A Novel ROPUF for Hardware Security

Sauvagya Ranjan Sahoo
NIT Rourkela
sauvagya.nitrkl@gmail.com

Sudeendra Kumar
NIT Rourkela
sudi_023@yahoo.co.in

Kamalakanta Mahapatra
NIT Rourkela
kkm@nitrkl.ac.in

***Abstract*—Physical Unclonable Functions (PUFs) are promising security primitives in recent times. A PUF is a die-specific random function or silicon biometric that is unique for every instance of the die. PUFs derive their randomness from the uncontrolled random variations in the IC manufacturing process which is used to generate cryptographic keys. Researchers have proposed different kinds of PUF in last decade, with varying properties. Quality of PUF is decided by its properties like: uniqueness, reliability, uniformity etc. In this paper we have designed a novel CMOS based RO PUF with improved quality metrics at the cost of additional hardware. The novel PUF is a modified Ring Oscillator PUF (RO-PUF), in which CMOS inverters of RO-PUF are replaced with Feedthrough logic (FTL) inverters. The FTL inverters in RO-PUF improve the security metrics because of its high leakage current. The use of pulse injection circuit (PIC) is responsible to increase challenge-response pairs (CRP's). Then a comparison analysis has been carried out by simulating both the PUF in 90 nm technology. The simulation results shows that the proposed modified FTL PUF provides a uniqueness of 45.24% with a reliability of 91.14%.**

***Keywords*— Physical Unclonable Function (PUF); Challenge-Response pair (CRP); Feedthrough logic (FTL); Ring Oscillator (RO); process variation (PV).**

I. INTRODUCTION

Various Si and non Si PUFs are described in the literature which uses complex mapping functions embedded in a physical structure. Lofstrom et al. in 2000 explored the pioneering work in the area of PUF by providing a method to extract chip specific data from manufacturing variation by comparing drain currents of two nominally identical transistors for IC identification [1]. In 2002, Pappu et al. presented the concept of non Si Physical one-way function i.e. optical PUF [2] proceeded by several other non Si PUF. However in this paper we will limit our discussion to Si PUFs only because they can be easily integrated into IC chips and it exploits manufacturing variability in interconnection /MOSFET delay to generate unique CRPs. Gassend et al. in 2002 were the first to implement Si PUF on FPGA [3] termed as arbiter PUF. Arbiter PUF extracts the chip signature from the delay variation between two identical symmetrical paths. Since the delay of different path can be easily modelled hence it is more susceptible to modelling attack. To improve its quality metrics Suh et al. in 2007 proposed RO-PUF [4]. Out of several PUF discussed in literature RO PUF [4, 5] is widely used for cryptographic key generation because of its better uniqueness and high reliability.

II. PROPOSED PULSE CONTROLLED RO PUF

The RO PUF discussed in [4] having a few CRPs, hence termed as a weak PUF. In this section we proposed a modified RO PUF to increase the CRPs along with improvement of various security metrics. The proposed a modified PUF termed as Pulse controlled RO PUF as shown in Fig. 1.

- The function of PIC block is to generate a pulse of variable width & amplitude which is applied to enable input (one input of NAND gate) of RO PUF.
- RO PUF consists of 13 RO. Each RO consist 12 stages of inverter and one NAND gate.
- Each inverter is designed using feedthrough logic (FTL) [6]. FTL inverters are faster as compared to its counterpart static CMOS, thus with equal no. of cascading inverters RO designed using FTL provides higher operating frequency.
- Few challenges drive PIC circuit and few challenges drive MUX to select a pair of RO, hence increases overall CRPs.
- The frequency of each RO is unique which depends upon process manufacturing variation (PMV) and different pulses generated from PIC.
- These frequencies are compared depending upon challenge input to MUX. Comparator produces a response of 0 or 1 depending upon count of counter.
- Response is obtained by comparing adjacent RO i.e. frequency on 1st RO is compared with 2nd, 2nd is compared with 3rd, and so on.

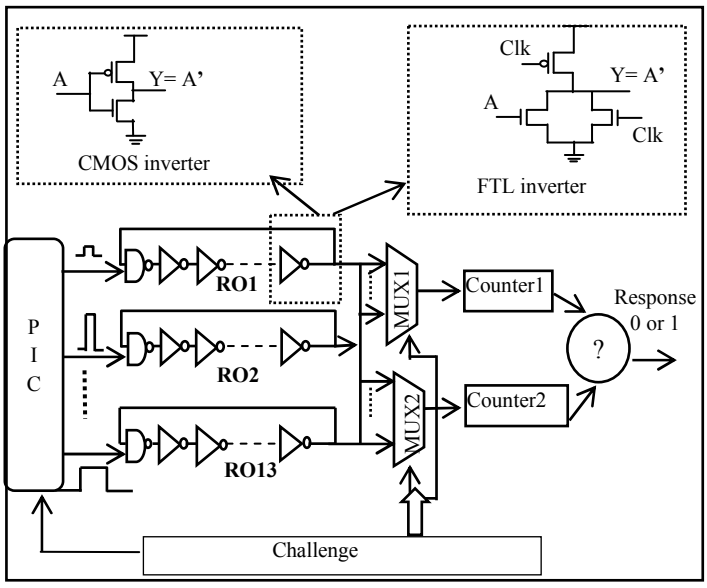

Fig. 1. Proposed Pulse Controlled RO PUF

978-1-4799-1743-3/15/$31.00 ©2015 IEEE

III. Simulation Results & Discussion

Simulations are carried out in Cadence Virtuoso Environment using SPECTRE Spice. The technology libraries used are from UMC foundry for CMOS 90nm process. Table 1 shows propagation delay (tp) and leakage current (I_{leak}) comparison for 10 stages of inverter simulated in 90 nm, 1 V CMOS process technology using CMOS and FTL. Simulation results shows that FTL is 1.5 times faster than CMOS logic and leakage current in FTL is also higher. This higher leakage current makes RO to more sensitive to process variation [5].

Table 2 shows the variation in CV [5] for the RO designed by static CMOS and FTL inverter for 20 Monte Carlo runs. It shows that standard deviation (σ) for FTL RO is more as compared to CMOS RO because of inverters designed in FTL possesses more leakage current as compared to CMOS. Higher σ means frequency separation between different RO in a group is very high which is responsible for improvement in CV of FTL RO. This higher CV of the RO designed by FTL leads to improvement in uniqueness of proposed PUF.

The variation in σ for frequency of RO with reduction in supply voltage V_{DD} at different corner is shown in Table 3. FF transistors retains higher value of σ because of its lower V_t. Reduction in supply voltage causes reduction in I_D and the MOSFET starts entering into subthreshold region from saturation region. Due to exponential nature of Isub [21] process variation is more which causes σ to increases.

A 16-bit signature is obtained for 20 different PUF. The number of CRP's collected for analyzed the security properties is 1024. Comparison between various security metrics [5] for both the PUF are shown in Table 4. Uniqueness of proposed PUF architecture increases due to higher leakage current of FTL inverter. Higher reliability of proposed PUF avoids the use of error correcting codes, this led to hardware efficient. Both the PUF exhibits nearly same uniformity.

The variation of security metrics for the proposed PUF architecture using high and low V_t MOSFET is shown in Table 5. Lower V_t MOSFET responsible for high leakage current hence largely affected by process variation which led to higher uniqueness.

TABLE 1 SIMULATION RESULTS FOR t_p & I_{leak} FOR THE CMOS AND FTL CASCADED INVERTERS (10-STAGES)

Logic family	t_p <ns>	I_{leak} <nA>
CMOS	0.421	12.57
FTL [6]	0.219	21.12

TABLE 2 FREQUENCY SEPARATIONS FOR RO IN DIFFERENT LOGIC FAMILY

Logic family	μ<in GHz>	σ<in MHz>	CV
CMOS	2.044	35.216	1.219
FTL	3.196	119.055	3.621

TABLE 3 FREQUENCY SEPARATIONS BETWEEN DIFFERENT CORNERS FOR RO

V_{DD} <in V>	σ<in MHz>					
	FF		NN		SS	
	CMOS	FTL	CMOS	FTL	CMOS	FTL
1	80.85	140.5	35.21	119.1	33.53	71.66
0.8	89	143.5	40.67	121	36.53	90
0.5	90.26	144	88.2	121.2	77.1	90.04

TABLE 4 SECURITY METRIC COMPARISONS

	RO PUF [5]	Proposed RO PUF	Ideal Value [5]
Uniqueness	41.23%	45.24%	50%
Reliability	89.15%	91.14%	100%
Uniformity	41.45%	41.15%	50%

TABLE 5 SECURITY METRIC COMPARISONS OF PROPOSED RO PUF AT DIFFERENT V_t

	Lower Vt MOSFET	Higher Vt MOSFET
Uniqueness	46.85%	41.71%
Reliability	92.54%	90.12%
Uniformity	40.79%	42.34%

IV. Conclusion

A modified pulse controlled RO PUF is proposed in this paper, which increases CRP's than the existing RO PUF. Using FTL instead of CMOS to design RO improves the security metrics like uniqueness and reliability. Further the security metrics are enhanced at lower VDD and by using lower threshold voltage transistor. These proposed PUF can be a better choice for security applications where area penalty is not a major issue.

References

[1] K. Lofstrom, W. R. Daasch, and D. Taylor, "IC identification circuit using device mismatch," *in IEEE Solid-State Circuits Conference*, pp. 372-373, 2000.

[2] R. S. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, "Physical one-Way functions," *Science,* vol. 297, pp. 2026-2030, Sep.2002.

[3] B. Gassend, D. Clarke, M. van Dijk, and S. Devdas, " Silicon physical random functions," in Proc. 9th ACM. Conf. Computer Communication security, pp. 148-160, 2002.

[4] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," *In Proc. of ACM/IEEE Design Automation Conference*, pp. 9–14, 2007.

[5] I. Kim, A. Maiti, L. Nazhandali, P. Schaumont, V. Vivekraja, and H. Zhang, "From statistics to circuits: Foundation for future PUF," in towards Hardware-intrinsic security, information security and cryptography,springer-verlag, pp. 55–78, 2010.

[6] V. Navarro-Botello, J. A. Montiel-Nelson, and S. Nooshabadi, "Analysis of high performance fast feedthrough logic families in CMOS," *IEEE Trans. Cir. & syst. II*, vol. 54, no. 6, pp. 489-493, 2007.