International Journal of Control and Automation
Vol. 9, No. 9 (2016), pp.407-414
http//dx.doi.org/10.14257/ijca.2016.9.9.38

PUF based Smart Meter Security with Sx Chain

Seonghan Ryu

Hannam University, Dept. of Information and Communication Engineering
70 Hannam-ro, Daedeok-gu, Daejeon, Korea
ilikeit@hnu.kr

Abstract

A smart meter is resource-constrained device, therefore lightweight cryptographic methods are required. Physical unclonable function(PUF) is promising hardware based lightweight security solution, which makes use of the inherent process variation in semiconductor fabrication process to generate unique ID. This paper presents an PUF based smart meter security with frequency synthesizer(Sx) chain composed of VCO and dynamic divider(DDiv), which use oscillation frequency variation characteristics. In the Sx chain PUF implementation, the output bits are obtained by comparing the oscillation frequencies of different VCO inductor banks or dynamic dividers. For the lightweight operability, simple VCO or DDiv-PUF based authentication protocol is also proposed.

Keywords*: Smart Meter, PUF, VCO, Dynamic Divider, CMOS*

1. Introduction

A smart meter is an essential device for smart power grid, which have an ability to check energy consumption remotely. Two-way communication is also available with smart meter. For an electric power providers and users, they can have the benefit of saving the total amount of energy and the energy costs by this electronic metering ability. Figure 1 shows the home area network based on smart meter[1].

Figure 1. Smart Meter based Home Area Network

ISSN: 2005-4297 IJCA

The smart meter is a resource constrained device and vulnerable to security attacks. Physical unclonable function is a promising security primitives based on hardware technology, which is favored by resource constrained devices such as smart meter. PUF makes use of the inherent process variation in semiconductor process such as CMOS technology. Most secure cryptographic algorithms use a private secret value, secret key for encryption and decryption. The key is stored in a non-volatile based memory and inherently vulnerable to invasive attacks such as tampering[2]-[4]. However, PUF uses the physical fingerprint of the silicon chip, variation of each device to generate a set of unique data. Though identical PUF chips are implemented, the variation between devices generate unique difference, thus duplication of PUF characteristics is inherently impossible. Figure 2 shows the general structure of a synthesizer(Sx) chain of RF transceiver for wireless connectivity. This paper presents a PUF based smart meter security using these Sx chain block circuitry with inherent silicon fabrication process variation.

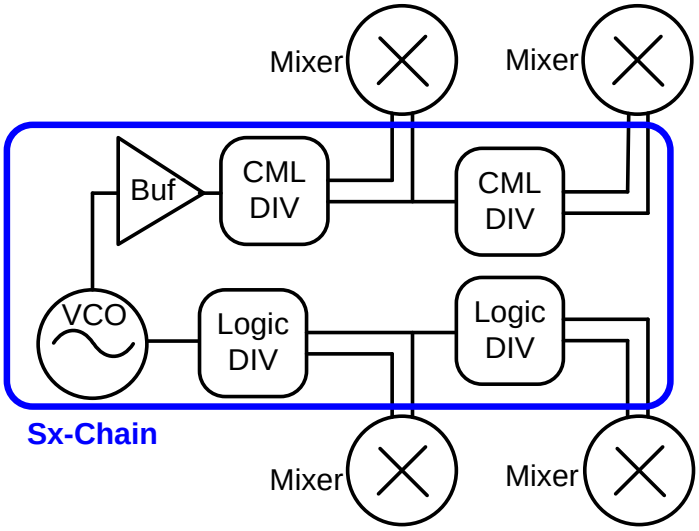

Figure 2. RF Transceiver Synthesizer (Sx) Chain structure

2. Sx-chain based PUF Implementation

Figure 3 shows the proposed Sx chain PUF implementation composed of VCO and DDiv-PUF circuit. Each VCO and divider has exactly same circuit structure and device size, however each oscillation frequency of VCO or divider has a little device to device variation and results in unique characteristics, and it can be used as a silicon fingerprint. Even within same chip, the imitation of unpredictable variation caused by process variation is impossible. The two multiplexers select two VCOs or two DDivs by challenge bit stream and two OSC frequencies are compared after two counting blocks during a fixed comparison time interval. The output is set to 0 or 1, depending on which counter value is high.

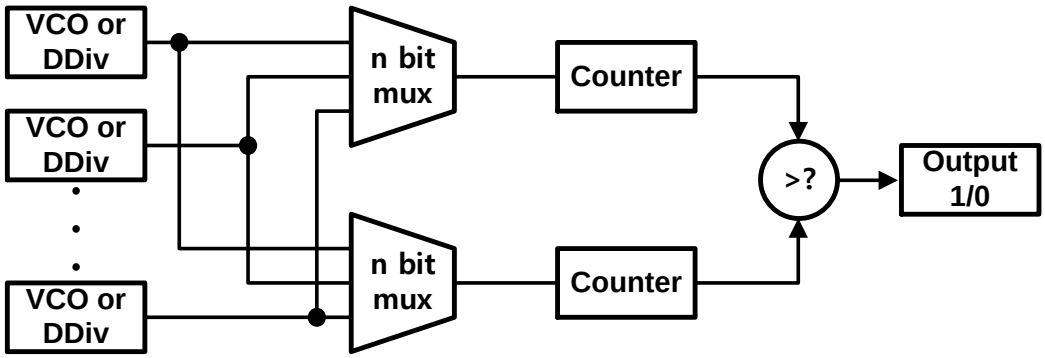

Figure 3. VCO and DDiv-PUF Circuit Implementation

3. VCO Based PUF

The proposed PUF VCO structure is shown in Figure 4. A switched bondwire inductor bank is used for wide frequency tunability, which enhances random variation. As depicted in Figure 4, mid and short length bondwire inductors are shunt-connected to long bondwire inductor. When all MOS switches are on state, switched inductor bank has lowest total inductance value, which causes highest OSC frequency. When all MOS switches in switched inductor bank are off, mid and short length bondwire inductors are disconnected, thus highest inductance value and lowest OSC frequency can be achieved. The challenge bit stream could select the Lbank bit which would be turned on, even if the same Lbank bit is selected and turned on, each VCO generates a little bit different OSC frequency and could show the silicon fingerprint. Though bondwire inductors are connected through MOS switches at on state, the Q factor degradation from MOS R_{on} resistance can be mitigated due to shunt connection with long bondwire inductor which is directly connected to VCO oscillation node without MOS switch. Therefore, oscillation is maintained during and after switching of the bondwire inductor bank.

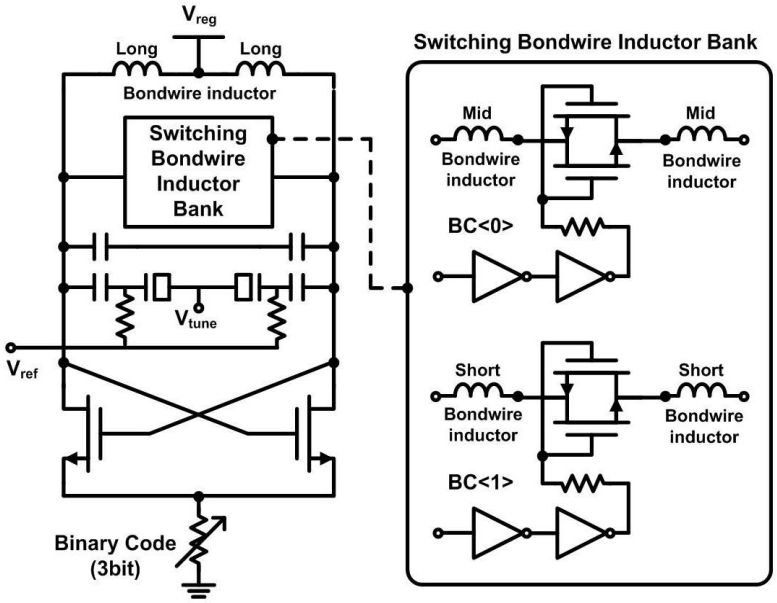

Figure 4. Proposed PUF VCO Structure with Bondwire Inductor Bank

For minimizing power consumption, the VCO bias current is varied between each frequency band by controlling the 3-bit binary weighted bias resistors. This programmability allows power consumption minimization. Considering these PUF VCO design issues, the proposed PUF VCO is designed in 65nm CMOS technology. Figure 5 shows the complete layout of the VCO. The chip size is 0.75 × 0.75 mm^2.

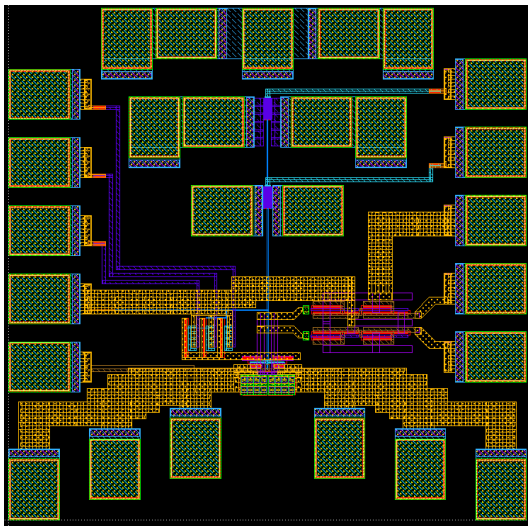

Figure 5. Complete Layout of the Proposed PUF VCO

The carrier signal frequency of the PUF VCO is tunable from 2.28 GHz to 2.33 GHz when all MOS switches are at off state, and when all MOS switches are at on state, the carrier signal frequency is tunable from 6.1 GHz to 6.38 GHz. The frequency band between 2.33 GHz and 6.1 GHz can be covered by controlling each MOS switch in the inductor bank separately. The full tuning range can also be covered by utilizing both switched capacitor bank and switched inductor bank. Figure 6 depicts the simulated frequency tuning range of the PUF VCO. The VCO core operates from 1.2V supply and biases at 6 mA.

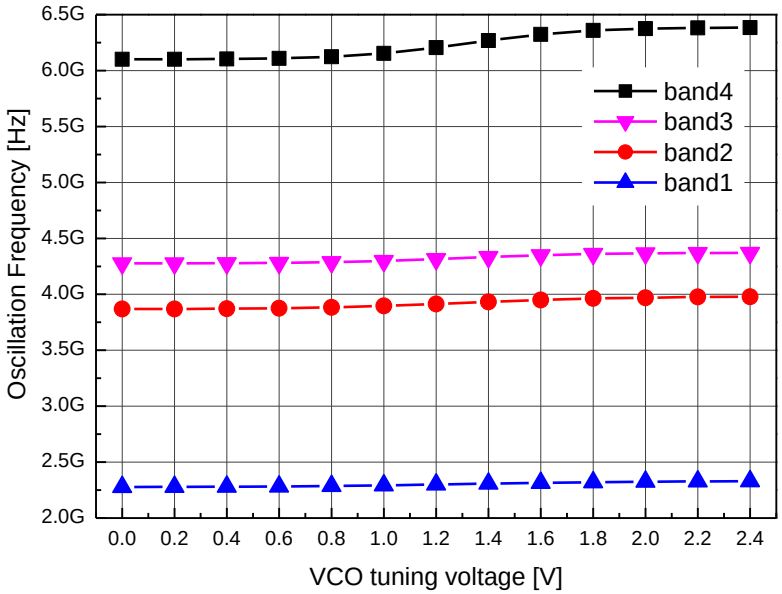

Figure 6. Simulated Frequency Tuning Range of the Proposed PUF VCO

4. Dynamic Divider based PUF

PUF does not store any secret key in device, the PUF device itself generates unique response immediately for the given challenge. Any invasive or semi-invasive attack will cause permanent alteration of the device physical characteristics and alter the PUF operation permanently. Figure 7 shows a schematic diagram of dynamic divider. Utilizing structures similar to digital logic gates, a rail-to-rail signal swing can be maintained by the energy from bias current[5, 6]. Full signal swing can be attained in this structure.

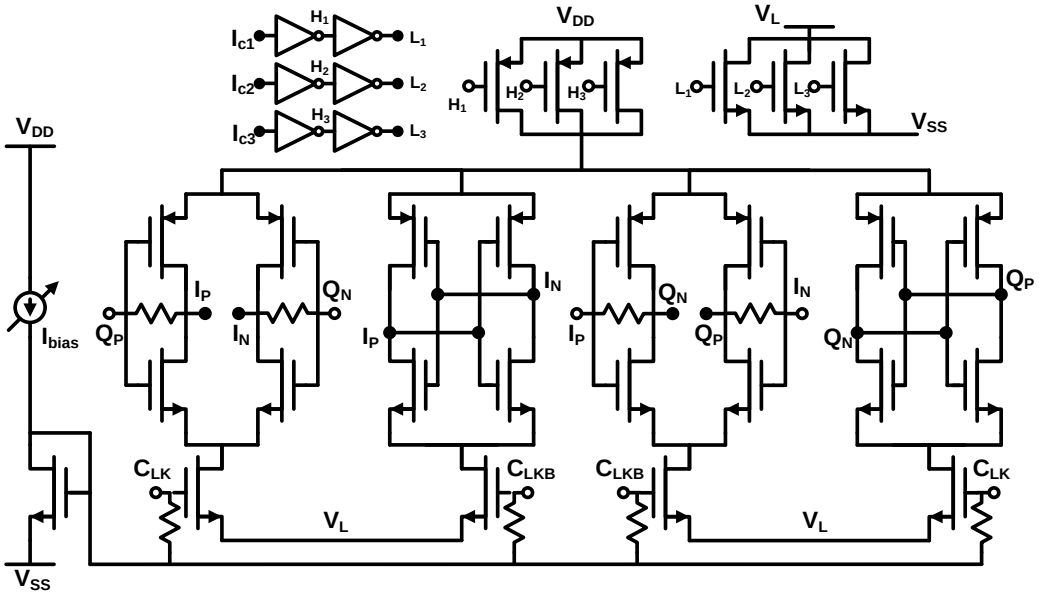

Figure 7. Schematic Diagram of Dynamic Divider

In the DDiv based PUF implementation, each divider has exactly same circuit structure and device size, however each self oscillation frequency(SoF) of divider has a little device to device variation and results in unique characteristics, silicon fingerprint. The flip-flops in dynamic divider have a feedback connection and generate self oscillation, which is depicted in Figure 8. Self oscillation frequency range of the divider can be largely varied by using current starved structure as dipicted in Figure 7, and Ibias can also change SoF by varying bias voltage of CLK and CLKB nodes[7, 8]. This wide tunability is helpful for enhancing random variation for PUF.

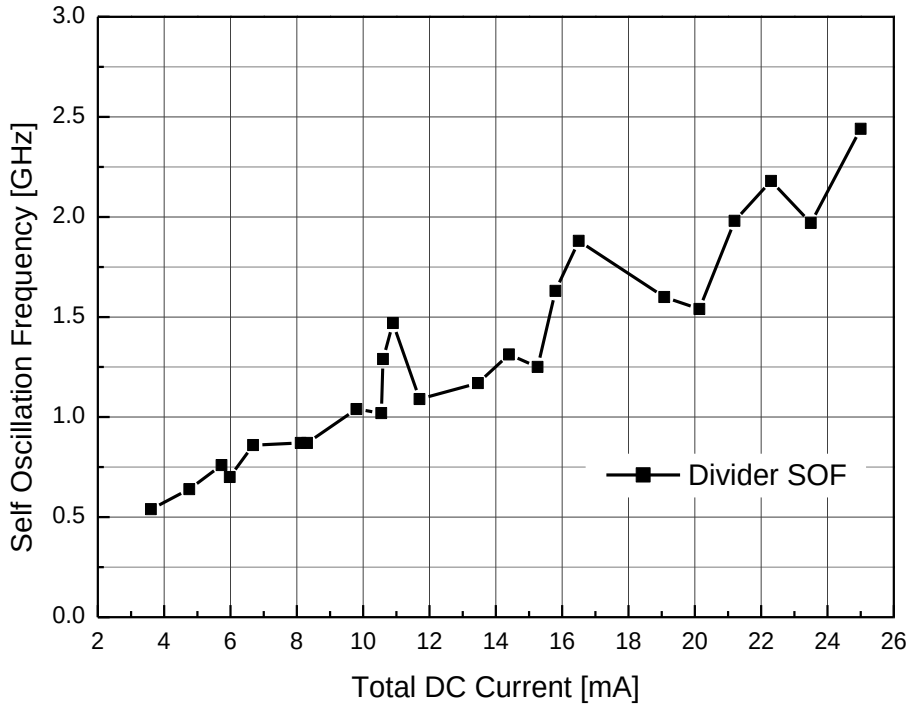

Figure 8. Self Oscillation Frequency Characteristics of DDiv

5. Sx-chain PUF based Authentication

Figure 9 shows a proposed simple authentication protocol for Sx-chain PUF based smart meter security. At first, smart meter gives a challenge(C) to energy monitor, The PUF in monitor generates unique response(R) and transfer this silicon fingerprint to smart meter. And smart meter checks the C to R data with PUF database(DB). If the acquired C to R data is matched with DB, smart meter authenticates the monitor. And then, in the same way, monitor gives a challenge to smart meter. The PUF in smart meter generates unique response and transfers the response to remote monitor. If the C to R is matched with DB in remote monitor, the monitor authenticates the smart meter, and the whole authentication process is finalized.

6. Conclusions

An Sx chain based PUF security for smart meter is proposed. Thanks to the oscillation frequency variation characteristics caused by semiconductor fabrication process, the lightweight and unclonable authentication method is proposed for resource-constrained smart meter security application. The simple authentication protocol is also presented for the Sx chain PUF based smart meter security.

Acknowledgments

This research was supported by Korea Electric Power Corporation through Korea Electrical Engineering & Science Research Institute. (grant number: R15XA03-67).

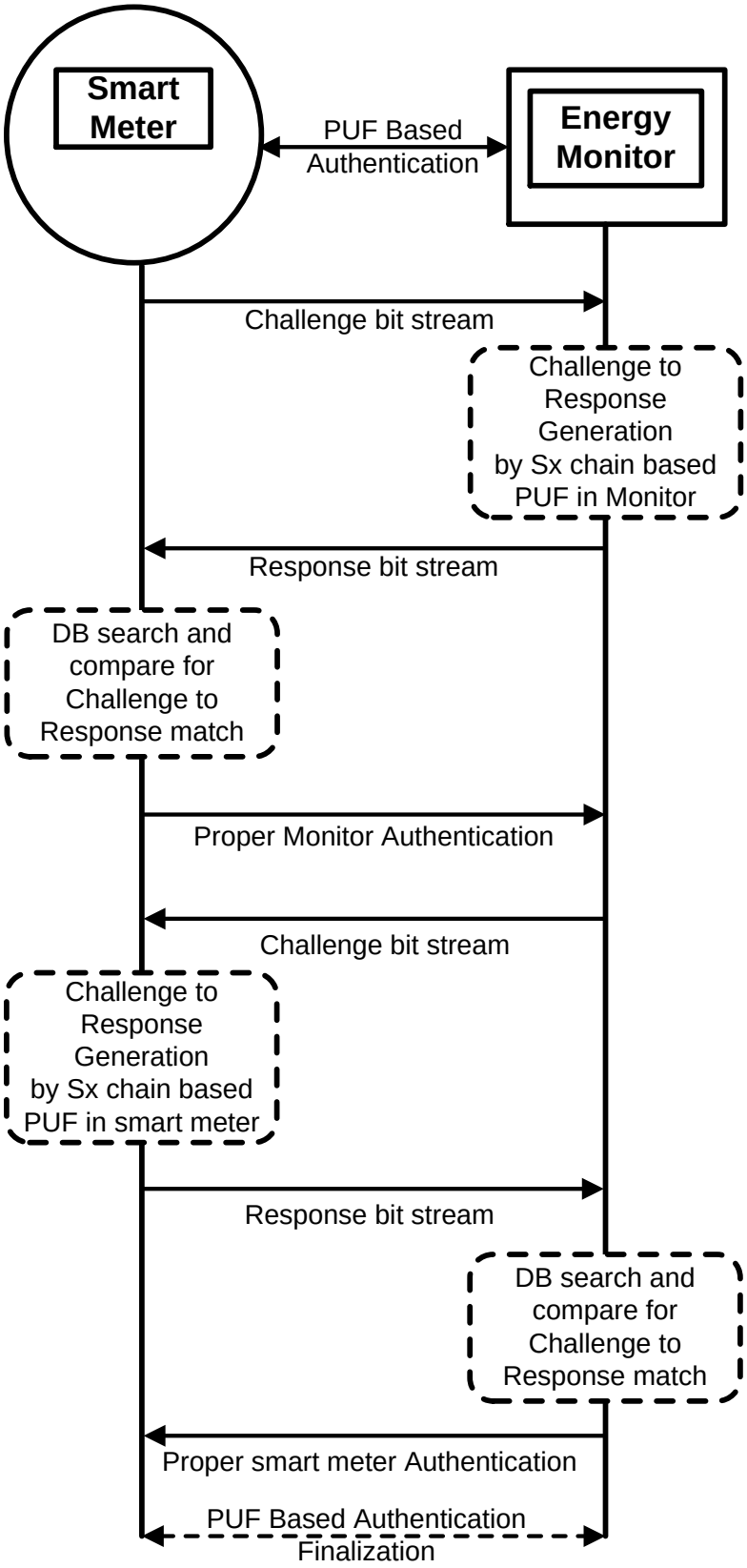

Figure 9. Sx chain PUF based Authentication Protocol

References

[1] M. D. H. Abdullah, Z. M. Hanapi, Z. A. Zukarnain and M. A. Mohamed, "Attacks, Vulnerabilities and Security Requirements in Smart Metering Networks", KSII Trans. on Internet and Information Systems, vol. 9, no. 4, **(2015)**, pp. 1493-1515.
[2] G. E. Suh, D. Clarke, B. Gassend, M. van Dijk, and S. Devadas, "Aegis: architecture for tamper-evident and tamper-resistant processing", in Proceedings of the 17th annual international conference on Supercomputing, **(2003)**.
[3] S. P. Skorobogatov, "Semi-invasive attacks – a new approach to hardware security analysis", University of Cambridge, Computer Laboratory, Tech. Rep. UCAM-CL-TR-630, **(2005).**
[4] S. Mangard, E. Oswald, and T. Popp, "Power Analysis Attacks: Revealing the Secrets of Smart Cards", Springer-Verlag New York, Inc., **(2007)**.
[5] C. Conroy and B. Kim, "RF Transceivers for wireless in standard CMOS: some perspectives", IEEE Radio and Wireless Symp., **(2006)**.
[6] M. Kim, T. Park, Y. Kwon, J. Lim, S. Park and S. Kim, "14-mW 5-GHz Frequency Synthesizer with CMOS Logic Divider and Phase-switching dual-modulus prescaler", in IEEE Radio Freq. Integr. Circuits Symp., **(2006)**.
[7] S. Ryu, "Multi-standard carrier generator with CMOS logic divider", in IEEE Int. Midwest Symp on Circuit and Systems, **(2009)**.
[8] A. Koukab, Y. Lei and M. J. Declercq, "A GSM-GPRS/UMTS FDD-TDD/WLAN 802.11a-b-g Multi-Standard Carrier Generation System", IEEE J. Solid-State Circuits, vol. 41, **(2006)**, pp. 1513-1521.

Author

Seonghan Ryu, he received the B.S. degree in Department of Electronic Engineering from Kyungpook National University in 1998. And M.S. degree in Department of Electronic and Electrical Engineering from POSTECH in 2000, Ph. D. degree from POSTECH in 2005. He is currently a professor at Department of Information and Communication Engineering, Hannam University since 2008. His research interests include RF transceiver architecture and CMOS IC design.

