Communications on Applied Electronics (CAE) – ISSN : 2394-4714
Foundation of Computer Science FCS, New York, USA
Volume 3– No.7, December 2015 – www.caeaccess.org

Robust Secure FPGA-based Wireless Smart Meters Utilizing PUF and CSI

M.M. Abutaleb
Electronic, Communication and
Computer Engineering,
Helwan University, Cairo, Egypt
Applied Natural Sciences,
UCC, Qassim University,
Unaizah, Saudi Arabia

ABSTRACT
Smart meters that measure the use of residential energy at fine granularities are the foundation of a future smart electricity grid. In this paper, a novel design of FPGA-based smart meters is proposed to measure the energy consumption and at the same time it provides secure wireless connections with the concentrator in Advanced Metering Infrastructure (AMI). A basic idea of this system is to use Physical Unclonable Function (PUF), which is a die-unique challenge–response function, for generating a unique signature of meter based on IC process variations and to use Channel Status Information (CSI) for providing a secure wireless channel between meter and concentrator.

Keywords
Electrical energy, smart meter, PUF, CSI, FPGA.

1. INTRODUCTION
The idea of smart grid refers to the renewal of the presented electrical grid, including bidirectional communication between meters and utilities, more accurate meter readings and flexible tariffs [1]. Expected electricity savings depend on matching generation and demand, which is done through feedback on consumers' electricity consumption, as well as on billing using flexible tariffs with higher rates during peak consumption periods.

Advance Metering Infrastructure (AMI) is one of the vital functional blocks of the Smart Grid. It is a system that supports two-way communications with customers and electric company [2]. AMI comprises of components such as the AMI meter, AMI head-end or concentrator, Meter Data Management System (MDMS), the communication network, the access points, and the endpoints. The AMI systems make use of smart meters, and In-home displays to assist in the determination of the usage pattern and make efficient allocation of resources wherever required. On the other hand, growing the use of smart-grid applications allow massive dangers in several areas and AMI is one such point that can be damaged by starting harmful attacks which is threaten the work of the smart-grid applications [3]. An efficient authentication is required in the AMI to support great number of smart meters that could be satisfied using the key management system. The like impersonation attack, man-in-the-middle attack and several attacks can be success in the lack of a strong authentication mechanism [4, 5].

The main contribution of this paper is to provide a robust authenticated secure design of smart meters for wireless communications with the concentrator in the AMI. The proposed scheme is based on the use of PUFs that are low-cost to manufacture and provide hardware based authentication and integrity mechanism resistant to impersonation attacks [6]. Moreover, the channel characteristics based on CSI is proposed to provide protection against data interception without using pre-shared or stored master key. Therefore, the proposed design scheme is to integrate smart meter functions with security services on a single low cost field-programmable gate array (FPGA) device.

2. SYSTEM MODEL
This section provides a high-level overview. The overview focuses on the aspects that are relevant for components and blocks of the proposed system. The AMI consists of four main components: the utility company or metering data management system, data collectors or concentrator, often located in the neighborhood, smart meters, and the home or office appliances. The communication between smart meters and appliances can use several communication protocols such as ZigBee, Wi-Fi, and Ethernet.

The communication between smart meters and concentrator is focused in this work. As shown in Fig. 1, the system consists of three main components:

- **Smart meter**: equipment that measures the power consumption by user and sends it to concentrator via wireless channel.
- **Concentrator**: equipment that aggregates the data of multiple smart meters and sends it to metering data management system.
- **Metering data management system (MDMS)**: The MDMS is responsible for aggregating, validating and permitting editing of meter data. It stores the data before it is goes to the dedicated storage facilities.

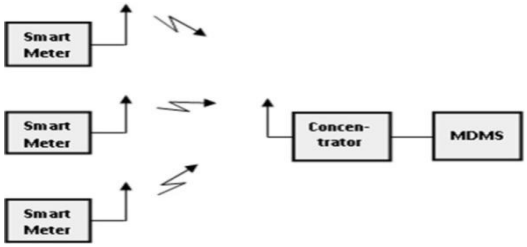

Fig. 1: System components

The proposed design can be summarized into two main blocks, first, using hardware authentication and integrity technique based on PUFs. Second, using the channel characteristics to provide confidentiality based on the CSI.

2.1 Physically Unclonable Function (PUF)

The need to ascribe a unique binary signature to an integrated circuit (IC) has applications in digital design and embedded systems. The PUF is a new concept in hardware security, and a promising candidate for IC signature generation [7]. An artifact of state-of-the-art sub-100 nm IC manufacturing is that random variations in doping concentrations, line widths, or other properties cause unpredictable variations in transistor speed and interconnect. Most PUF designs compute unique signatures by exploiting such delay differences. At a high level, the approach taken in PUF design is to incorporate multiple identical copies of a particular combinational path into an IC design. Since the copies are identical, delay differences between the copies are due to random variations that are inherent to the manufacturing process, and cannot be controlled or cloned. PUF circuitry measures the delay differences between path copies to generate the unique PUF signature.

There are practical reasons why FPGA-based PUF implementation is necessary. First, FPGAs are suitable for faster implementation of cryptographic algorithms on hardware because of their reconfigurable nature. Additionally, the regular structure of FPGAs prevents identification of the implemented circuit through an invasive attack. FPGAs contain arrays of identical logic and routing circuitry. This underlying architectural regularity is used to realize matched copies of combinational paths whose delay differences stem from manufacturing variations [8, 9]. In [9], the FPGA-specific PUF design, that takes advantage of the FPGA logic and routing architecture, was introduced on Virtex-5 FPGAs. This paper utilizes the PUF specifically designed for FPGAs to demonstrate with low cost Xilinx Spartan-3E FPGAs.

2.2 Channel State Information (CSI)

The CSI has been used to identify wireless users and provide privacy for transmitted data from eavesdropper [10]. It commonly indicates the channel impulse response. The foundation behind these scheme is that the CSI location-specific and privacy-preserving due to path loss and channel fading. An attacker, who is at a different location from the genuine user, will incur different CSI profile as observed by monitors/access points.

In this paper, a real-time FPGA-based confidentiality method in physical layer is proposed based on instantaneous CSI. This method differs with the existed methods on that the CSI is estimated, and then modulate the transmitted signal with it to compensate the effect of channel between transmitter and receiver.

3. DESIGN FLOW

The overall system consists of three main parts:

- Metering unit used to precisely measure the use of residential energy.
- PUF instances used in both hardware authentication of meter and message integrity with measured data.
- CSI estimation used for detecting characteristics of wireless channel between meter and concentrator to compensate them for the transmitting data from meter and PUFs.

The proposed smart meter is based on FPGA technology, and for consistency the design is implemented over a single FPGA chip starting from reading energy consumption passing with security embodies service till transmitting/receiving data. The merit of this design is providing the desired services with low cost design because of building on Xilinx Spartan-3E FPGA chip.

Here the first FPGA-based prototype is presented for CSI based encryption scheme and PUF generator used for both integrity and authentication. The proposed smart meter, which is required to achieve the contribution of this paper, consists of three main components: *Meter Module*, *Channel Compensator*, and *PUF Generators*.

The first components of the proposed design has been presented and implemented in the previous work [11]. The FPGA-based *Meter Module* [11] is capable of precisely measuring the use of residential energy and instantaneously transmitting the reading to concentrator. Other components of the proposed design will be discussed here in the following subsections.

3.1 FPGA-specific PUF Generator

Spartan-3E logic blocks called Configurable Logic Blocks (CLBs) are arranged in a regular array of rows and columns as shown in Fig. 2 and can be connected to one another through a programmable interconnection matrix. Each CLB comprises four interconnected slices that are grouped in pairs. Each pair is organized as a column with an independent carry chain. The left pair supports both logic and memory functions and its slices are called SLICEM. The right pair supports logic only and its slices are called SLICEL.

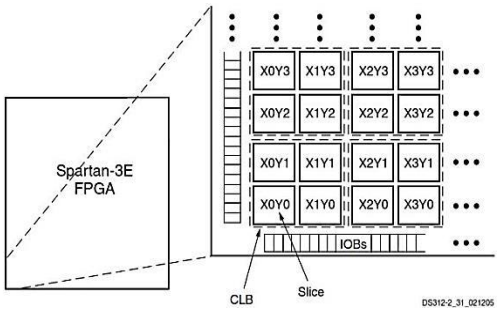

Fig. 2: Spartan-3E CLB Locations

Fig. 3 shows SLICE details. Each slice contains two Look-Up Tables (LUTs) to implement logic and two dedicated storage elements that can be used as flip-flops or latches. The LUTs can be used as a 16x1 memory (RAM16) or as a 16-bit shift register (SRL16), and additional multiplexers and carry logic simplify wide logic and arithmetic functions. The vertical chain of 2-to-1 multiplexers is called the carry chain and it is intended for implementing fast arithmetic operations. The carry multiplexers are used in the PUF design implementation.

The FPGA-specific PUF design is shown in Fig. 4. Two LUTs, A and B are used in 16-bit shift register mode. The shift register contents are pre-initialized as follows [9]:

- LUT A: 0101010101010101 (0x5555) and
- LUT B: 1010101010101010 (0xAAAA).

Note that LUT A's initialization bits is the complement of LUT B's bits. Both carry multiplexers have their data input (I1, I2) tied to logic-0. The bottom carry chain multiplexer has its data input (I3) tied to logic-1. The output of the bottom multiplexer drives the data input of the top multiplexer. Consider the dynamic clocked behavior of the circuit in Fig. 4. Initially, the output of LUT A is at logic-0, and therefore signal O2 is at logic-0. The output of LUT B is logic1, setting signal O1 to be logic-1. At the rising clock edge, the output of LUT A will transition from logic-0 to logic-1, and the output of LUT B will transition from logic-1 to logic-0. Although LUT A and the multiplexer it drives should be identical to LUT B and its multiplexer, the two pieces of circuitry in fact experience different delays due to random process variations. This property is exploited here for PUF signature generation.

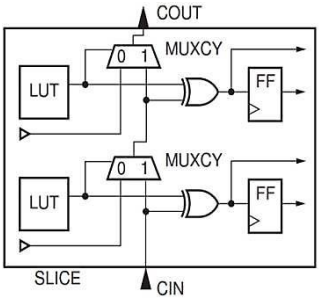

Fig. 3: SLICE Details

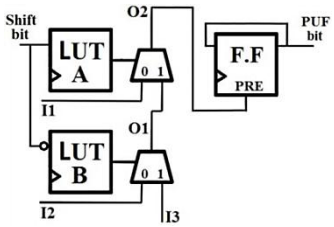

Fig. 4: PUF-bit Generation

There are two cases worth highlighting. First, consider the case wherein LUT B and the multiplexer it drives are faster than LUT A and its multiplexer. In this case, when LUT B transitions from logic-1 to logic-0, signal O1 also transitions from logic-1 to logic-0. Following that, the slower LUT A transitions from logic-0 to logic-1, and signal O2 is held constant at logic-0 throughout the process. The second case is the opposite one where LUT A and its multiplexer are the faster ones. In this case, LUT A's output transitions from logic-0 to logic-1 and net O1 has not yet transitioned from logic-1 to logic-0. A short positive spike (a glitch) will appear on O2 for the period before O1 transitions to logic-0.

The presence or absence of a positive spike on O2, and the length of the spike pulse, are due to process variations that impact the relative delays of LUTs A and B and the carry chain multiplexers. The presence/absence of a positive spike on O2 is used to determine a PUF bit. O2 is connected to the asynchronous preset input of a flip-flop, as shown in Fig. 4. The flip-flop is initialized to logic-0 and has its output Q fed back to its D input. In this work, LUTs A and B and the flip-flop are located in different SLICEs within the same CLB as shown in Fig. 5 to maximize the PUF utility by tuning the the glitch pulse width. Each individual PUF bit is computed within a single CLB. In the event that a tuned glitch on signal O2 reaches the preset, the flip-flop output becomes logic-1 and the PUF bit is logic-1. Otherwise, the PUF bit is logic-0. The key benefit of this PUF design is that it is described completely in VHDL and can be automatically handled by synthesis, place and route tools, without manual intervention.

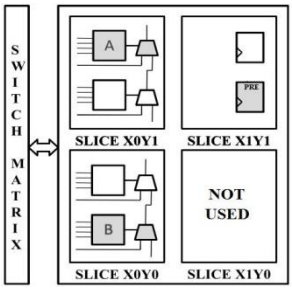

Fig. 5: The mapping of a PUF in a single CLB on a Xilinx Spartan 3E platform

A proposed challenge/response approach is to have the challenge input bit drive the select input on 2-to-1 multiplexer, as shown in Fig. 6. The challenge selects two different PUF bits to produce a response bit depending on the challenge and integrated PUF.

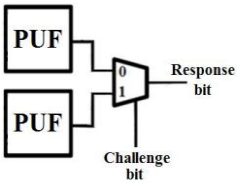

Fig. 6: Signature-bit Generation

The methodology of using multiple unique implementations of the same circuit on a single chip can only be applied for reconfigurable platforms such as FPGAs. The prototype instantiate 160 instances of the PUF design to generate 64-bit signature for authentication and 16-bit message integrity which is composed with 24-bit reading of energy consumption. PUFs are characterized to extract all possible independent challenge–response pairs (CRPs) at normal environmental condition, which are stored in a database of concentrator. The meter sends the data after signal compensation based on the detected CSI.

3.2 FPGA-based Channel Compensator

The main task of the *Channel Compensator* design is to track the wireless channel phase-shift and attenuation via comparison between the received pilot signal $S_P(t)$ of concentrator and reference signals in transmitting section, and then compensate the transmitted data signals. Its architecture is composed of three basic parts: *Channel Phase Compensator* (CPC), *Channel Attenuation Compensator* (CAC), and *Transmission Data Compensator* (TDC). In this work, the timing signal (Fig. 7) of Tx/Rx Control is assumed to be '0' through the processing period and '1' through the data transmitting $S_D(t)$ and receiving $S_R(t)$ between pilots.

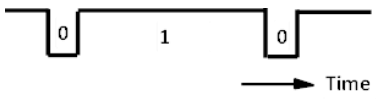

Fig. 7: Timing Control Signal

Communications on Applied Electronics (CAE) – ISSN : 2394-4714
Foundation of Computer Science FCS, New York, USA
Volume 3– No.7, December 2015 – www.caeaccess.org

The architecture of *Channel Phase Compensator* (CPC) consists of the *Synchronization Block* (SB) and *Generator Block* (GB) as shown in Fig. 8. *Synchronization Block* (SB) is a circuit which synchronizes the phase (ϕ_{vco}) of the output signal generated by a voltage controlled oscillator (VCO) with the phase (ϕ_i) of the input signal. The phase difference between the input signal and VCO signal is called phase error (ϕ_e) and the control mechanism acts on the oscillator in such a way to reduce the phase error. Therefore, it is similar to the system PLL. Multiplier has two inputs and produces the output voltage that mixes the two input signals. This mix produces the sum and difference phases. The loop filter removes the high-frequency component and produces the output voltage that contains only a DC component. VCO will take this voltage which is proportional to the phase difference and then shift its output signal.

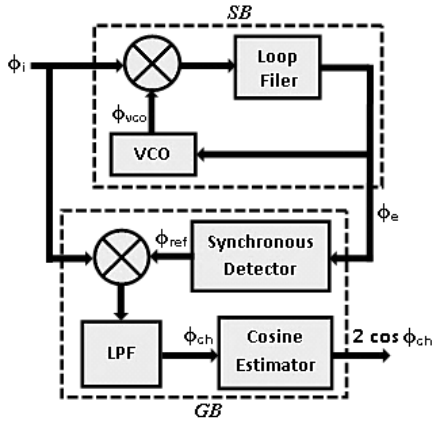

Fig. 8: Block diagram of CPC

Generator Block (GB) is a circuit which generates the cosine value of channel phase (ϕ_{ch}) with gain of 2. The phase difference between the synchronized input signal and reference signal is called channel phase (ϕ_{ch}). The reference phase (ϕ_{ref}) signal will be generated from the Synchronous Detector depending on the least phase error (ϕ_e) in the synchronization block. The synchronized input signal will multiply with reference signal. Low pass filter (LPF) is used to reject the high frequencies of this signal and then the channel phase (ϕ_{ch}) can be obtained in its cosine value with gain of 2 using the *Cosine Estimator*.

The architecture of *Channel Attenuation Compensator* (CAC) is shown in Fig. 9. The CAC system is an automatic system that can detect the peak value of the input signal, and then estimate the inverse value of channel attenuation that is used as compensator for the channel attenuation. The function of the *Peak Detector* is to detect the peak value (a_P) of the input signal $S_P(t)$. It means that if the amplitude of input signal increases, the peak detector searches about the peak value while if the amplitude of input signal decreases, the peak detector keeps the last peak value in its output and so on. The divider is used to calculate the channel attenuation (a_{ch}) by dividing the peak value (a_P) of the input signal by the peak value (a_{ref}) of the *Reference*. The channel attenuation (a_{ch}) can be compensated by inverting its value using the *Inverse Estimator*.

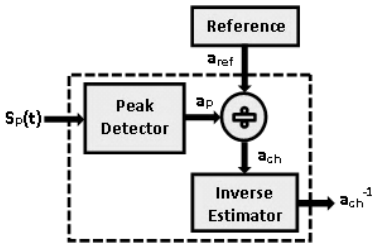

Fig. 9: Block diagram of CAC

The architecture of *Transmission Data Compensator* (TDC) is shown in Fig. 10. It is used to compensate the transmission data (QAM) signal that has amplitude a_i and phase φ_i:

$$s_D(t) = a_i \cos(\omega t + \varphi_i) \quad (1)$$

to generate the compensated signal:

$$s_c(t) = \frac{a_i}{a_{ch}} \cos(\omega(t + \tau_{ch}) + \varphi_i) \quad (2)$$

which can be written as:

$$s_c(t) = \frac{a_i}{a_{ch}} \cos(\omega t + \varphi_{ch} + \varphi_i) \quad (3)$$

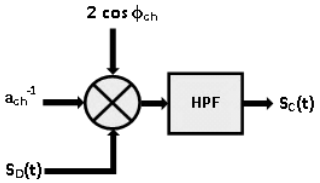

Fig. 10: Block diagram of TDC

Here, multiplier produces the output voltage that contains the sum and difference phases. The high-pass filter (HPF) is used to pass the high-frequency component and produce the compensated signal $S_C(t)$ for secure transmission.

3.3 Experimental and Synthesis Results

The result of PUF reliability is on average 3.7% of signature bits flip under high temperature conditions, which is in line with other published PUF circuits. The simulation result is shown in Fig. 11 during the generation of PUF bit. The first four rows show the system clock, the input of LUT A, the PUF output, and the input of LUT A, respectively. The fifth row and the sixth row are the outputs of LUT A and of LUT B, respectively. The last two rows show the outputs of the bottom and top multiplexers, respectively. The Spartan-3E FPGA chip XC3S500E has about 9,312 LUTs/Flip-Flops, of which about 4,656 may be used as RAMs/SRLs. Our 160-bit for PUF designs uses less than 7% of such RAM/SRL LUTs and 2% of such Flip-Flops.

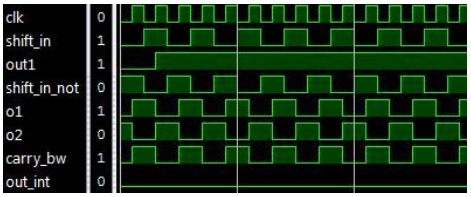

Fig. 11: Result of the PUF bit Generation

The simulation result is shown in Fig. 12 during the estimation and compensation of channel phase-shift and

attenuation. The first three rows show the system clock, the coherence control signal ('0'), and the pilot signal, respectively. The fourth row and the fifth row are the generated reference-phase signal and the estimated cosine-value of channel phase with gain of 2, respectively. The last three rows show the detected peak-value of pilot signal, the reference peak-value, and the inverting-value of channel attenuation, respectively.

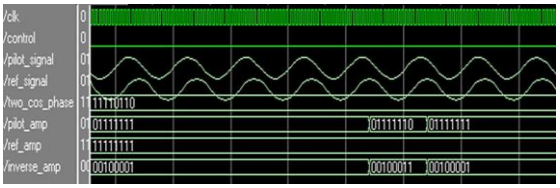

Fig. 12: Result of the Channel Compensator

In regard to the hardware realization for the whole design of the smart meter with CIA services, the VHDL code is synthesized by considering Spartan-3E Xilinx chip XC3S500E. Design is synthesized with Xilinx Synthesize Tool (XST), here it can be concluded that the total critical path delay is 47.320ns and the total circuit area is 2116 slices with 45% utilization; an additional advantage of our low cost design is its small size. Upon author Knowledge, it is the first time to design an AMI smart meter with security services using FPGA technology.

4. CONCLUSION

In this paper, the design and implementation of FPGA-based smart energy meter, that integrates metering functions with security services for wireless transmitting data, has been presented.

The proposed approach shows that it is practical and efficient to provide robust secure wireless communications for smart meters by utilizing PUF generators and CSI compensation methodology via the FPGA technology. Besides that, it shows a quite simple, real-time performance and cost effective structure.

5. REFERENCES

[1] A. Cavoukian, J. Polonetsky, and C. Wolf, “Smart privacy for the smart grid: embedding privacy into the design of electricity conservation,” in Identity in the Information Society, Volume 3, Number 2, Pages 275-294, 2010.

[2] I. Yang, N. Jung and Y. Kim, "Status of Advanced Metering Infrastructure development in Korea", in Proceedings of Transmission & Distribution Conference & Exposition, Daejeon, South Korea, Oct. 26-30, 2009.

[3] D.G. Hart, "Using AMI to realize the Smart Grid", in Proceedings of the Conference on Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century, Pittsburgh, PA, July 20-24, 2008.

[4] P. McDaniel and S. McLaughlin, "Security and Privacy Challenges in the Smart Grid," IEEE Security Privacy Magazine, vol. 7, no. 3, pp. 75-77, 2009.

[5] G. Kalogridis, C. Efthymiou, S. Z. Denic, T. A. Lewis, and R. Cepeda, "Privacy for Smart Meters: Towards Undetectable Appliance Load Signatures," in 2010 First IEEE International Conference on Smart Grid Communications, pp. 232-237, 2010.

[6] G. T. Becker and R. Kumar,” Active and Passive Side-Channel Attacks on Delay Based PUF Designs,” IACR Cryptology ePrint Archive, 2014:287, 2014.

[7] M. Majzoobi, F. Koushanfar, and M. Potkonjak, “Techniques for design and implementation of secure reconfigurable PUFs,” In ACM Trans. on Reconfigurable Technology and Systems, vol. 2, no. 1, pp. 1–33, 2009.

[8] H. Yu, P. Leong, H. Kinkelmann, L. Moller, and M. Glesner, “Towards a unique FPGA-based identification circuit using process variations,” In IEEE Int’l Conf. on Field Programmable Logic and Applications, pp. 397–402, 2009.

[9] J.H. Anderson, "A PUF design for secure FPGA-based embedded systems," IEEE/ACM Asia and South Pacific Design Automation Conference, Taiwan, pp. 1-6, 2010.

[10] IEEE 802.15.4, ”Wireless medium access control (MAC) and physical layer (PHY) specifications for low-rate wireless personal area networks (LR-WPANs),” 2003.

[11] M. M. Abutaleb and A. M. Allam, “Secure Low Cost FPGA-based AMI System using LTE Technology”, CiiT International Journal of Networking and Communication Engineering, vol. 4, no 7, pp. 377-383, June 2012.