Secure, Reliable and Low-Energy Hardware Architecture Design

Sandhya Koteshwara and Keshab K. Parhi (Advisor)
Department of Electrical Engineering, University of Minnesota, Twin Cities
Email : {kotes001, parhi}@umn.edu
Expected Graduation Date : Summer, 2018

***Abstract*—This research work focuses on development of hardware architectures to achieve high end- to-end security and low cost, low energy solutions using both Application-Specific Integrated Circuits (ASIC) designs and Field Programmable Gate Array (FPGA) implementations. The proposed architectures are targeted at securing communication between devices in safety critical systems, ensuring reliability in manufacturing of semiconductor circuits and creating minimalistic diagnosis and treatment solutions applicable to the biomedical device industry.**

I. Background

Modern devices are not only shrinking in size but also being increasingly connected to each other. These smart, connected devices are broadly termed Internet of Things or IoT. Examples of IoT applications range from safety critical automotive IoT employed in self-driving cars, smart cards and radio-frequency identification (RFIDs), high speed wireless sensor nodes, consumer electronics such as smart TVs, refrigerators and critical, life-saving systems such as implantables and medical devices. The devices used in these applications demand low cost, high efficiency and high security algorithms to be implemented using the most resource efficient platforms. To keep up with the changing application scenario, new architectural mappings and techniques for designs beyond traditional optimization has become a necessity.

II. Research Goals and Objectives

The architectures proposed in my research target three major areas of IoT applications and semiconductor circuits.

- **Objective 1: Hardware obfuscation architectures for reliability in manufacturing:** Hardware security has emerged as an important topic over the last decade due to reports of counterfeit devices in safety critical defense systems [1]. With the upcoming era of IoT, security is only going to increase in importance with more devices being manufactured and connected to a common network. Hardware obfuscation, which is defined as hiding functionality of designs and locking them using secret keys before sending for manufacturing (Fig. 1), attempts to alleviate some of these problems. This ensures that the circuit is not understandable or usable by parties not possessing the correct key. Once the chips are obtained back from the untrusted manufacturing units, they are unlocked and distributed to the end user, ensuring reliability. Development of novel architectures and schemes for obfuscation is the first area of my research.
- **Objective 2: Authenticated Encryption architectures for secure communication:** Authenticated encryption with Associated Data (AEAD) is a form of encryption which simultaneously provides confidentiality, integrity, and authenticity assurances on the data. Authentication verifies that the source of information is a trusted device and encryption ensures that the message has been protected from modifications and eavesdropping across the channel (Fig. 2). To ensure secure communication between two devices connected on the network, low cost and low power AEAD schemes are of paramount importance. To address design of authenticated encryption algorithms tailored towards changing application scenarios, a Competition for Authenticated Encryption: Security, Applicability, and Robustness (CAESAR) is currently in progress [2]. Mapping of algorithms from CAESAR to low power and energy architectures using FPGA is my second area of research.

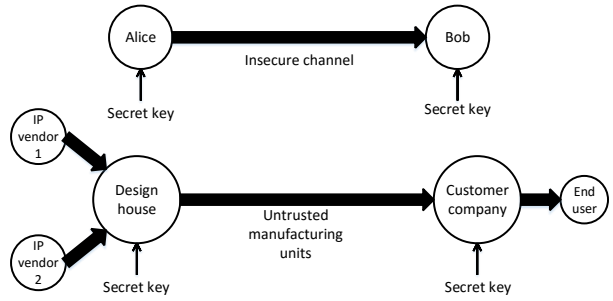

Fig. 1. Comparison of encryption scheme as defined in cryptography with hardware obfuscation technique

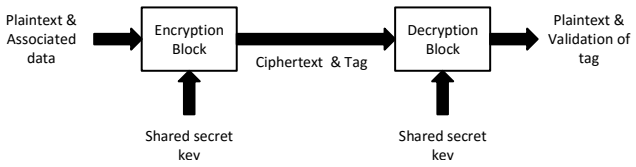

Fig. 2. General scheme of an Authenticated Encryption scheme withAssociated Data

- **Objective 3: Low energy machine learning architectures for biomedical devices:** Biomedical applications such as implantables require low power and energy efficient architectures to perform machine learning tasks. For example, seizure detection aims to classify between resting and seizure state of electroencephalogram (EEG) signals. To differentiate between the two states, distinguishing features need to be extracted from these signals and classifiers which are trained on large amounts of training data need to be employed. The units required to extract features involve power spectral density (PSD) computation (Fig. 3) and support vector machine (SVM) classifiers, which require high energy. A technique

termed approximate computing is applied to decrease the energy consumption of systems [3]. Specifically, applying bit-width reduction to modify architectures to consume lower energy, while maintaining accuracy is the third focus of my research work.

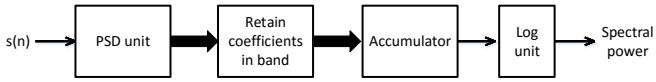

Fig. 3. Top level block diagram of a feature extraction unit extracting spectral power

III. Contributions to the Field

- **Mode-based and Hierarchical obfuscation using Control-Flow modifications.** In this task, I proposed a novel technique to hardware obfuscation using modifications to control signals of the architecture [4] and extended the technique for application in a hierarchical manner to a complete integrated circuit [5]. Using ASIC implementations and a case study on fast Fourier transform (FFT) and Convolution modules, I demonstrated that the proposed technique is a simple solution requiring changes only to the control flow of the design, compared to existing techniques which require major modifications to the design flow. Also, the cost of this technique is low at only 8% area and 10% power overhead compared to a traditional implementation, making it a feasible solution to obfuscation.
- **Dynamic mode of obfuscation offering stronger security at low cost.** In recent literature, some tool based techniques have demonstrated that the current methods of obfuscation are not secure enough and can be easily broken. To address this concern, I modified the mode-based technique of obfuscation to create a dynamic method of obfuscation [6] which uses time-varying and random modes to increase security of the design. Using FFT circuits, I applied three different attack strategies and proved that the dynamic technique has higher security compared to existing methods.
- **Exploration of algorithms for Authenticated Encryption targeting lightweight IoT.** In this task, I worked on understanding of candidates selected to the second round of CAESAR competition with respect to architectural features. I then proposed mappings of these algorithms to different IoT applications, based on their hardware, software and security performance numbers in comparison to an existing standard, AES-GCM [7]. An overview of this kind, considering functional and architectural aspects, performance measures, comparison with AES-GCM and an application oriented discussion does not exist in current literature and will be highly beneficial for designers of cryptographic protocols for embedded system platforms and SoCs.
- **FPGA implementations of Deoxys, AES-GCM-SIV and comparison with AES-GCM.** I completely designed and implemented two architectures for candidates Deoxys [8] from the CAESAR competition and AES-GCM-SIV on Altera Cyclone V FPGA and performed an area, power and energy analysis with respect to the architectural implementation of current standard, AES-GCM on the same platform. The proposed implementations and comparisons are the first of their kind in literature and will serve as guidelines for future users of the algorithms. Moreover, the proposed optimizations and power measurement techniques are powerful tools, useful in deployment of not only these algorithms but for authenticated encryption based architectures in general.
- **Error vs Energy analysis of Approximate Computing based Feature extraction unit.** This task involves adoption of approximate computing via bit-width reduction on the architecture of feature extraction unit of seizure detection application. I developed models using mathematical measurements for quantization error and fixed point conversion tools in MATLAB. Using these models, a lower bound on precision is obtained and energy measurements can be performed to understand the savings in energy consumption. For the seizure detection application, it was shown that lowering precision to 12 bits (compared to a full precision implementation of 16 bits), lowers the energy by 30%.

IV. Future Work

- *Hardware/Software Co-design of Authenticated Encryption algorithms.* My next task in the design and implementation of authenticated encryption algorithm will be to address a hardware/software co-design approach to obtain better resource efficiency on modern application platforms.
- *Theory of incremental classification for low energy classifier.* I am currently also working on developing a theory for low energy classification architectures as used in the seizure detection application, by incrementally increasing bit precision of components from 10 bits to 16 bits.
- *Implementation of Low power feature extraction and classification system using FPGA.* As an extension of the approximate computing based feature extraction unit and the incremental classification based classifier unit, I will work on creation of a complete classification system and its implementation on FPGA platforms. This low energy implementation will be targeted to serve as a prototype for medical devices.

References

[1] M. Rostami, F. Koushanfar, and R. Karri, "A primer on hardware security: Models, methods, and metrics," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1283–1295, 2014.

[2] [Online]. Available: http://competitions.cr.yp.to/caesar-call.html

[3] J. Han and M. Orshansky, "Approximate computing: An emerging paradigm for energy-efficient design," in *Test Symposium (ETS), 2013 18th IEEE European*. IEEE, 2013, pp. 1–6.

[4] S. Koteshwara, C. H. Kim, and K. K. Parhi, "Mode-based Obfuscation using Control-Flow Modifications," in *Proceedings of the Third Workshop on Cryptography and Security in Computing Systems*. ACM, 2016, pp. 19–24.

[5] S. Koteshwara, C. H. Kim, and K. K. Parhi, "Hierarchical Functional Obfuscation of Integrated Circuits using a Mode-Based Approach," in *Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS), 2017*.

[6] S. Koteshwara, C. H. Kim, and K. K. Parhi, "Key-Based Dynamic Functional Obfuscation of Integrated Circuits using Sequentially-Triggered Mode-Based Design," *IEEE Transactions on Information Forensics and Security, 2017*, (Under Review).

[7] S. Koteshwara and A. Das, "Comparative study of Authenticated Encryption targeting lightweight IoT applications," *IEEE Design & Test*, 2017.

[8] S. Koteshwara, A. Das, and K. K. Parhi, "FPGA implementation and comparison of AES-GCM and Deoxys Authenticated Encryption schemes," in *Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS), 2017*.