib, N. K. Jha, and N. Verma, “Algorithm-driven architectural design space exploration of domain-specific medical-sensor processors,” *IEEE Trans. VLSI Syst.*, vol. 21, no. 10, pp. 1849-1862, 2013.

[7] 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.

[8] 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.

[9] U.S. Food and Drug Administration, Device Classification, 2009. [Online]. Available: http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/Overview/ClassifyYourDevice.

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

[11] 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.

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

[13] C. H. Gebotys, “Security in embedded devices,” Springer-Verlag, New York, 2010.

[14] T. Stapko, “Practical embedded security,” Elsevier/Newnes, Amsterdam, 2008.

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

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

[17] M. Mozaffari Kermani, R. Ramadoss, and R. Azarderakhsh, "Efficient error detection architectures for CORDIC through recomputing with encoded operands," in *Proc. IEEE Int. Symp. Circuits and Systems (ISCAS)*, pp. 2154-2157, May 2016.

[18] M. Mozaffari Kermani and R. Azarderakhsh, "Reliable hash trees for post-quantum stateless cryptographic hash-based signatures," in *Proc. IEEE Int. Symp. Defect and Fault Tolerance in VLSI Systems (DFT)*, pp. 103-108, Oct. 2015.

[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.*, vol. 34, no. 4, pp. 656-667, Apr. 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.*, vol. 23, no. 12, pp. 2804-2812, Dec. 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.

[35]. M. Mozaffari Kermani, R. Azarderakhsh, and A. Aghaie, “Fault detection architectures for post-quantum cryptographic stateless hash-based secure signatures benchmarked on ASIC,” *ACM Trans. Embedded Computing Syst.* (special issue on Embedded Device Forensics and Security: State of the Art Advances), to appear in 2016.

[36]. R. Azarderakhsh, B. Koziel, A. Jalali, M. Mozaffari Kermani, and D. Jao, “NEON-SIDH: Efficient implementation of supersingular isogeny Diffie-Hellman key-exchange protocol on ARM,” in *Proc. eprint 2016/669*, pp. 1-16, 2016.

[37]. B. Koziel, R. Azarderakhsh, S. H. Fatemi Langroudi, and M. Mozaffari Kermani, “Post-quantum cryptography on FPGA based on Isogenies on elliptic curves,” *IEEE Trans. Circuits Syst. I, Reg. Papers*, to appear in 2016.

[38]. P. Chen, S. N. Basha, M. Mozaffari Kermani, R. Azarderakhsh, and J. Xie, “FPGA realization of low register systolic all-one-polynomial multipliers over GF(2^m) and their applications in trinomial multipliers,” *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, to appear in 2016.

[39]. R. Azarderakhsh, B. Koziel, S. H. Fatemi Langroudi, and M. Mozaffari Kermani, “FPGA-SIDH: high-performance implementation of supersingular isogeny Diffie-Hellman key-exchange protocol on FPGA,” in *Proc. eprint 2016/672*, pp. 1-18, 2016.

[40] B. Koziel, R. Azarderakhsh, and M. Mozaffari Kermani, "Low-resource and fast binary Edwards curves cryptography using Gaussian normal basis," in *Proc. Int. Conf. INDOCRYPT*, pp. 347-369, Dec. 2015.

[41] C. E. Kennedy and M. Mozaffari Kermani, "Generalized parallel CRC computation on FPGA," in *Proc. IEEE Conf. Elec. Comput. Eng.*, pp. 107-113, May 2015.

[42] M. Zhang, M. Mozaffari Kermani, A. Raghunathan, and N. K. Jha, “Energy-Efficient and Secure Sensor Data Transmission Using Encompression,” in *Proc. IEEE Int. Conf. VLSI Design*, pp. 31-36, Jan. 2013.

[43] R. Azarderakhsh and M. Mozaffari Kermani, "High-performance two-dimensional finite field multiplication and exponentiation for cryptographic applications," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst*., vol. 34, no. 10, pp. 1569-1576, Oct. 2015.

[44] R. Azarderakhsh, M. Mozaffari Kermani, S. Bayat-Sarmadi, and C. Lee, "Systolic Gaussian normal basis multiplier architectures suitable for high-performance applications," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 23, no. 9, pp. 1969-1972, Sep. 2015.

[45] R. Azarderakhsh, M. Mozaffari Kermani, and K. U. Jarvinen, "Secure and efficient architectures for single exponentiation in finite field suitable for high-performance cryptographic applications," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 34, no. 3, pp. 332-340, Mar. 2015.

[46] J. Pan, R. Azarderakhsh, M. Mozaffari Kermani, C. Lee, C. Chiou, and J. Lin, "Low latency digit-serial systolic double basis multiplier over GF(2^m) using subquadratic Toeplitz Matrix-Vector product approach," *IEEE Trans. Comput.*, vol. 63, no. 5, pp. 1169-1181, May 2014.

[47] S. Bayat-Sarmadi, M. Mozaffari Kermani, R. Azarderakhsh, and C. Lee, "Dual basis super-serial multipliers for secure applications and lightweight cryptographic architectures," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 61, no. 2, pp. 125-129, Feb. 2014.

[48] Fault Detection Schemes for High Performance VLSI Implementations of the Advanced Encryption Standard, M. Mozaffari Kermani, The University of Western Ontario, Thesis, 2007.

[49] M. Mozaffari Kermani and R. Azarderakhsh, “Integrating emerging cryptographic engineering research and security education,” American Society for Engineering Education (ASEE), 2015.

[50] Reliable and High-Performance Hardware Architectures for the Advanced Encryption Standard/Galois Counter Mode, M. Mozaffari-Kermani, The University of Western Ontario, Thesis, 2011.

[51] M. Mozaffari Kermani, R. Azarderakhsh, K. Ren, and J.-L. Beuchat, "Guest Editorial: Introduction to the Special Issue on Emerging Security Trends for Biomedical Computations, Devices, and Infrastructures," *IEEE/ACM Transactions on Computational Biology and Bioinformatics*, vol. 13, no. 3, pp. 399-400, June 2016.

[52] M. Mozaffari Kermani, E. Savas, and S. Upadhyaya, "Guest Editorial: Introduction to the Special Issue on Emerging Security Trends for Deeply-Embedded Computing Systems," *IEEE Trans. Emerging Topics in Computing*, vol. 4, no. 3, pp. 318-320, Sep. 2016.