PUF based Implantable Medical Device Security

Seonghan Ryu
Department of Information and Communication Engineering, Hannam University, Daejeon, Republic of Korea

Keywords: PUF, IMD, Dynamic Divider, CMOS, SoF.

Abstract: For the resource-constrained device such as Implantable Medical Device(IMD), lightweighting 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 IMD security with local oscillator(LO) chain composed of VCO and dynamic divider(DDiv), which use self oscillation frequency(SoF) variation characteristics. In the LO chain PUF implementation, the output bits are obtained by comparing the oscillation frequencies of different VCO L banks or dynamic dividers. For the lightweight operability, simple VCO and DDiv-PUF based authentication protocol is also proposed.

1 INTRODUCTION

Physical unclonable function is a hardware based promising security primitives, which is favored by resource constrained devices such as IMD. PUF makes use of the inherent process variation in semiconductor process such as CMOS technology. Implantable medical devices are widely used these days. In general, only monitoring function such as EEG, ECG and EMG are major application category, however stimulator such as deep brain stimulator(DBS) and pacemaker are also widely adopted. Therefore, the IMD security is becoming essential and cardinal issues. 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(Suh, 2003)-(Mangard, 2007). 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 and duplication of PUF characteristics is inherently impossible. Figure 1 shows the local oscillator(LO) chain for RF transceiver of IMD for wireless connectivity. This paper presents a PUF based IMD security using these LO chain block circuitry with inherent silicon fabrication process variation

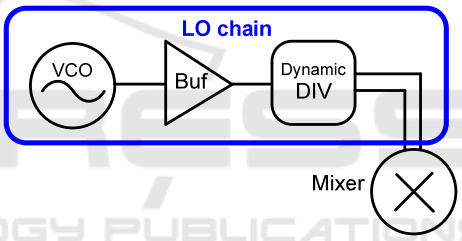


Figure 1: RF transceiver local oscillator(LO) chain structure.

2 LO-CHAIN BASED PUF IMPLEMENTATION

Figure 2 shows the proposed LO chain PUF implementation composed of VCO and DDiv-PUF circuit.

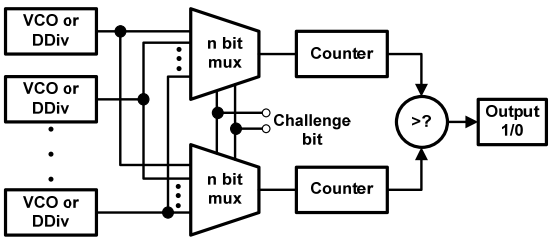


Figure 2: VCO and DDiv-PUF circuit implementation.

Each VCO and dynamic divider have unique oscillation(OSC) frequency, even within same chip,

Ryu, S.
PUF based Implantable Medical Device Security.
DOI: 10.5220/0008983701650168
In *Proceedings of the 13th International Joint Conference on Biomedical Engineering Systems and Technologies (BIOSTEC 2020) - Volume 1: BIODEVICES*, pages 165-168
ISBN: 978-989-758-398-8; ISSN: 2184-4305

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

3 DYNAMIC DIVIDER BASED PUF

Each divider has exactly same circuit structure and device size, however each self oscillation frequency of divider has small device to device variation and results in unique characteristics such as silicon fingerprint.

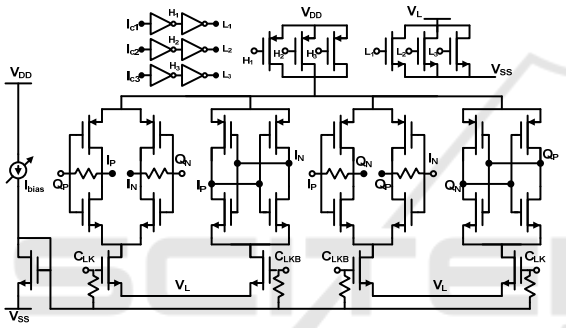


Figure 3: Schematic diagram of dynamic divider.

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 3 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(Conroy, 2009)~(Kim, 2006). Full signal swing can be attained in this structure. The flip-flops in dynamic divider have a feedback connection and generate self oscillation, which is depicted in Figure 4. Self oscillation frequency range of the divider can be largely varied by using current starved structure as dipicted in Fig. 3, and Ibias can also change SOF by varying bias voltage of CLK and CLKB nodes(Ryu, 2009)~(Koukab, 2006). This wide tunability is helpful for enhancing random variation for PUF.

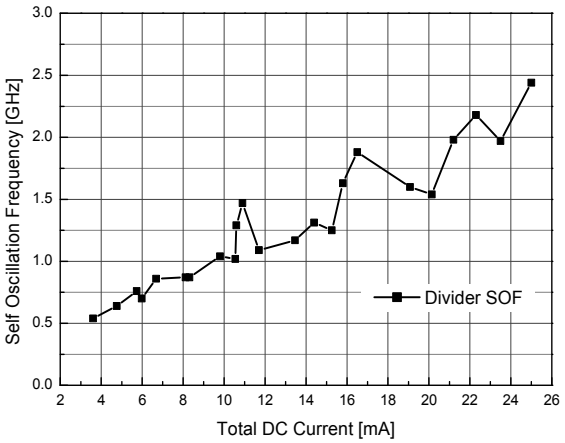


Figure 4: Self oscillation frequency characteristics of DDiv.

4 VCO BASED PUF

The proposed PUF VCO structure is shown in Figure 5. A switched bondwire inductor bank is used for wide frequency tunability, which enhances random variation.

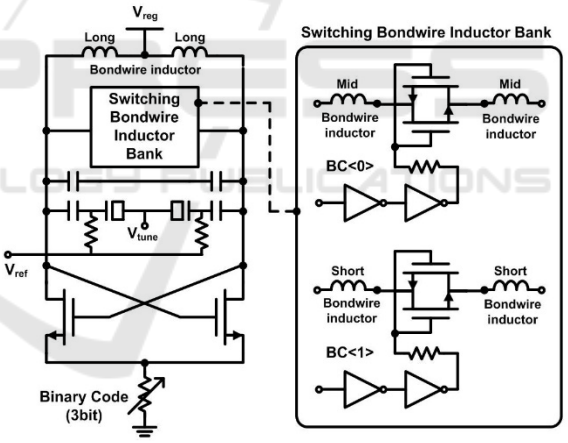


Figure 5: Proposed PUF VCO structure with bond-wire inductor bank.

As depicted in Figure 5, 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 and highest inductance value, therefore lowest OSC frequency can be achieved. The challenge bit stream could select the L bank bit which would be turned on, even if the same L bank 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 Ron 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 bondwire L bank switching.

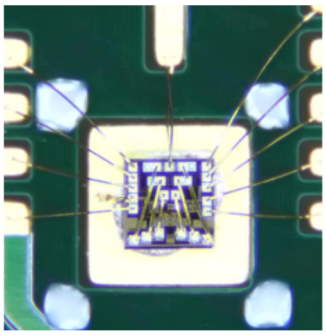
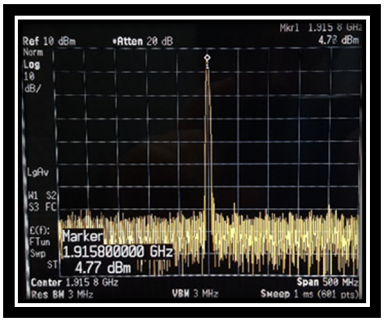


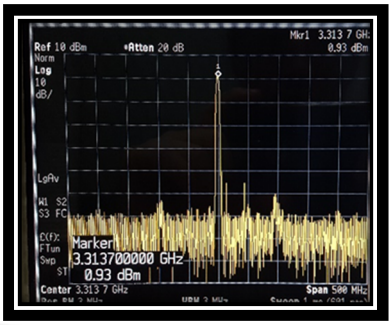
Figure 6: The fabricated PUF chip on board.

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 implemented in 65nm CMOS technology. Figure 6 shows the fabricated chip on board with bondwire incuctor. The chip size is 0.75 × 0.75 mm^2.

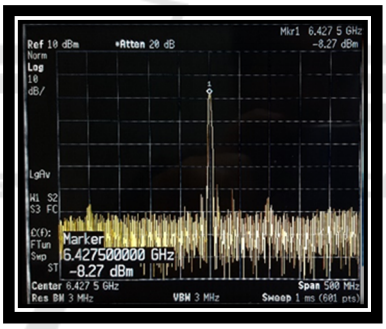
Figure 7 depicts the measured frequency tuning range for the proposed PUF VCO. The carrier signal frequency of the PUF VCO is tunable from 1.91GHz when all MOS switches are at off state to 6.42GHz when all MOS switches are at on state. The whole frequency band can be covered by controlling each MOS switch in the inductor bank separately. The full tuning range can also be covered by utilizing both switched capacitor bank and switched inductor bank. The VCO core operates from 1.2V supply and biases at 6 mA.



(a)



(b)



(c)

Figure 7: Measured oscillation frequency of the proposed PUF VCO when (a) all MOS switches are at off state (b) one switch is at on and another is at off state (c) all MOS switches are at on state.

5 LO-CHAIN PUF BASED AUTHENTICATION

Figure 8 shows a proposed simple authentication protocol for LO(Sx) Chain PUF based implantable medical device security. At first, IMD gives a challenge(C) to remote health monitor/stimulator, The PUF in monitor/stimulator generates unique response(R) and transfer this silicon fingerprint to IMD. And IMD check the C to R data with PUF database(DB). If the acquired C to R data is matched

with DB, IMD authenticate the health monitor/stimulator. And then, in the same way, health monitor/stimulator gives a challenge to IMD. The PUF in IMD generates unique response and transfers the response to remote monitor. If the C to R is matched with DB in remote monitor, the monitor authenticate the IMD, and the whole authentication process is finalized.

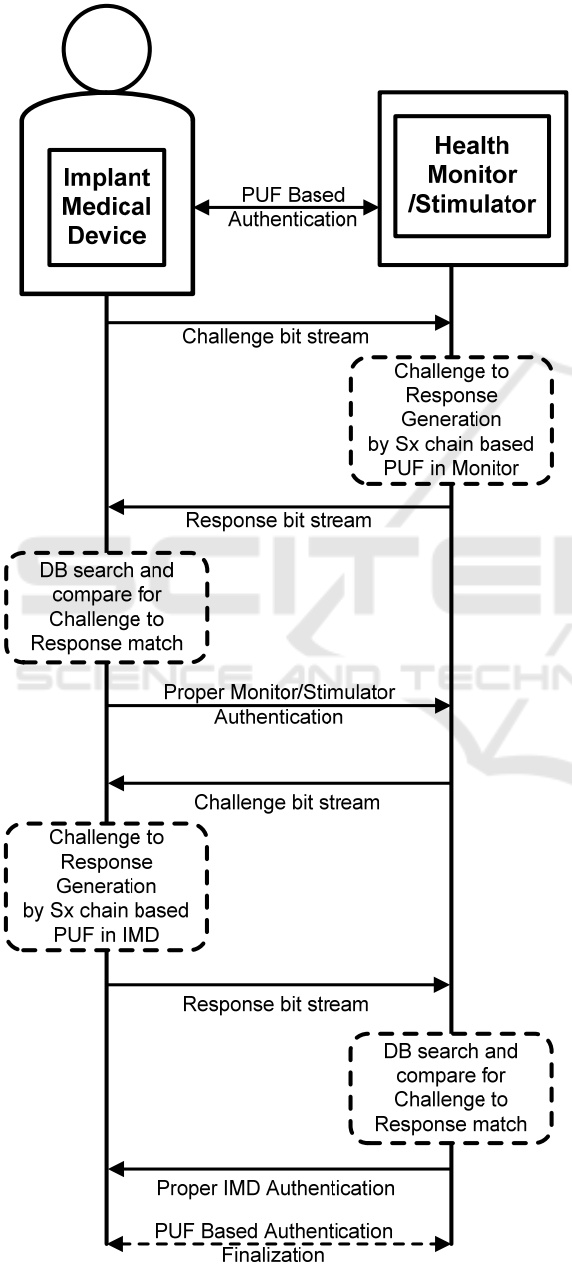


Figure 8: LO(Sx) chain PUF based authentication protocol.

6 CONCLUSIONS

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

ACKNOWLEDGEMENTS

This work was supported by the National Research Foundation of Korea under Grant NRF-2017R1D1A1B03036412; IDEC(EDA Tool, MPW).

REFERENCES

G. E. Suh, D. Clarke, B. Gassend, M. van Dijk, and S. Devadas, 2003. “Aegis: architecture for tamper-evident and tamper-resistant processing,” in *Proceedings of the 17th annual international conference on Supercomputing, ser. ICS ’03*. New York, NY, USA: ACM.

S. P. Skorobogatov, 2005. “Semi-invasive attacks – a new approach to hardware security analysis,” *University of Cambridge, Computer Laboratory,* Tech. Rep. UCAM-CL-TR-630.

S. Mangard, E. Oswald, and T. Popp, 2007. Power Analysis Attacks: Revealing the Secrets of Smart Cards. *Springer-Verlag New York, Inc.*

C. Conroy and B. Kim, 2006. “RF Transceivers for wireless in standard CMOS: some perspectives,” *IEEE Radio and Wireless Symp.*, pp. 7–10, Oct.

M. Kim, T. Park, Y. Kwon, J. Lim, S. Park and S. Kim, 2006. “14-mW 5-GHz Frequency Synthesizer With CMOS Logic Divider and Phase-switching dual-modulus prescaler,” in *IEEE Radio Freq. Integr. Circuits Symp*., pp. 4, Jun.

S. Ryu, 2009. “Multi-standard carrier generator with CMOS logic divider,” in *IEEE Int. Midwest Symp on Circuit and Systems., Cancun*. pp. 1059–1062, Aug.

A. Koukab, Y. Lei, M. J. Declercq, 2006. “A GSM-GPRS/UMTS FDD-TDD/WLAN 802.11a-b-g Multi-Standard Carrier Generation System,” *IEEE J. Solid-State Circuits, vol. 41*, pp. 1513-1521.