Energy and Area Aware Digital Fingerprint Generator Using Intrinsic Randomness

Jawar Singh, Sandeepkumar Pandey and Pramod K Tiwari
Energy and Area Aware Digital Fingerprint Generator Using Intrinsic Randomness

Sandeepkumar Pandey
Department of Electronics Engineering,
Shri Ramdeobaba College of Engineering and Management,
Nagpur, India, 440013
Email:pandeys@rknec.edu

Jawar Singh and Pramod K Tiwari
Department of Electrical Engineering,
Indian Institute of Technology Patna,
Bihar, India, 801106
Email:(jawar, pktwari}@iitp.ac.in

Abstract—Manufacturing variability/fluctuations is a major concern in integrated circuits and this has been exploited to design a hardware security primitive or digital fingerprint generator, referred as physical unclonable function (PUF) for resource constrained low power applications. The proposed architecture employs single transistor as PUF cell, one operational amplifier (OpAmp), and little peripheral circuitry, thereby making it very light and suitable for resource constrained applications. Simulation results show that the energy consumption of proposed design is 30fJ/bit which is 6.33 \times lesser than earlier reported design, it has 0.0025\mu m² area/bit and the values of 1s and 0s are equi-probable with probability of a ‘1’ being 50.2%. The mean measured by inter HD plot is 49.72 which is very close to an ideal value of 50%. This affirms that the proposed PUF can supply unique identifiers.

Keywords—Physical Unclonable Function (PUF), Security, Low energy consumption, Digital fingerprint.

I. INTRODUCTION

Aggressive scaling of CMOS technology, two major sources of process variations manifest themselves in the form of sub-wavelength lithographic variation and variations resulting from variations in quantity and locality of dopant atoms [2]–[4]. Random Dopant Fluctuation (RDF) and Line Edge Roughness (LER) influence the threshold voltage \(V_T\) of the MOSFET, which in turn becomes a random function. This random function could be exploited to generate a hardware circuitry and whose electrical properties are unique and driven by physical traits of MOSFETs called PUF. These are emerging hardware security primitive circuits widely used for secret key generation, identification, and authentication of electronic devices. Different approaches and various topologies for PUF realization have been studied and proposed in the literature. Published PUF implementations could broadly be classified as: SRAM based PUFs, arbiter PUFs, RO (Ring Oscillator) PUFs, and optical PUFs [5]–[8].

However, main challenges associated with PUF designs include: relatively small challenge space, high resource utilization, power consumption, and susceptibility to modeling attacks. Particularly, the PUF architectures proposed in [9]–[11] have high resource utilization overhead. This presents serious bottleneck in resource constrained designs. We propose a PUF architecture which extracts and amplifies the process variations outlined above to generate secret keys. The proposed PUF is evaluated on important performance matrices of standard PUF design and it is observed that our design has extremely low power and resource utilization.

II. SELF-CORRECTING OVERDRIVE VOLTAGE TRACKING CIRCUIT ALONG WITH AMPLIFIER STAGE

We propose a PUF architecture which extracts and amplifies the random fluctuations or intrinsic randomness that arises during manufacturing of integrated circuits to generate secret keys. A sub-threshold CMOS PUF cell is proposed as shown in Fig. 1, where, transistor \((M_1)\) is used to extract process fluctuations and made to operate in sub-threshold region by applying appropriate \(V_{GG}\) and \(I_{DM1}\). The reason of operating \(M_1\) in sub-threshold region is that process fluctuations are dominant and related to overdrive voltage \(V_{DS} - V_T\) that yields percentage variation in \(I_{DS}\) versus \(V_{GS}\) higher in this region. Also the transistors \(M_3\) and \(M_4\) of amplifier stage, as shown in Fig. 1 are operated in sub-threshold region to have lower energy dissipation.

If we ensure constant \(V_{DS}\) and \(I_{DS}\) through \(M_1\) then, the overdrive voltage would be constant. However, random fluctuation in \(V_T\) forces the \(V_{GS}\) for self-correction to keep \((V_{GS} - V_T)\) constant. In other words, random fluctuation in \((V_T)\) of \(M_1\) is translated to change in \((V_{GS})\) and later...
amplified by the amplifier stage for secret key generation. In Fig. 1, a constant current $I_{DM1}$ through $M_1$ is set and the source follower ensures fixed $V_{DS}$ across $M_1$. If the $(V_T)$ of the $M_1$ changes then so does the source voltage thereby keeping the term $(V_{GS} - V_T)$ as constant. Since threshold voltage fluctuation is random in nature, we can say that $V_{GS}$ variation is random too. For array of such devices whose $(V_T)$ is assumed to vary randomly due to process fluctuations and same is extracted for generation of secret keys. The extracted randomness in the form of source voltage variation in correspondence with $(V_T)$ variation is further amplified by the presented amplifier stage comprising of $M_3$ and $M_4$. The $I_{DS}$ in sub-threshold region changes exponentially with $V_{GS}$. Therefore, $V_S$ gets amplified at $V_{out}$. Node voltage $V_S$ corresponds to the sensed change in threshold voltage which is amplified by amplifier stage. The voltage variation at $V_S$ are such that it never goes beyond the threshold voltage of $M_3$. This means that $M_3$ always operates in sub-threshold region. The amplifier stage is designed to improve the voltage swing available at $V_S$. The gain of the amplifier has been obtained analytically using small signal equivalent model of amplifier in [18], as shown in Fig. 2. Due to small variation at node $V_S$, the gain is expressed as:

$$\frac{v_{out}}{v_s} = g_{mM3} (r_{oM3}/r_{oM4})$$  \hspace{1cm} (1)$$

Because of sub-threshold operation, the current is expressed as [19]:

$$I_{sub} = A \times e^{(V_{gs} - V_{th0} - \gamma V_{st} + n V_{ds})/m v T} \times (1 - e^{(-V_{ds}/v_T)}) \hspace{1cm} (2)$$

where,

$$A = \mu_0 C_{ox} \frac{W}{L_{eff}} v_T^2 e^{1.8} \hspace{1cm} (3)$$

$\mu_0$ is carrier mobility, $\eta$ is the drain induced barrier lowering (DIBL) coefficient, $\gamma$ is the body effect coefficient, $m$ is the sub-threshold swing coefficient of the transistor and $V_T$ is the thermal voltage. From (2) the small signal parameters i.e $g_m$, $r_o$ are calculated as

$$g_{mM3} = \frac{\partial I_{ds}}{\partial V_{gs}} = \frac{\partial I_{ds}}{\partial V_S} = \frac{I_{ds}}{m_{M3} v_T} \hspace{1cm} (4)$$

$$r_{oM3} = \frac{1}{\frac{\partial I_{ds}}{\partial V_{ds}}} = \frac{1}{\frac{m_{M3} I_{ds}}{m_{M3} v_T}} \hspace{1cm} (5)$$

$$r_{oM4} = \frac{1}{\frac{\partial I_{ds}}{\partial V_{ds}}} = \frac{1}{\frac{m_{M4} I_{ds}}{m_{M4} v_T}} \hspace{1cm} (6)$$

by combining (1) , (4) , (5) , (7), we get:

$$\frac{v_{out}}{v_s} = \frac{m_{M4}}{m_{M3} \eta + m_{M3} \eta m_{M4}} \hspace{1cm} (7)$$

The length of the transistor $M_3$ and $M_4$ is used for gain enhancement of amplifier stage since it modifies the respective DIBL coefficients.

III. THE PUF ARCHITECTURE OF SECRET KEY GENERATION

The complete PUF architecture of secret key generation is shown in Fig. 3. This is based on the self-correcting excess voltage tracking circuit described in Fig. 1. Challenges are applied to row and column decoders based on which a particular device is selected. The applied row challenges select the gate of row transistors $R_x$ (i.e,1,2,3,...N), such that the source voltage $V_{Sx}$ (x=1,2,3,...N) gets applied to the input of source follower circuit. The same gets applied to the amplifier stage for amplification. The output of source follower circuit is applied to the non-inverting input of the OpAmp. The other input (inverting) of the OpAmp is obtained from $V_{DSX}$ (x=1, 2, 3, 4, 5,..N). For example the applied challenge to the row decoder and column is such that it internally selects row-0 and column-4 so that $C_2=0$, $C_{4bar}=1$ and $R_0=1$. This selects the green colored transistor in dashed ellipse, as shown in Fig. 3. Fixed constant current $I_{DSM}$ is made to flow through the path OpAmp-$V_{DS1}$-V$S_{1}$-ground. This is shown with red arrow in Fig. 3, and corresponding flow of current is as shown in Fig. 1 with same red colored arrow. Source follower and OpAmp together ensure that the constant $V_{DS}$ is applied to the green transistor (or any other selected device). Also the current source $I_{DMN}$ ensures constant current is applied through the selected transistor. Hence, the random process variations in threshold voltage are available at node $V_{S1}$ in the Fig. 3 that is further amplified by amplifier stage and given to key storage register through buffer circuit. The switching threshold of the buffers is designed at half of the swing available at the output of the amplifier stage. Complete process for secret key generation is shown step-by-step in Fig. 4 with the help of a flow chart. Therefore, random but consistent outputs are generated out of the buffer circuit which is stored in the secret key storage register.

More popular PUF architectures such as delay-based PUFs are prone to modeling attacks, because their basic building topologies can be mathematically represented by model whose unknown delay coefficients can be estimated by machine learning techniques from the gathered challenge-response pairs. Our proposed PUF architecture directly uses a random amount of $V_T$ fluctuation available in manufacturing process. This will make it more resilient to attacks. The single transistor selection for random $V_T$ extraction employs a two dimensional array structure addressable by row and column decoders. This increases the challenge response space. For proposed PUF with M challenge bits applied at the row decoder for row selection and N challenge bits applied at the column decoder for column selection, there could be $2^M \times 2^N$ challenge-response pairs. This satisfies the criterion for strong PUF. The proposed architecture selects one
transistor at a time for secure bit generation. Thus, required variable key lengths could be generated based on platform requirements and computational constraints.

The threshold voltage \( V_T \) fluctuations or the mobility \( \mu \) fluctuations during fabrication are the two MOSFET parameters which could be effectively used to realise PUFs. Since these parameters show local fluctuations due to statistical fluctuations. Our PUF working in the sub-threshold region is characterized by the \( V_T \) variations of the selected MOSFETs. The \( V_T \) can be expressed as a function of temperature as \[ V_T(T) = V_T(T_0) \cdot (1 + TCV_T \cdot (T - T_0)) \] (8) where \( V_T \) is measured at the temperature \( T_0 \) and the temperature coefficient of \( V_T \) is defined as:

\[ TCV_T = \frac{1}{V_T} \cdot \frac{\partial V_T}{\partial T} \] (9)

In our PUF design, temperature dependence can be compensated by varying the bias current with temperature. Thus, \( V_{GS} \) changes corresponding to \( V_T \) changes in selected transistors could be made to stay constant with varying temperature.

IV. SIMULATION RESULTS

All the simulation results are obtained from 50 nm CMOS technology models with \( V_{DD}=1V \). The energy consumption \( E_{\text{bit}} \) of the proposed PUF is evaluated as: \[ E_{\text{bit}} = I_{\text{drawn}} \cdot V_{DD} / f_{\text{clk}} \] where, \( I_{\text{drawn}} \) is the current drawn from supply to produce the response bit, \( V_{DD} \) is the supply voltage, and \( f_{\text{clk}} \) is the applied clock frequency. The circuit draws 30nW for 1us for one bit generation thereby giving \( E_{\text{bit}} \) of 30 fJ/bit which is 6.33X lesser than \[12\]. A comparison of energy efficiency of the proposed PUF design with the earlier reported PUF designs is shown in Fig. 5. At the nominal operating condition, the proposed PUF achieves an \( E_{\text{bit}} \) of 30 fJ/bit.

Uniqueness is another very important security metric for PUF. The quality of a given PUF instance to provide an unambiguously distinct behavior in comparison with different other PUFs with the identical topology implemented on different chips is measured by this quantity. Suppose the two PUFs (each with a challenge response pair (CRP) of 6 bits are to be realized on two distinct chips. When both the PUFs are subjected to same challenge say (010101) then the response obtained from each PUF is distinct. Assuming the Hamming distance between obtained response is 2, which implies that 25% of the response bits differ. Ideally Uniqueness should be close to 50%. Fig. 7 shows the inter Hamming distance (HD) of die for one thousand runs. The mean measured by inter HD plot, as shown in Fig. 7 with mean of 49.72 which is very close to an ideal value of 50%. This affirms that the proposed PUF can supply unique identifiers.


