Statistical Analysis of MUX-based Physical Unclonable Functions

Yingjie Lao, *Student Member, IEEE*, and Keshab K. Parhi, *Fellow, IEEE*

***Abstract*— Physical unclonable functions (PUFs) can store secret keys in integrated circuits by exploiting the uncontrollable randomness due to manufacturing process variations. These PUFs can be used for authentication of devices and for key generation in security applications. This paper presents a rigorous statistical analysis of various types of multiplexer PUFs including the MUX PUF, the feed-forward MUX PUF, the modified feed-forward MUX PUF, and multiplexer-demultiplexer (MUX/DeMUX) PUF. The modified feed-forward MUX PUF structure is a new structure that is introduced in this paper. Three types of feed-forward PUFs are analyzed in this paper. These include feed-forward overlap, feed-forward cascade and feed-forward separate. The performance analysis quantifies inter-chip and intra-chip variations as a function of the number of stages for different PUFs, the process variation variance, the environmental noise variance, and the arbiter skew. Three other metrics of performance are also introduced and analyzed in this paper; these include *reliability*, *uniqueness* and *randomness*. A PUF is more reliable if it has less intra-chip variation. A PUF is more unique if the inter-chip variation is closer to 50%. A PUF is more random if its response bit is 0 or 1 with equal probability. Our statistical analysis shows that the intra-chip variation is less dependent on the number of stages, N, if N is greater than 10. However, the inter-chip variation is dependent on N if N is less than 100. It is shown that the feed-forward PUFs have higher intra-chip variation than MUX PUFs; however, the modified feed-forward PUFs have significantly lower intra-chip variation than the feed-forward PUFs. It is shown that the modified feed-forward cascade MUX PUF has the best uniqueness and randomness, while the MUX PUF has the best reliability. The analysis presented in this paper can be used by the designer to choose an appropriate PUF based on the application's requirement. This eliminates the need for fabrication and testing of many PUFs for selecting an appropriate PUF.**

***Index Terms*—Physical Unclonable Function, Multiplexer-based Structures, Statistical Analysis, Feed-Forward MUX PUF, Reliability, Randomness, Uniqueness, Intra-Chip Variation, Inter-Chip Variation.**

I. Introduction

Physical Unclonable Functions (PUFs) [1]–[3] are novel security primitives which store secret keys in physical objects by exploiting the uncontrollable randomness due to manufacturing process variations. PUFs generate signatures based on the unique intrinsic uncontrollable physical features, which can then be used for hardware authentication or the generation of secret keys. Contrary to standard digital systems, PUFs extract secrets from complex properties of a physical material rather than storing them in a non-volatile memory. Since the physical characteristics of the devices are practically unclonable, PUFs are almost impossible to clone, predict, or reproduce. Furthermore, an adversary cannot easily mount an attack to counterfeit the secret information without changing the physical randomness. Based on these advantages, PUFs can efficiently and reliably generate volatile secret keys for cryptographic operations and enable lightweight and cost-effective authentication of ICs.

The performance of a PUF depends on both process variation and environmental conditions. Designing a PUF that is close to truly random in nature and that can operate reliably over a wide range of operating conditions is still a challenge. Some metrics have been introduced to evaluate the performances of PUFs by analyzing the outputs of PUF instances. These considered metrics include *reliability*, *uniqueness*, and *randomness*. PUF *reliability* captures how efficient a PUF is in reproducing the response bits of an IC chip. When the same challenge is applied repetitively to a MUX-based PUF, the responses are expected to be identical. *Uniqueness* represents the ability of a PUF to uniquely distinguish a particular chip among a group of chips of the same type. When the same challenge sets are applied to different PUFs, the output responses are expected to be different. Ideally, the Hamming distances between the responses of different PUFs should be 50%. *Randomness* indicates the unbiasedness of the PUF response. However, these metrics need to be characterized over a large population of chips to validate the effectiveness of PUFs. This can involve a long and costly chip manufacturing process followed by many measurements after the circuits are fabricated. Furthermore, since the manufacturing process variation and the environmental variation are uncontrollable, it is hard to get a very accurate estimation of the performance during the design stage. *Security* is another performance metric of PUFs, which is not addressed in this paper. A PUF is more *secure*, if an adversary finds it harder to break in.

There seems little consensus about which PUF is more suitable for a specific application or a particular device in the existing literature. However, knowledge about the circuit-level behavior such as process variation pattern, variation of circuit parameters (delay, threshold voltage) over changing operating conditions could help designers to predict the performance comparisons among different PUF designs. Conducting the performance comparison among detailed PUF designs before fabrication would guarantee robust on-chip PUF performance. Monte-Carlo simulations of netlists that take process and environment variations into account can be used for this purpose. These simulations can provide approximate results, which can be used as indicators of the true performances of different PUFs. An alternate approach to evaluate the performance of the PUFs is by modeling the physical components of PUFs in a statistical manner. A number of such efforts have been developed in the literature. Statistical analysis on Coating PUF has been presented in [4]. In [5], entropy analysis of Optical PUF has been discussed. The statistical properties of Ring Oscillator PUF [6], [7] and MUX PUFs [8]–[10] have also been studied in the literature. Additionally, the work in [11] relates the statistical analysis of PUFs to circuit-level optimization and architecture-level optimization, which leads to interesting results that could improve the design and implementation of reliable and efficient PUFs.

The objective of this paper is to theoretically compare the

performances of different multiplexer-based PUFs to predict the relative advantages of various MUX-based PUF designs. The work presented in this paper differs from existing efforts in several respects. First, to the best of our knowledge, this paper, for the first time, presents a systematic statistical analysis of the performances of various MUX PUFs. These include the MUX PUF, feed-forward MUX PUFs, and multiplier-demultiplier (MUX/DeMUX) PUF. The focus of our work is on the comparison of performance of various MUX PUFs, which could help the designer to select an appropriate PUF during the design stage. Finally, the statistical analysis performed is very comprehensive which provides a deeper insight into the nature of various MUX-based PUFs. A number of equations about the PUF performances are derived; these equations allow the designer to calculate some of the metrics theoretically. In addition, we also introduce a class of *modified feed-forward MUX PUFs* obtained by modifying the standard feed-forward path. These structures are also analyzed statistically. It is shown that the modified feed-forward MUX PUFs have less intra-chip variations than standard feed-forward MUX PUFs.

The rest of the paper is organized as follows. In Section II, we introduce the background of MUX-based PUFs and their applications. In Section III, we propose several modified feed-forward MUX PUF structures with novel modified feed-foward paths. Section IV defines the metric indicators of PUF performance. Section V describes statistical modeling of the physical components in a MUX-based PUF, and then presents the statistical analysis results of the original MUX PUF. These results are also validated by comparing with experimental results. In Section VI, we analyze the statistical properties of feed-forward MUX PUFs and MUX/DeMUX PUF from the perspectives of the defined performance indicators. We summarize the performance comparisons of various MUX-based PUFs in Section VII. Section VIII validates the statistical analysis results by experimental results using SPICE simulations. Finally, Section IX concludes the paper.

II. Background

A. Silicon MUX PUF

There are several subtypes of PUFs, each with its own applications and security features. A major type is the so-called silicon PUFs, which exploit the delay variations of circuit components to generate a unique signature for each IC. Silicon PUFs can be integrated into chips very conveniently since these are implemented with standard digital logic and do not require any special fabrication. The examples of Silicon PUFs include: Multiplexer (MUX) PUF [12], Ring Oscillator PUF [2], SRAM PUF [13] and Butterfly PUF [14].

A MUX PUF is an example of a "Strong" PUF [15] that is unclonable due to manufacturing process variations, and can accommodate many possible challenge-response pairs (CRPs). For transistors, manufacturing randomness exists due to variations in transistor length, width, gate oxide thickness, doping concentration density, body bias, metal width, metal thickness, and ILD (inter-level dielectric) thickness, etc [16]. These manufacturing variations lead to a significant amount of variability for the MUX-based PUFs, which are sufficient to generate unique challenge-response pairs for each IC by comparing the delays of two paths. As illustrated in Figure 1, in a MUX PUF, each challenge creates two paths through the circuit that are excited simultaneously. The output is generated according to the delay difference between the two paths. A MUX PUF consists of N stages of MUXs and one arbiter which connects the final stage of the two paths. MUXs in each stage act as a switch to either cross or straight propagate the rising edge signals, based on the corresponding challenge bit. Each MUX should be designed equivalently, while variations will be introduced during manufacturing process. Finally, the arbiter translates the analog timing difference into a digital value. For instance, if the rising edge signal arrives at the top input of the arbiter earlier than the signal arriving at the bottom input, the output will be one; otherwise, if it reaches the bottom path first, the output will be zero. The output response depends on the applied challenge bits and will be permanent for each IC after fabrication or only vary in a small range due to environmental variations.

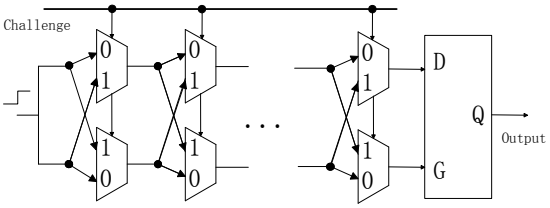

Fig. 1: Silicon MUX Physical Unclonable Function.

B. Feed-Forward MUX PUF

In order to improve the *security*, a feed-forward structure has been proposed in [17] to add non-linearity into the original MUX PUF. Figure 2 shows one basic structure of the feed-forward MUX PUF, which uses the *racing result of an intermediate stage* as the select signal for a later MUX stage. This structure increases the complexity of numerical modeling attacks [18]. However, the reliability of the PUF has been degraded since some select signals of the MUXs may also be affected by environmental variations.

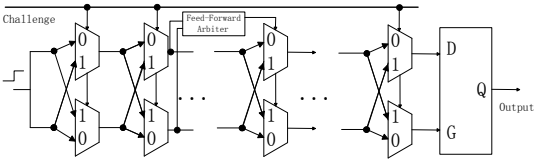

Fig. 2: Feed-Forward MUX PUF Structure.

C. MUX-based Reconfigurable PUFs

Based on the MUX PUF and its feed-forward variants, we have proposed several novel reconfigurable PUFs [19], [20], where the challenge-response pairs (CRPs) can be reconfigured. Reconfigurable PUFs satisfy the updatable key requirement for PUF-based authentication systems. Furthermore, reconfigurability improves the security against modeling attacks by limiting the amount of information leaked for each configuration. Such architectures are classified into two categories:

(a) *CRP-Reconfigurable PUF*: The challenge-response pairs are reconfigured directly by adding some additional

configure circuits into the structure, but without configuring the main PUF structure. This can be achieved by pre-processing the challenge before applying to the PUF or pre-processing the response before using it for authentication.

(b) *Logic-Reconfigurable PUF*: The underlying logic of the PUF circuit is reconfigured in these structures; therefore, the challenge-response pairs are reconfigured.

Logic-Reconfigurable PUFs have better performance from a security perspective, as reconfiguration leads to a different mathematical model of the PUF circuit, while the CRP-Reconfigurable PUFs only update the CRPs. The CRP-Reconfigurable PUFs are not studied in this paper. The examples of Logic-Reconfigurable PUFs include *Logic-Reconfigurable Feed-Forward MUX PUF*, and *Logic-Reconfigurable MUX/DeMUX PUF*.

1) Logic-Reconfigurable Feed-Forward MUX PUF: In a feed-forward MUX PUF, the output of a feed-forward arbiter from an intermediate stage is used as a challenge to a subsequent stage [18]. In [19], [20], we had introduced three different types of feed-forward MUX PUFs. These structures include *Feed-Forward Overlap (FFO)*, *Feed-Forward Cascade (FFC)*, and *Feed-Forward Separate (FFS)*. These structures are classified by the nature of interconnections of various feed-forward patterns in these PUFs. We also showned that the performance of a feed-forward MUX PUF depends on locations and the number of *feed-forward paths* (sometimes referred as *feed-forward loops* in the literature [18]). The three feed-forward structures are described below.

(a) *Feed-Forward Overlap (FFO)*: this structure has at least one stage overlap between two feed-forward paths as illustrated in Figure 3.

(b) *Feed-Forward Cascade (FFC)*: the ending stage of a feed-forward path will be the starting stage of another feed-forward path. This is illustrated in Figure 4.

(c) *Feed-Forward Separate (FFS)*: different feed-forward paths are separate; thus, no stage overlap exists between the two feed-forward paths. This is illustrated in Figure 5.

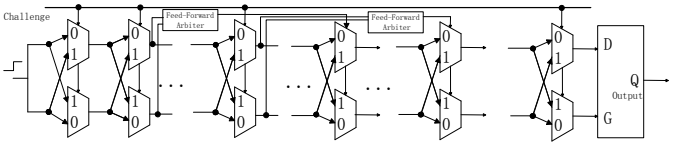

Fig. 3: Feed-Forward MUX PUF Overlap Structure.

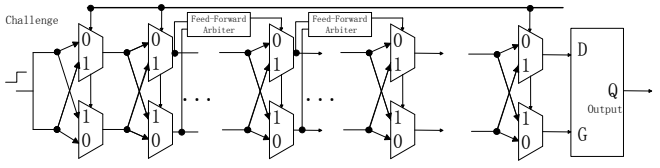

Fig. 4: Feed-Forward MUX PUF Cascade Structure.

We have simulated these three feed-forward structures and have shown that these structures satisfy different inter-chip and intra-chip characteristics [19], [20]. Based on this property, we have proposed a *Reconfigurable Feed-forward MUX PUF*, which can be configured to any of these three different structures (i.e., FFO, FFC, and FFS) [19], [20].

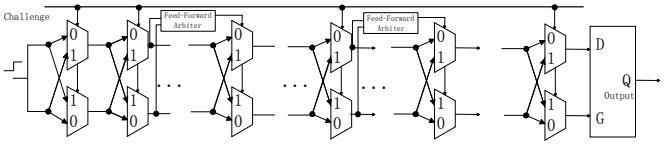

Fig. 5: Feed-Forward MUX PUF Separate Structure.

2) Logic-Reconfigurable MUX/DeMUX PUF: Another MUX-based Reconfigurable PUF is the *Reconfigurable MUX/DeMUX PUF*, which alters the PUF logic by using DeMUX. DeMUX enables the circuit to select the direction of the propagating signals, and makes the original MUX PUF reconfigurable.

A basic *Logic-Reconfigurable MUX/DeMUX PUF* structure is shown in Figure 6. Instead of propagating the rising edge signal successively, some stages can be skipped by the DeMUX, which allows the challenge-response behavior to be reconfigurable.

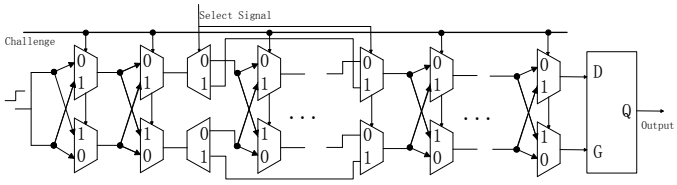

Fig. 6: Reconfigurable MUX/DeMUX PUF.

III. Modified Feed-Forward MUX PUFs

A. Modified Feed-Forward Path

In this paper, we propose a novel *modified feed-forward MUX PUF* structure shown in Figure 7. In this structure, the output of a feed-forward arbiter from an intermediate stage is input as the challenge bit to two consecutive late MUX stages. By employing this *modified feed-forward path*, the reliability of the feed-forward PUF structure can be improved, while the same level of security will be retained. This structure is analyzed statistically in this paper.

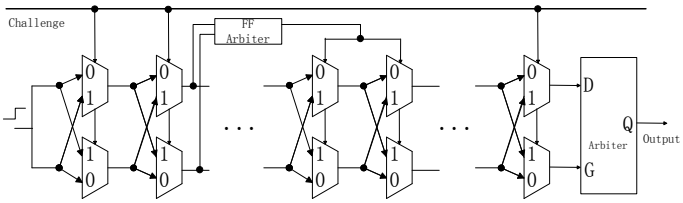

Fig. 7: Modified Feed-Forward MUX PUF Structure.

The complexity of the modified feed-forward MUX PUFs can be further improved by using several modified feed-forward paths in a PUF circuit. Note that if we want to maintain the length of challenge bits as N, we need to increase the number of MUX stages to $N+2M$ for the modified feed-forward structure, compared to $N+M$ of the standard feed-forward PUF. Besides, the design overhead will also include

M arbiters for both the standard feed-forward MUX PUF and the modified feed-forward MUX PUF.

B. Different Types of Modified Feed-Forward MUX PUFs

Similar to the three types of the standard feed-forward MUX PUFs as discussed in Section II.C, the modified feed-forward MUX PUFs can also be classified as *Modified Feed-Forward Overlap (MFFO)*, *Modified Feed-Forward Cascade (MFFC)*, and *Modified Feed-Forward Separate (MFFS)* as shown in Figure 8, Figure 9, and Figure 10, respectively.

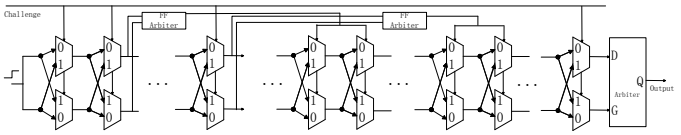

Fig. 8: Modified Feed-Forward MUX PUF Overlap Structure.

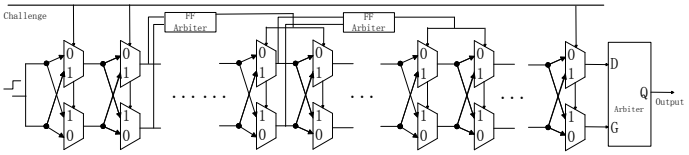

Fig. 9: Modified Feed-Forward MUX PUF Cascade Structure.

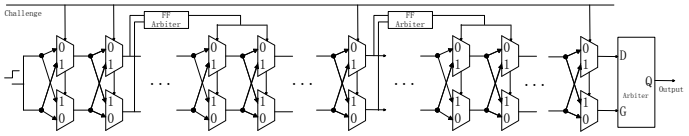

Fig. 10: Modified Feed-Forward MUX PUF Separate Structure.

These three different structures also have different inter-chip and intra-chip behaviors, which are analyzed in Section VI. Additionally, the modified feed-forward paths can also be used in the *Reconfigurable Feed-forward MUX PUF* to improve the reliability while retaining the high security.

IV. Definition of PUF Performance

As discussed in Section I, Monte-Carlo simulation can be used to provide performance indicators for different PUF designs. For example, by simulating the three feed-forward MUX PUF structures with the same parameter variations and environmental conditions, we were able to conclude in [19], [20] that the FFO structure is the most reliable among the three feed-forward structures. In this paper, we focus on analyzing the quantitative performance of various MUX-based PUFs through statistical modeling of the delay variations and environmental variations. Performance indicators ranging from 0 to 1 with 1 representing the best performance are generated through a theoretical analysis. The notations used in this paper are listed in Table I.

In this section, we introduce three PUF metrics to quantify the performance of MUX-based PUFs. The relative performance behaviors of the PUF structures are the main concern of this paper rather than the absolute value of each indicator.

A. Reliability

Intra-chip variation is a measure of the *reliability* of PUF, which is determined by comparing the digital signatures of the PUF to the same challenge under different environmental conditions.

Let P_{intra} represent the probability that a certain bit of a response will flip when applying a randomly selected challenge multiple times. Since all bits of a PUF response have equivalent statistical properties, P_{intra} can be used to represent the intra-chip variation for the entire L-bit response. In particular, the average Hamming distance (HD) between the responses is used to measure the intra-chip variations of MUX-based PUFs. The P_{intra} and the averaged HD are described by:

$$E(HD_{intra}) = P_{intra} = E\left(\frac{1}{m}\sum_{i=1}^{m}\frac{HD(R,R')}{L}\times 100\%\right), \tag{1}$$

where m is the number of HD comparisons, and R and R' represent two measurements of the PUF response under different conditions. The expected value of HD_{intra} is equal to P_{intra}. If the responses are sampled sufficient number of times, the averaged intra-chip variation would be close to the value of P_{intra}.

As smaller intra-chip variation means better reliability, the reliability indicator is defined as

$$Reliability = 1 - P_{intra}. \tag{2}$$

B. Uniqueness

Inter-chip variation is a measure of the uniqueness of PUF, which is determined by comparing the digital signature of a PUF to that of another. Similarly, we can also define P_{inter} as the probability that the bits generated by the same challenge for different PUF instances are different. Since uniqueness is a measure of inter-chip performance, all possible chip-combinations should be considered. Therefore, the average inter-chip HD of K PUFs can be described as:

$$\begin{aligned} &E(HD_{inter}) = P_{inter} \\ =&E\left(\frac{2}{(K-1)K}\sum_{i=1}^{K-1}\sum_{j=i+1}^{K}\frac{HD(R(i),R(j))}{L}\times 100\%\right). \end{aligned} \tag{3}$$

It can also be seen that P_{inter} represents the expected value of the inter-chip variation. We define uniqueness using Equation (4) as the inter-chip performance indicator.

$$Uniqueness = 1 - |2P_{inter} - 1|. \tag{4}$$

C. Randomness

A MUX-based PUF is expected ideally to produce unbiased 0's and 1's. Randomness represents the ability of the PUF to output 0 and 1 response with equal probability. One measurement of the randomness can be expressed as:

$$Randomness = 1 - |2P(R=1) - 1|. \tag{5}$$

Therefore, a randomness of 1 indicates unbiased PUF responses.

TABLE I: Notation Used in the Paper

Notation	Explanation
N	Number of MUX stages in a PUF instance
M	Number of feed-forward paths
L	Length of a response
C_i	Challenge bit of the i-th MUX stage
D_i^t	Delay of the top element of the i-th MUX stage
D_i^b	Delay of the bottom element of the i-th MUX stage
Δ_i	Delay difference between top and bottom elements of the i-th MUX stage
Δ_{Arb}	Skew effect of the arbiter
r_N	Delay difference of N stages
R	Response

V. Performance Analysis of the Original MUX PUF

A. Physical Component Modeling of MUX-based PUFs

As shown in Figure 1, a MUX PUF consists of a sequence of MUXs and an arbiter. The rising edge signal excites the two paths at the first stage simultaneously. The actual propagated paths are determined by the external challenge bits. After the last stage, the arbiter will generate the output bit by comparing the arrival time of the two paths at its input. It has become standard to model the MUX PUF via an additive linear delay model [8], [9]. According to the efforts in the field of statistical static timing analysis (SSTA) [16], the manufacturing process variations for the parameters of transistors can be modeled as Gaussian distributions. As a result, the variations of the delays will also be approximately Gaussian.

Process variations are classified as follows: inter-die variations are the variations from die to die, while intra-die variations correspond to variability within a single chip. Inter-die variations affect all devices on the same chip similarly, while intra-die variations affect different devices differently on the same chip. A very widely used model for delay spatial correlation is the "grid model" [16], which assumes perfect correlations among the devices in the same grid, high correlations among those in nearby grids, and low or zero correlations in faraway grids, since devices close to each other are more likely to have similar characteristics than those placed far away.

Additionally, experimental results in [12] have already shown that the inter-chip variation for MUX PUF across the wafers is similar to that within a single wafer, as the output of the arbiter in silicon MUX PUF is only based on the difference of two selected paths. Therefore, these die-to-die, wafer-to-wafer, and lot-to-lot manufacturing variations will have minimum effect on the output response.

Based on the facts discussed above, for simplicity, we can model the delay of each single MUX as an independent identically distributed (i.i.d.) random variable D_i, modeled by a Gaussian random variable $N(\mu, \sigma^2)$, where μ represents the mean and σ represents the standard deviation of the delay of each MUX. Therefore, the total delay of the N stages is modeled by $N(N\mu, N\sigma^2)$. The delay difference between top and bottom MUXs of the i-th stage will also follow a Gaussian distribution, and can be expressed as:

$$\Delta_i = D_i^t - D_i^b \sim N(0, 2\sigma^2). \tag{6}$$

For the original MUX PUF, the response is dependent on the delay difference of the two selected paths. The sign of the delay difference of each stage is determined by the external challenge bits. Consequently, the delay difference after the last stage can be modeled as

$$r_N = \sum_{i=1}^{N} (-1)^{C_i'} \Delta_i, \tag{7}$$

where $C_i' = \oplus_{j=i+1}^{N} C_j$ and $C_N' = 0$. The output bit is generated by

$$R = sign(r_N) = \begin{cases} 1, & r_N \geq 0 \\ 0, & r_N < 0 \end{cases}. \tag{8}$$

It can be seen that the original MUX PUF forms an additive linear model.

In a real PUF circuit, the arbiter would not be ideal. The skew effect of the arbiters also affects the performance of MUX-based PUFs by reducing the uniqueness, producing a biased response, and even degrading the security. If we assume that the threshold of the arbiter is Δ_{Arb}, the response is given by

$$R = sign(r_N) = \begin{cases} 1, & r_N \geq \Delta_{Arb} \\ 0, & r_N < \Delta_{Arb} \end{cases}, \tag{9}$$

since the arbiter is preset to 0 and requires a setup time constraint to switch to 1.

B. Probability Distribution of Output Delay Difference

Figure 11 shows a scatter plot of output samples from the simulations of 100-stage original MUX PUFs. Note that there are overlaps between the regions of output 1's and output 0's, which makes it difficult to estimate Δ_{Arb} accurately. This could be because the measured delay differences (measured for each path at the 50% point in the transition) and the actual delay differences that the arbiter operates at are different. Since the delay difference can be modeled by $N(0, 2N\sigma^2)$, we fit a Gaussian distribution to the delay differences, as shown in Figure 12. The standard deviation $\sqrt{2N\sigma^2}$ of the generated Gaussian distribution is 5.2936×10^{-11}. It can be seen that the skew effect of the arbiter leads to biased outputs with 32.8% 1's and 67.2% 0's.

Moreover, the average of the total delay of one path is $1.2667 \times 10^{-8}s$ in our simulation results. Therefore, the percent of delay deviation of 100 stages is about 0.4% (i.e., $\frac{5.2936 \times 10^{-11}}{1.2667 \times 10^{-8}s}$), which conforms with other published results of 65nm technology (e.g., [21]).

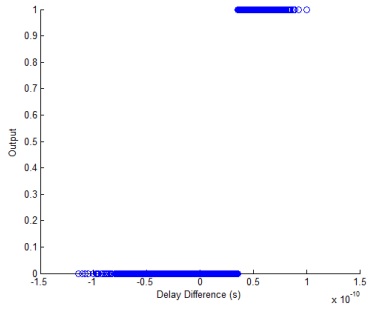

Fig. 11: Scatter Plot of Outputs.

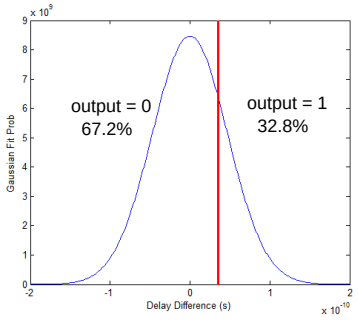

Fig. 12: Gaussian Fit Curve of Delay Difference Distribution.

C. Effect of Number of Stages

The probability that the output is equal to 1 can be derived as:

$$\begin{aligned} P(R=1) &= P(\sum_{i=1}^{N}(-1)^{C_i'}\Delta_i \geq \Delta_{Arb}) \\ &= \int_{\Delta_{Arb}}^{\infty} \frac{1}{\sqrt{2\pi N 2\sigma^2}} exp(\frac{-x^2}{2N2\sigma^2})dx \\ &= \frac{1}{2} - \frac{1}{2}erf(\frac{\Delta_{Arb}}{\sqrt{2N2\sigma^2}}). \end{aligned} \tag{10}$$

It can be seen that $P(R=1)$ is also dependent on the number of stages in a MUX PUF. If we only consider the number of stages N as a variable, the above equation can be rewritten as

$$P(R=1) = \frac{1}{2} - \frac{1}{2}erf(\frac{K}{\sqrt{N}}), \tag{11}$$

where K is a constant and is equal to $\frac{\Delta_{Arb}}{\sqrt{4\sigma^2}}$. Thus, although the value of Δ_{Arb} is unclear, we can still estimate the K based on the experimental results:

$$K = \sqrt{N} \times erfinv(1 - 2P(R=1)). \tag{12}$$

In our simulations, the 50-stage MUX PUF structure is only able to generate 1's with probability 25.6%, which is very close to the value of $P(R=1) = 26.4\%$ that is calculated theoretically from Equation (11).

D. Statistical Properties of the Original MUX PUF

1) Reliability: In order to analyze the reliability, we need to consider the effect of environmental noise. As a usual practice, we assume that the noise n_i of the i-th stage follows a zero-mean Gaussian distribution with variance σ_n^2. Then, P_{intra} can be described as:

$$\begin{aligned} P_{intra} =& P[sign(\sum_{i=1}^{N}(-1)^{C_i'}\Delta_i + \sum_{i=1}^{N} n_i) \\ & \neq sign(\sum_{i=1}^{N}(-1)^{C_i'}\Delta_i + \sum_{i=1}^{N} n_i')], \end{aligned} \tag{13}$$

where n_i and n_i' represent the noise under different environmental conditions. As each individual stage follows the zero-mean i.i.d. Gaussian distribution, then the intra-chip variation probability is equivalent to a single stage intra-chip variation probability:

$$P_{intra} = P[sign(s_i + n_i) \neq sign(s_i + n_i')] \tag{14}$$

where $s_i = (-1)^{C_i}(D_i^t - D_i^b)$ has a variance that is equal to $2\sigma^2$.

As manufacturing process variation and environmental noise of the delay difference both follow zero-mean Gaussian distribution, their probability density functions (PDF) are given by:

$$f_s(s) = \frac{1}{\sqrt{2\pi\sigma_s^2}} exp(-\frac{s^2}{2\sigma_s^2}), f_n(n) = \frac{1}{\sqrt{2\pi\sigma_n^2}} exp(-\frac{n^2}{2\sigma_n^2}). \tag{15}$$

Note that $\sigma_s^2 = 2\sigma^2$ in Equation (6). P_{intra} of an original MUX PUF can be calculated as

$$\begin{aligned} P_{intra} =& P[sign(s_i + n_i) \neq sign(s_i + n_i')] \\ =& 4\int_0^{\infty} \frac{1}{\sqrt{2\pi\sigma_s^2}} exp(-\frac{s^2}{2\sigma_s^2}) \int_{-\infty}^{-s} \frac{1}{\sqrt{2\pi\sigma_n^2}} exp(-\frac{n^2}{2\sigma_n^2}) dn \\ & \int_{-s}^{\infty} \frac{1}{\sqrt{2\pi\sigma_n^2}} exp(-\frac{n'^2}{2\sigma_n^2}) dn' ds \\ =& 4\int_0^{\infty} \frac{1}{\sqrt{2\pi\sigma_s^2}} exp(-\frac{s^2}{2\sigma_s^2})(\frac{1}{4} - \frac{1}{4}erf^2(\frac{s}{\sqrt{2\sigma_n^2}})) ds \\ =& \int_0^{\infty} \frac{1}{\sqrt{2\pi\sigma_s^2}} exp(-\frac{s^2}{2\sigma_s^2}) ds - \\ & \int_0^{\infty} \frac{1}{\sqrt{2\pi\sigma_s^2}} exp(-\frac{s^2}{2\sigma_s^2}) erf^2(\frac{s}{\sqrt{2\sigma_n^2}}) ds \\ =& \frac{1}{2} - \frac{1}{\pi} arctan(\sqrt{\frac{\sigma_s^4}{2\sigma_s^2\sigma_n^2 + \sigma_n^4}}), \end{aligned} \tag{16}$$

where the first of the two integrals in the fourth line represents integrating just a Gaussian over half of the space, and the second is a known definite integral [22].

It can be seen that by increasing the ratio of manufacturing process variation to environmental variation, the intra-chip variation can be reduced to close to 0.

If we consider the P_{intra} of the PUF response with a given challenge, the conditional probability can be derived as

$$P[sign(s_i + n_i) \neq sign(s_i + n_i')|s_i] = \frac{1}{2} - \frac{1}{2}erf^2(\frac{|s_i|}{\sqrt{2\sigma_n^2}}). \tag{17}$$

The reliability for a certain challenge-response pair is greatly dependent on the manufacturing process variation between the two generated paths. If a challenge selects two paths with $r_N \approx 0$, the variation is large, since the above equation achieves maximum at $s_i = 0$. Otherwise, if $|r_N|$ is relatively large, the manufacturing process variation would be the prima-

ry factor to determine the output and the noise would hardly flip the response.

However, if we take the skew effect of non-ideal arbiters into consideration, the intra-chip variation behaviors would also be dependent on the number of stages and the performance of the arbiter. The response then can be described as $sign(\sum_{i=1}^{N}(s_i+n_i)-\Delta_{Arb})$. Therefore, P_{intra} is given by

$$P[sign(\sum_{i=1}^{N}(s_i+n_i)-\Delta_{Arb}) \neq sign(\sum_{i=1}^{N}(s_i+n_i')-\Delta_{Arb})]. \tag{18}$$

If we combine $\sum_{i=1}^{N} s_i$ and Δ_{Arb} as a variable $X \sim (\Delta_{Arb}, N\sigma_s^2)$, P_{intra} can be expressed as $P[sign(x+n) \neq sign(x+n')]$, where $x \sim N(-\frac{\Delta_{Arb}}{\sqrt{N}}, \sigma_s^2)$ and $n \sim N(0, \sigma_n^2)$. Therefore, according to Equation (18), the intra-chip variation probability decreases with the increase of Δ_{Arb}. Intuitively we would expect this as when Δ_{Arb} is relatively large and the number of stages is small, $\sum_{i=1}^{N}(s_i+n_i)$ will have a high probability of unaltered $sign()$ value. However, if the number of stages is relatively large that $\frac{\Delta_{Arb}}{\sqrt{N}}$ approaches to 0, P_{intra} will be reduced to Equation (16).

A closed-from expression for P_{intra} (i.e., Equation (18)) does not exist, but we can derive the expression by using a first-order approximation of the exponential function:

$$\begin{aligned}
&P[sign(\sum_{i=1}^{N}(s_i+n_i)-\Delta_{Arb}) \neq sign(\sum_{i=1}^{N}(s_i+n_i')-\Delta_{Arb})] \\
=&2\int_{-\infty}^{\infty}\frac{1}{\sqrt{2\pi\sigma_s^2}}exp(-\frac{s^2}{2\sigma_s^2})(\frac{1}{4}-\frac{1}{4}erf^2(\frac{|s-\frac{\Delta_{arb}}{\sqrt{N}}|}{\sqrt{2\sigma_n^2}}))ds \\
=&2\int_{-\infty}^{\infty}\frac{1}{\sqrt{2\pi\sigma_s^2}}exp(-\frac{(x+\frac{\Delta_{arb}}{\sqrt{N}})^2}{2\sigma_s^2})(\frac{1}{4}-\frac{1}{4}erf^2(\frac{|x|}{\sqrt{2\sigma_n^2}}))dx \\
\approx&2\int_{-\infty}^{\infty}\frac{1}{\sqrt{2\pi\sigma_s^2}}exp(-\frac{x^2}{2\sigma_s^2})(1-\frac{\Delta_{Arb}}{\sigma_s^2\sqrt{N}}x) \\
&(\frac{1}{4}-\frac{1}{4}erf^2(\frac{|x|}{\sqrt{2\sigma_n^2}}))dx \\
=&\frac{1}{2}-\frac{1}{\pi}arctan(\sqrt{\frac{\sigma_s^4}{2\sigma_s^2\sigma_n^2+\sigma_n^4}})- \\
&4\frac{\Delta_{Arb}}{\sigma_s^2\sqrt{N}}\int_0^{\infty}\frac{1}{\sqrt{2\pi\sigma_s^2}}xexp(-\frac{x^2}{2\sigma_s^2})(\frac{1}{4}-\frac{1}{4}erf^2(\frac{x}{\sqrt{2\sigma_n^2}}))dx \\
=&\frac{1}{2}-\frac{1}{\pi}arctan(\sqrt{\frac{\sigma_s^4}{2\sigma_s^2\sigma_n^2+\sigma_n^4}})- \\
&\frac{\Delta_{Arb}}{\sqrt{2\pi N\sigma_s^2}}(1-\frac{2}{\pi}\sqrt{\frac{\sigma_s^2}{\sigma_s^2+\sigma_n^2}}arctan(\sqrt{\frac{\sigma_s^2}{\sigma_s^2+\sigma_n^2}}))
\end{aligned} \tag{19}$$

It can be seen that P_{intra} increases with the number of stages, since $\frac{2}{\pi}\sqrt{\frac{\sigma_s^2}{\sigma_s^2+\sigma_n^2}}arctan(\sqrt{\frac{\sigma_s^2}{\sigma_s^2+\sigma_n^2}})$ is less than 1. Additionally, the term of $\sqrt{\frac{\sigma_s^2}{\sigma_s^2+\sigma_n^2}}$ is close to 1, while the ratio of $\frac{sigma_s}{sigma_n}$ is relatively large. As a result, $(1-\frac{2}{\pi}\sqrt{\frac{\sigma_s^2}{\sigma_s^2+\sigma_n^2}}arctan(\sqrt{\frac{\sigma_s^2}{\sigma_s^2+\sigma_n^2}}))$ will be close to 0. Therefore, in this case, the number of the stages only has a minor influence on the intra-chip variation of the original MUX PUF.

Conclusion 1: The reliability indicator of a original MUX PUF is

$$\begin{aligned}
Reliability =&1-P_{intra}=\frac{1}{2}+\frac{1}{\pi}arctan(\sqrt{\frac{\sigma_s^4}{2\sigma_s^2\sigma_n^2+\sigma_n^4}}) \\
&+\frac{\Delta_{Arb}}{\sqrt{2\pi N\sigma_s^2}}(1-\frac{2}{\pi}\sqrt{\frac{\sigma_s^2}{\sigma_s^2+\sigma_n^2}}arctan(\sqrt{\frac{\sigma_s^2}{\sigma_s^2+\sigma_n^2}}))
\end{aligned} \tag{20}$$

where σ_s is the standard deviation of manufacturing process variation for a single stage, σ_n is the standard deviation of environmental noise, Δ_{Arb} is the skew effect of the arbiter, and N is the number of stages in a original MUX PUF. ■

2) Uniqueness: In order to compute inter-chip variation based on the same mathematical model, we need to compare the responses of different PUFs. The Gaussian fit curve for the inter-chip variations of the 100-stage MUX PUF is shown in Figure 13. The average of the inter-chip variation is 43.2%.

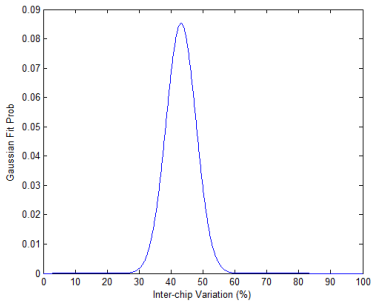

Fig. 13: Gaussian Fit Curve of Inter-Chip Variation Distribution.

Theoretically, if the PUFs are uncorrelated, the expected inter-chip variation of the original MUX PUF is simply given by

$$\begin{aligned}
P_{inter} &= 2P(R=1)(1-P(R=1)) \\
&= \frac{1}{2}-\frac{1}{2}erf^2(\frac{K}{\sqrt{N}}),
\end{aligned} \tag{21}$$

where $K=\frac{\Delta_{Arb}}{\sqrt{4\sigma^2}}=\frac{\Delta_{Arb}}{\sqrt{2\sigma_s^2}}$. Therefore, the value of uniqueness indicator can be expressed as

$$\begin{aligned}
Uniqueness =&1-|2P_{inter}-1| = 4P(R=1)(1-P(R=1)) \\
=&1-erf^2(\frac{\Delta_{Arb}}{\sqrt{2N\sigma_s^2}}).
\end{aligned} \tag{22}$$

According to the value of $P(R=1)$, we could expect the average of the inter-chip variation to be $2\times 0.328\times(1-0.328)=44\%$, which is also consistent with our experimental results.

3) Randomness: Similarly, the randomness of a original MUX PUF is

$$Randomness = 1-|2P(R=1)-1| = 1-erf(\frac{\Delta_{Arb}}{\sqrt{2N\sigma_s^2}}). \tag{23}$$

E. Design Example

The above equations are useful for designing a PUF that could meet the specific application requirement. Consider the scenario that the PUF designer has fabricated a PUF and tested

its performance. However, the designer found the performance of the current PUF cannot satisfy the application requirement. Instead of fabricating a large number of different PUF designs, the designer could utilize the statistical analysis results to predict the performances of PUF designs theoretically, since some of the parameters can be calculated from the results of the current PUF. For example, if we fabricate a 100-stage original MUX PUF which has the performance similar to our experimental results, we can calculate the value of K in Equation (12) based on the performance of the 100-stage MUX PUF. We can then substitute different values of N to predict the performances of the original MUX PUFs for different numbers of stages. For the intra-chip variation, we can obtain the relations among σ_s, σ_n, and Δ_{Arb} by utilizing Equations (19) and (23) together. The various performance results for different values of N are calculated theoretically and are summarized in Table II (the bold line indicates the results obtained from the current measured or simulated PUF).

Therefore, the statistical analysis can be used to decide how many MUX stages should be used to design the PUF to match the application requirements. Note that the values may not be exact, but we can obtain the trends of the performance metrics from the statistical analysis results. These results show that inter-chip variation is strongly dependent on N for $N < 100$, while intra-chip variation is almost independent of N, for $N > 25$.

VI. Performance Analysis of Feed-Forward MUX PUFs and MUX/DeMUX PUF

A. Statistical Properties of Feed-Forward MUX PUF

1) Reliability: As shown in Figure 2, some of the challenge bits of a feed-forward MUX PUF will be the intermediate stage arbiter outputs instead of the external bits in a feed-forward MUX PUF. For instance, if there is only one feed-forward path in a MUX PUF, which is from the a-th stage to the b-th stage, the time difference of the b-th stage could be expressed as:

$$\Delta_b = (-1)^{sign(r_a)}(D_b^t - D_b^b). \tag{24}$$

It can be expected intuitively that the intra-chip variation will be greatly dependent on the location of the ending stage of the feed-forward path. If the challenge of the last stage flips, the output bit will be $sign(-\sum_{i=1}^{N-1}(-1)^{C_i'}\Delta_i + \Delta_N)$ compared to $sign(\sum_{i=1}^{N-1}(-1)^{C_i'}\Delta_i + \Delta_N)$ while there is no error. We can also illustrate this characteristic of the feed-forward PUF mathematically. As an example, if the challenge of the k-th stage flips in an N-stage structure, the probability that the output bit will change, P_e, is given by (without considering noise):

$$\begin{aligned}
P_e =& P[sign(\sum_{i=1}^{k-1}(-1)^{C_i'}\Delta_i + \sum_{i=k}^{N}(-1)^{C_i'}\Delta_i) \\
&\neq sign(-\sum_{i=1}^{k-1}(-1)^{C_i'}\Delta_i + \sum_{i=k}^{N}(-1)^{C_i'}\Delta_i)] \\
=& 2\int_0^{\infty}\frac{1}{\sqrt{2\pi(N-k+1)\sigma_s^2}}exp(-\frac{s^2}{2(N-k+1)\sigma_s^2}) \\
&(1-\int_{-s}^{s}\frac{1}{\sqrt{2\pi(k-1)\sigma_s^2}}exp(-\frac{w^2}{2(k-1)\sigma_s^2}))dwds \\
=& 2\int_0^{\infty}\frac{1}{\sqrt{2\pi(N-k+1)\sigma_s^2}}exp(-\frac{s^2}{2(N-k+1)\sigma_s^2}) \\
&(1-erf(\frac{s}{\sqrt{2\pi(k-1)\sigma_s^2}}))ds \\
=& 1-\frac{2}{\pi}arctan(\sqrt{\frac{N-k+1}{k-1}}) \\
=& \frac{2}{\pi}arctan(\sqrt{\frac{k-1}{N-k+1}})
\end{aligned} \tag{25}$$

where the second integral in the third line is also a known definite integral in [22].

It can be seen that the probability P_e increases with k. Obviously, the problem for this structure is that if the ending stage of a feed-forward path is close to the last stage, the reliability of the PUF will be degraded significantly. If $k = N$, i.e., the ending stage of the feed-forward path is the last stage, P_e will be $\frac{2}{\pi}arctan(\sqrt{N-1})$, which is close to 1.

Therefore, P_{intra} of this feed-forward MUX PUF with single feed-forward path can be described as

$$(1-P_1)P_1 + P_1\frac{2}{\pi}arctan(\sqrt{\frac{k-1}{N-k+1}}). \tag{26}$$

There could be several feed-forward paths in one PUF design. In these PUFs, if the ending stage of a feed-forward path is close to the last stage, the reliability of the PUF will be degraded significantly.

B. Statistical Properties of Modified Feed-Forward MUX PUF

Motivated by this analysis, we propose the *modified feed-forward MUX PUF* structure shown in Figure 7, which is presented in Section III. The modified feed-forward path mitigates the effect of the locations of feed-forward paths. In this structure, the modified feed-forward path only affects the delay difference of one stage. For example, if the two consecutive ending stages of a feed-forward path are the k-th and $(k+1)$-th stages respectively, we can derive C' for the *modified feed-forward MUX PUF* as follows:

$$C'_{k-1} = \oplus_{j=k+2}^{N}C_j \oplus C_k \oplus C_{k+1}, \tag{27}$$

$$C'_k = \oplus_{j=k+2}^{N}C_j \oplus C_{k+1}, \tag{28}$$

$$C'_{k+1} = \oplus_{j=k+2}^{N}C_j. \tag{29}$$

Since $C_k = C_{k+1}$ in this structure, the modified feed-forward path will only affect the value of C'_k.

As a result, by employing this modified feed-forward path, only one stage will be affected by each feed-forward arbiter.

TABLE II: MUX PUF Performance Prediction based on Statistical Analysis

N	Intra-chip Variation	Reliability	Inter-chip Variation	Uniqueness	$P(R=1)$	Randomness
25	5.3%	94.7%	30.3%	60.7%	18.7%	37.3%
50	5.6%	94.4%	38.9%	77.8%	26.4%	52.9%
75	5.7%	94.3%	42.3%	84.6%	30.4%	60.7%
100	**5.8%**	**94.2%**	**44.1%**	**88.2%**	**32.8%**	**65.6%**
150	5.9%	94.1%	46.0%	91.9%	35.8%	71.6%
200	5.9%	94.1%	46.9%	93.9%	37.7%	75.3%

Thus, this structure will have lower intra-chip variation, compared to the standard feed-forward MUX PUF. However, the nonlinearity of mathematical models for the modified feed-forward MUX PUF and the standard feed-forward MUX PUF are similar, except the challenge mapping C_i'. Therefore, we can conclude that one benefit of using the proposed modified feed-forward path is that the reliability of the feed-forward MUX PUF can be improved. Furthermore, the modified feed-forward path can lead to higher security, as the degree of nonlinearity can be increased without significant increase of intra-chip variation.

The designer can predict the performances of different implementations of the feed-forward MUX PUFs based on above statistical analysis results. For example, we consider the 100-stage feed-forward MUX PUFs with one feed-forward path (assuming that the feed-forward path starts from the output of the 20th stage, and the ends at the k-th stage). If error occurs in the feed-forward path, the probabilities that the output bit will change P_e and the intra-chip variation probabilities, P_{intra}, are summarized in Table III (P_1 is equal to 5.8% in our experimental results). Note that the probabilities of errors in the feed-forward paths are the same for all the feed-forward MUX PUFs with single feed-forward path, since there is no feed-forward path in previous stages.

It can be seen that the modified feed-forward path can reduce the intra-chip variation of the feed-forward MUX PUF. Compared to the original MUX PUF, the intra-chip variation of the modified feed-forward MUX PUF with single feed-forward path is only increased very slightly. Based on Table III, it can also be concluded that if the designer want to design a standard feed-forward MUX PUF, the designer could adjust the locations of the feed-forward paths according to the particular design performance requirement.

1) Reliability: In this structure, the delay difference of the ending stage of the first feed-forward path (from stage *a* to stage *b*) will be $(-1)^{C'_{b+1}}(D_b^t - D_b^b)$ with probability $1-P_1$, and will be $-(-1)^{C'_{b+1}}(D_b^t - D_b^b)$ with probability P_1. We define the *stage variation probability* as the probability that the sign of the delay difference for each stage changes from positive to negative or *vice versa*. Note that the stage variation probability is a good indicator of the effect of the noise at each MUX stage. The greater the stage variation probability, the less reliable the response. It is obvious that for the MUX PUF, the stage variation probability for each stage is equal to the intra-chip variation probability $P_{intra} = P_1$. For the modified feed-forward structure, the stage variation probability for the stage whose select signal is from the first feed-forward arbiter can be calculated as

$$\begin{aligned}&P[sign(s_i+n_i)sign(s_b+n_b) \neq sign(s_i+n_i')sign(s_b+n_b')]\\ =&2(1-P_1)P_1 = \frac{1}{2} - \frac{2}{\pi^2}arctan^2(\sqrt{\frac{\sigma_s^4}{2\sigma_s^2\sigma_n^2+\sigma_n^4}}).\end{aligned} \tag{30}$$

Note that, for simplicity, the following analysis on reliability will focus on the case without considering the skew effect of arbiters (i.e., Equation (16) instead of Equation (19)), as the number of stages and the skew effect do not have a significant impact on intra-chip variation are described in Section V. Since $arctan(\sqrt{\frac{\sigma_s^4}{2\sigma_s^2\sigma_n^2+\sigma_n^4}}) \leq \frac{\pi}{2}$, we can conclude that

$$\begin{aligned}&\frac{1}{2} - \frac{2}{\pi^2}arctan^2(\sqrt{\frac{\sigma_s^4}{2\sigma_s^2\sigma_n^2+\sigma_n^4}})\\ =&\frac{1}{2} - \frac{2}{\pi}arctan(\sqrt{\frac{\sigma_s^4}{2\sigma_s^2\sigma_n^2+\sigma_n^4}})\frac{1}{\pi}arctan(\sqrt{\frac{\sigma_s^4}{2\sigma_s^2\sigma_n^2+\sigma_n^4}})\\ \geq&\frac{1}{2} - \frac{1}{\pi}arctan(\sqrt{\frac{\sigma_s^4}{2\sigma_s^2\sigma_n^2+\sigma_n^4}}).\end{aligned} \tag{31}$$

Therefore, it can be concluded that the stage variation probability is increased by introducing feed-forward arbiters. This is similar to the scenario where the environmental noise can cause large variations of the time difference to the ending stages of feed-forward paths. The intra-chip variation probability of a feed-forward MUX PUF can be expressed as

$$P_{intra} = \frac{1}{2} - \frac{1}{\pi}arctan(\sqrt{\frac{\sigma_s^4}{2\sigma_s^2\tilde{\sigma}^2+\tilde{\sigma}^4}}), \tag{32}$$

where $\tilde{\sigma}^2 = \sigma_n^2 + \frac{1}{N}\sum_{k=1}^{M}\sigma_k'^2$, and M is the number of feed-forward paths and σ_k' is the additional deviation introduced by the feed-forward paths. The value of σ_k' for each feed-forward path is different, which is dependent on the noise in previous stages. Therefore, unlike the original MUX PUF, the feed-forward MUX PUF structure has large number of variants. The differences in both the number and the locations of the feed-forward paths result in different mathematical models, which will lead to different values of P_{intra}.

Conclusion 2: Although a general expression cannot be derived for P_{intra} of the modified feed-forward MUX PUF, we can still conclude from Equation (32) and Table III that

$$\begin{aligned}&P_{intra}(\text{feed-forward MUX PUF})\\ >&P_{intra}(\text{modified feed-forward MUX PUF})\\ >&P_{intra}(\text{original MUX PUF}).\end{aligned} \tag{33}$$

Thus, the modified feed-forward MUX PUF has lower value of the reliability indicator than the original MUX PUF, since $Reliability = 1 - P_{intra}$. If we take skew effect of the

TABLE III: Performances of Different Feed-Forward MUX PUFs

	Standard Feed-Forward MUX PUF			Modified Feed-Forward MUX PUF		
k	50	70	90	50	70	90
P_e	49.4%	62.4%	78.5%	6.4%	6.4%	6.4%
P_{intra}	8.33%	9.09%	10.02%	5.83%	5.83%	5.83%

arbiter into consideration, the same conclusion above can also be reached, since the feed-forward PUF has larger stage variations (assuming all other parameters to be the same). ■

2) Uniqueness: If we still assume that the arbiters are ideal, the inter-chip variation will not be affected by the modified feed-forward paths. The delay differences of the ending stages of feed-forward paths still follow a zero-mean Gaussian distribution. Thus, the mean of total time difference of the two generated paths is 0. Since the manufacturing process variations are uncorrelated for different PUFs, P_{inter} will remain 50% for the modified feed-forward MUX PUFs.

However, if we consider the skew effect of arbiters, the inter-chip variation behaviors would be different for the original MUX PUFs and the feed-forward MUX PUFs. We consider the Gaussian random variable Y that follows the distribution $N(0, N\sigma_s^2+\sum_{i=1}^{N}\sigma_{n_i}^2)$. Without loss of generality, we assume $\Delta_{Arb} \geq 0$. Thus, the probability that the PUF output is 1 is given by:

$$P(R=1) = P(Y > \Delta_{Arb}) = \frac{1}{2} - \frac{1}{2} erf\left(\frac{\Delta_{Arb}}{\sqrt{2N\sigma_s^2 + 2\sum_{i=1}^{N}\sigma_{n_i}^2}}\right). \tag{34}$$

If we consider two variables Y and Y', where Y' has larger stage variations (i.e., larger $\sum_{i=1}^{N}\sigma_{n_i}^2$), we can obtain the relation that $P(Y > \Delta_{Arb}) < P(Y' > \Delta_{Arb}) < \frac{1}{2}$ from Equation (34). In this case, P_{inter} for the two different PUFs are $2P(Y > \Delta_{Arb})(1 - P(Y > \Delta_{Arb}))$ and $2P(Y' > \Delta_{Arb})(1 - P(Y' > \Delta_{Arb}))$, respectively. We can show that

$$\begin{aligned} &2P(Y > \Delta_{Arb})(1 - P(Y > \Delta_{Arb})) \\ &- 2P(Y' > \Delta_{Arb})(1 - P(Y' > \Delta_{Arb})) \\ =&2(P(Y > \Delta_{Arb}) - P(Y' > \Delta_{Arb})) \\ &(1 - P(Y > \Delta_{Arb}) - P(Y' > \Delta_{Arb})) \\ <&0. \end{aligned} \tag{35}$$

Thus we conclude that the PUF structure with larger stage variations has a larger inter-chip variation. In particular, we can conclude that the modified feed-forward MUX PUF has a greater inter-chip variation probability P_{inter} than the original MUX PUF, since the stage variation probability for a modified feed-forward MUX PUF is larger.

Conclusion 3: The values of P_{intra} and P_{inter} of a modified feed-forward MUX PUF are both greater than those of the original MUX PUF. Therefore, it can be concluded that the feed-forward MUX PUF has higher uniqueness than the original MUX PUF, as P_{inter} of the modified feed-forward MUX PUF is closer to $\frac{1}{2}$. ■

3) Randomness: If we still consider the variable Y, we can get $P(R=1) = P(Y > \Delta_{Arb})$ while taking the skew effect of the arbiters into consideration. Since $P(Y > \Delta_{Arb}) < \frac{1}{2}$, we can obtain the expression for the randomness as

$$Randomness = 1 - |2P(R=1) - 1| = 2P(Y > \Delta_{Arb}). \tag{36}$$

Therefore, we can also conclude that the modified feed-forward MUX PUF has better randomness than the original MUX PUF, as the value of $P(Y > \Delta_{Arb})$ for the modified feed-forward MUX PUF is greater.

C. Statistical Properties of Different Types of Modified Feed-forward MUX PUFs

As discussed in Section III.B, modified feed-forward MUX PUFs can be classified into three different structures, which have different inter-chip and intra-chip characteristics. We examine the relations of these structures statistically in this subsection.

1) Reliability: From Conclusion 2, the stage variation probability of the ending stage of the first modified feed-forward path is given by

$$P_2 = (1 - P_1)P_1 + P_1(1 - P_1) > P_1. \tag{37}$$

Similarly, the stage variation probability of the ending stage of the second modified feed-forward path can be written as

$$P_3 = (1 - P_2)P_1 + P_2(1 - P_1). \tag{38}$$

Generally speaking, if we have the stage variation probability for the ending stages of the first m modified feed-forward paths and $P_1 < P_2 < ... < P_m$, then the stage variation probability for the ending stage of the $(m+1)$-th modified feed-forward path is given by

$$P_{m+1} = (1 - P_m)P_1 + (1 - P_1)P_m > P_m. \tag{39}$$

This can be proved as follows:

$$\begin{aligned} P_{m+1} - P_m =&(1 - P_m)P_1 + (1 - P_1)P_m \\ &- (1 - P_{m-1})P_1 - (1 - P_1)P_{m-1} \\ =&(P_{m-1} - P_m)P_1 + (1 - P_1)(P_m - P_{m-1}) \\ =&(P_m - P_{m-1})(1 - 2P_1). \end{aligned} \tag{40}$$

As we have already shown that $P_1 < \frac{1}{2}$ and we have $P_m > P_{m-1}$, therefore, we can conclude that $P_{m+1} > P_m$.

Conclusion 4: In a modified feed-forward MUX PUF structure, the stage variation probability of the ending stage of a modified feed-forward path is greater than the stage variation probabilities of the ending stages of previous modified feed-forward paths. ■

It can be expected that the stage variation probability of a modified feed-forward overlap structure is less than the separate or cascade structure, since there is no feed-forward arbiter in previous path for any of the modified feed-forward paths in the overlap structure. We can show this property by combining the feed-forward paths and other stages together.

The stage variation probability of the first feed-forward arbiter is equal to P_1, since there is no feed-forward path involved. Then, the stage variation probability of the second feed-forward arbiter is given by (assuming there are K_2 stages before the second feed-forward path and the b-th stage is the ending stage of the first feed-forward path):

$$\begin{aligned} P_2 =& P[sign(\sum_{i=1,i\neq b}^{K_2} s_i + s_b + \sum_{i=1}^{K_2} n_i) \\ & \neq sign(\sum_{i=1,i\neq b}^{K_2} s_i + x_b + \sum_{i=1}^{K_2} n_i')] \end{aligned} \tag{41}$$

where $x_b = s_b$, with probability $1 - P_1$, and $x_b = -s_b$, with probability P_1.

In the expression above, we have $\sum_{i=1,i\neq b}^{K_2} s_i \sim N(0,(K_2-1)\sigma_s^2)$, $s_b \sim N(0,\sigma_s^2)$ and $\sum_{i=1}^{K_2} n_i \sim N(0,K_2\sigma_n^2)$. This involves triple integrals over Gaussian distributions and does not have a closed-form expression. Therefore, we use Monte-Carlo simulation method to examine the performance. Figure 14 shows the stage variation probabilities of the second feed-forward arbiter for different K_2.

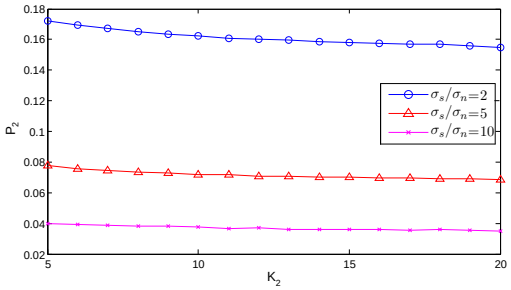

Fig. 14: Stage Variation Probability of the Ending Stage of the Second Feed-Forward Arbiter.

It can be observed from Figure 14 that the stage variation probability is decreased with the increase of K_2, since the error in feed-forward path is more likely to be averaged out by more stages. For the third feed-forward arbiter, the stage variation probability is

$$\begin{aligned} P_3 =& P[sign(\sum_{i=1,i\neq b,d}^{K_3} s_i + s_b + s_d + \sum_{i=1}^{K_3} n_i) \\ & \neq sign(\sum_{i=1,i\neq b,d}^{K_3} s_i + x_b + x_d + \sum_{i=1}^{K_3} n_i')] \end{aligned} \tag{42}$$

where $x_b = s_b$, with probability $1 - P_1$, and $x_b = -s_b$, with probability P_1; $x_d = s_d$, with probability $1 - P_2$, and $x_d = -s_d$, with probability P_2. We can find that P_3 also decreases with K_3.

In the modified feed-forward separate structure, K_i is greater than the corresponding K_i in the cascade structure. Therefore, the stage variations of the ending stages of feed-forward paths in the cascade structure are larger. Furthermore, large stage variation probability in previous path is more likely to lead to a large stage variation probability of the following feed-forward arbiters. As a result, we can conclude that the modified feed-forward separate structure is more reliable than the modified feed-forward cascade structure.

Conclusion 5: Based on the stage variation properties, we conclude that P_{intra} of the three structures satisfy

$$P_{intra}(MFFO) < P_{intra}(MFFS) < P_{intra}(MFFC). \tag{43}$$

The MFFO structure has the best reliability, while the MFFC structure is the least reliable. Note that the above statistical analysis approach can also be applied to the three different types of standard feed-forward MUX PUFs. These feed-forward MUX PUFs exhibit similar characteristics as the modified feed-forward MUX PUFs. ■

2) Uniqueness: According to the derivation in Section VI.B.2, the MFFC structure has the largest stage variation probability and, thus, has the best uniqueness, while the MFFO has the lowest value of the uniqueness indicator among the three modified feed-forward structures.

3) Randomness: Similarly, as discussed in Section VI.B.3, the randomness of the three structures satisfy the relation:

$$\begin{aligned} & Randomness(MFFC) \\ >& Randomness(MFFS) \\ >& Randomness(MFFO). \end{aligned} \tag{44}$$

D. Statistical Properties of MUX/DeMUX PUF

1) Reliability: The analysis of the MUX/DeMUX PUF is similar to the feed-forward structure. If the select signal of a DeMUX flips, the intra-chip variation of the response is given by (assuming the DeMUX acts as skipping K stages, while there are N stages in total):

$$\begin{aligned} & P[sign(\sum^{N} s_i + n_i) \neq sign(\sum^{N-K} s_i + n_i)] \\ =& 2\int_0^{\infty} \frac{1}{\sqrt{2\pi(N-K)(\sigma_s^2+\sigma_n^2)}} exp(-\frac{x^2}{2(N-K)(\sigma_s^2+\sigma_n^2)}) \\ & \int_{-\infty}^{-x} \frac{1}{\sqrt{2\pi K(\sigma_s^2+\sigma_n^2)^2}} exp(-\frac{y^2}{2K(\sigma_s^2+\sigma_n^2)}) dydx \\ =& 2\int_0^{\infty} \frac{1}{\sqrt{2\pi(N-K)(\sigma_s^2+\sigma_n^2)}} exp(-\frac{x^2}{2(N-K)(\sigma_s^2+\sigma_n^2)}) \\ & (\frac{1}{2} - \frac{1}{2}erf(\frac{x}{\sqrt{2K(\sigma_s^2+\sigma_n^2)}}))dx \\ =& \frac{1}{2} - \frac{1}{\pi} arctan(\sqrt{\frac{N-K}{K}}). \end{aligned} \tag{45}$$

It can be seen that the probability $P[sign(\sum^{N} s_i + n_i) \neq sign(\sum^{N-K} s_i + n_i)]$ increases with K.

If we also employ feed-forward path to generate the select signal of the DeMUXs, then P_{intra} of the MUX/DeMUX PUF with a single feed-forward path can be expressed as

$$P_{intra} = (1-P_1)P_1 + P_1 \times \left(\frac{1}{2} - \frac{1}{\pi} arctan(\sqrt{\frac{N-K}{K}})\right), \tag{46}$$

where $P_1 = \frac{1}{2} - \frac{1}{\pi} arctan(\sqrt{\frac{\sigma_s^4}{2\sigma_s^2\sigma_n^2+\sigma_n^4}})$, which is equal to P_{intra} of the original MUX PUF. If $\frac{N-K}{K} < \frac{\sigma_s^4}{2\sigma_s^2\sigma_n^2+\sigma_n^4}$, P_{intra} of MUX/DeMUX PUF will be greater than P_{intra} of the original MUX PUF. Therefore, similar to the feed-forward MUX PUF, the intra-chip variation of the MUX/DeMUX PUF

will also depend on the number and the locations of the signal propagation paths.

2) Uniqueness: As shown in Section V, the greater of the number of stages in the original MUX PUF, the less biased the output will be. Therefore, the MUX/DeMUX PUF will have less uniqueness, as some stages will be skipped under certain configurations. In other words, P_{inter} of the MUX/DeMUX PUF is expected to be smaller than the P_{inter} of the original MUX PUF.

3) Randomness: Since the output will be more biased, we can conclude that the randomness will also be degraded by introducing DeMUXs into the original MUX PUF.

VII. Performance Comparison of Various MUX-based PUFs

Based on the statistical analysis results, the performance comparisons of the MUX-based PUFs are summarized in Table IV.

These analysis enables deeper understandings of the MUX-based PUFs from the results of the analysis, which could be exploited to improve the performance during PUF design. A number of claims are listed below:

(a) In a MUX PUF, if we increase the number of stages, uniqueness and randomness will improve while reliability will be degraded.
(b) Smaller skew of the arbiter will lead to higher uniqueness and randomness.
(c) The stage variation probability will increase with the number of previous feed-forward paths in a feed-forward structure, as the error in previous path would propagate to later stages.
(d) When designing the feed-forward PUF, an appropriate tradeoff point should be achieved based on the particular application and the performance requirement. Designer should be careful in selecting the type, the number, and the locations of feed-forward paths.
(e) The number and the locations of the paths in the *MUX/DeMUX PUF* also provide a tradeoff between reliability and uniqueness.

VIII. Experiments

A. Experimental Setup

Experiments were carried out by SPICE simulations on a 65-nm technology process. We use the Monte-Carlo method to simulate the effect of process variations and environmental variations. In our simulation, we set up the transistor parameters and process variations based on a major industrial standard model, according to the findings in the area of statistical static timing analysis [16], [23]. All of the simulated MUX-based PUFs have 100 MUX stages. We placed 10 feed-forward paths regularly on the MUX stages for each PUF structure with feed-forward paths and 10 DeMUXs regularly for MUX/DeMUX PUFs. We generated 100-bit responses for measurement in our experiments. All the structures were tested by at least 1000 Monte-Carlo runs.

The inter-chip variations and the intra-chip variations are computed according to the Hamming distances obtained for different chips and the same chip under different readouts, respectively. Part of these results have already been presented in [19], [20]. The randomness values are calculated based on the total numbers of 0's and 1's for each MUX-based PUF structure.

B. Results

Table V presents the results of inter-chip variations, intra-chip variations, and the percentage of 1's in the response., while Table VI presents the results of the three performance indicators: *reliability*, *uniqueness*, and *randomness*. First, it can be observed that the minimum inter-chip variation is larger than the maximum intra-chip variation for all of the simulated structures. Thus, we can conclude that the variations caused by the randomness in manufacturing process are more significant than the variations under different environmental conditions. Therefore, these PUFs can be used as reliable secret keys with some error correcting techniques. Second, it can also be observed that by adding feed-forward arbiters into the MUX PUF circuit, the inter-chip variations and intra-chip variations are both increased, since the noise influences the select signals of some of the intermediate stages. Furthermore, it can be seen that the modified feed-forward structures lead to better reliability than the standard feed-forward MUX PUFs. Compared to the original MUX PUF, the intra-chip variation of the standard feed-forward MUX PUF is increased by 68% on average. But the intra-chip variation of the modified feed-forward MUX PUF is only increased by 17% on average, which is only $\frac{1}{4}$ of the standard feed-forward PUFs. Therefore, we can conclude that the reliability is improved by adopting the proposed modified feed-forward path. Finally, it can also be observed that the randomness is improved by introducing feed-forward paths into the original MUX PUF.

C. Discussion

By comparing the experimental results presented in Table V and Table VI, it can be concluded that the relations between the performances of different types of MUX-based PUFs are consistent with the theoretical results shown in Table II. Note that the value of $P(R = 1)$ which is more close to 0.5 indicates better randomness. It can also be observed from Table V and Table VI that the feed-forward separate structure is the most reliable structure while the feed-forward cascade is the least reliable one among the three feed-forward structures. Moreover, the Reconfigurable MUX/DeMUX PUF has relatively low inter-chip variations; as a result, the uniqueness of this structure is decreased.

These experimental results validate the correctness of our statistical analysis. Overall, all the MUX-based PUF structures can be used as reliable secret keys for authentication and identification within certain error tolerance, as the PUFs exhibit sufficient gaps between the minimum of the inter-chip variations and the maximum of intra-chip variations.

IX. Conclusion and Future Work

We have presented a systematic statistical approach to quantitatively evaluate various types of MUX-based PUFs. We defined three performance indicators - reliability, uniqueness, and randomness - to compare the performances of these MUX-based PUFs. These indicators are also validated by the corresponding simulation results. The experimental results show that the proposed statistical analysis approach effectively reflects the characteristics of various PUF designs. We have also proposed a novel modified feed-forward MUX PUF structure, which has better reliability than the standard feed-forward MUX PUF. Future work will be directed towards the evaluation of MUX-based PUFs from a security perspective by various types of modeling attacks.

TABLE IV: Performance Indicators Comparison

Indicator	Expression	Relation
Reliability	$1 - P_{intra}$	original MUX > MFFO > MFFS > MFFC
Uniqueness	$1 - \|2P_{inter} - 1\|$	MFFC > MFFS > MFFO > original MUX > MUX/DeMUX
Randomness	$1 - \|2P(R = 1) - 1\|$	MFFC > MFFS > MFFO > original MUX > MUX/DeMUX

TABLE V: Results of Inter-Chip and Intra-Chip Variations for 100-Stage PUFs

Structures	Inter-Chip Variation		Intra-Chip Variation		$P(R = 1)$
	Max	Min	Max	Avg	
Original MUX	59%	22%	13%	5.8%	32.8%
Feed-forward Overlap	66%	27%	15%	8.7%	38.8%
Feed-forward Cascade	64%	25%	20%	10.7%	42.1%
Feed-forward Separate	65%	26%	17%	9.9%	40.3%
Modified Feed-forward Overlap	61%	25%	14%	6.6%	37.3%
Modified Feed-forward Cascade	64%	25%	15%	7.0%	39.9%
Modified Feed-forward Separate	61%	27%	15%	6.9%	38.4%
MUX/DeMUX	57%	23%	16%	7.1%	29.9%

TABLE VI: Results of Performance Indicators for 100-Stage PUFs

Structures	Reliability	Uniqueness	Randomness
Original MUX	94.2%	88.2%	65.6%
Feed-forward Overlap	91.3%	95.0%	77.6%
Feed-forward Cascade	89.3%	97.5%	84.2%
Feed-forward Separate	90.1%	96.2%	80.6%
Modified Feed-forward Overlap	93.4%	93.5%	74.6%
Modified Feed-forward Cascade	93.0%	95.9%	79.8%
Modified Feed-forward Separate	93.1%	94.6%	76.8%
MUX/DeMUX	92.9%	83.8%	59.8%

REFERENCES

[1] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, "Physical one-way functions." *Science*, vol. 297(5589), pp. 2026–2030, 2002.

[2] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas, "Silicon physical random functions," in *Proceedings of ACM Conference on Computer and Communications Security*, 2002, pp. 148–160.

[3] B. Gassend, D. Clarke, M. V. Dijk, and S. Devadas, "Controlled physical unclonable functions," in *Proceedings of 18th Annual Computer Security Application Conference*, 2002, pp. 149–160.

[4] B. Škorić, S. Maubach, T. Kevenaar, and P. Tuyls, "Information-theoretic analysis of capacitive physical unclonable functions," *Journal of Applied physics*, vol. 100, no. 2, pp. 024 902–024 902, 2006.

[5] B. Škorić, "On the entropy of keys derived from laser speckle; statistical properties of gabor-transformed speckle," *Journal of Optics A: Pure and Applied Optics*, vol. 10, no. 5, p. 055304, 2008.

[6] A. Maiti, J. Casarona, L. McHale, and P. Schaumont, "A large scale characterization of RO-PUF," in *Proceedings of IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, 2010, pp. 94–99.

[7] R. Maes, P. Tuyls, and I. Verbauwhede, "Statistical analysis of silicon PUF responses for device identification," in *Proceedings of SECSI Workshop*, vol. 2008, 2008.

[8] Z. C. Jouini, J. Danger, and L. Bossuet, "Performance evaluation of physically unclonable function by delay statistics," in *Proceedings of IEEE 9th International New Circuits and Systems Conference (NEWCAS)*, 2011, pp. 482–485.

[9] Z. Tariguliyev and B. Ors, "Reliability and security of arbiter-based physical unclonable function circuits," *International Journal of Communication Systems*, 2012.

[10] Y. Hori, T. Yoshida, T. Katashita, and A. Satoh, "Quantitative and statistical performance evaluation of arbiter physical unclonable functions on FPGAs," in *Proceedings of International Conference on Reconfigurable Computing and FPGAs (ReConFig)*, 2010, pp. 298–303.

[11] I. Kim, A. Maiti, L. Nazhandali, P. Schaumont, V. Vivekraja, and H. Zhang, "From statistics to circuits: Foundations for future physical unclonable functions," pp. 55–78, 2010.

[12] D. Lim, J. W. Lee, B. Gassend, G. E. Suh, M. van Dijk, and S. Devadas, "Extracting secret keys from integrated circuits," *IEEE Transaction on Very Large Scale Integration Systems*, vol. 13(10), pp. 1200–1205, 2005.

[13] J. Guajardo, S. S. Kumar, G.-J. Schrijen, and P. Tuyls, "FPGA intrinsic PUFs and their use for IP protection," in *Proceedings of Cryptographic Hardware and Embedded Systems (CHES 2007)*, 2007, pp. 10–13.

[14] S. Kumar, J. Guajardo, R. Maesyz, G. Schrijen, and P. Tuyls, "Extended abstract: The butterfly PUF protecting IP on every FPGA," in *Proceedings of Hardware-Oriented Security and Trust (HOST 2008)*, 2008, pp. 67–70.

[15] U. Rührmair, H. Busch, and S. Katzenbeisser, "Strong PUFs: models, constructions, and security proofs," pp. 79–96, 2010.

[16] H. Chang and S. Sapatnekar, "Statistical timing analysis considering spatial correlation in a pert-like traversal," in *Proceedings of IEEE International Conference Computer-Aided Design Integrated Circuits and Systems*, 2003, pp. 621–625.

[17] J.-W. Lee, D. Lim, B. Gassend, G. E. Suh, M. van Dijk, and S. Devadas, "A technique to build a secret key in integrated circuits with identification and authentication applications," in *Proceedings of IEEE International Conference Computer-Aided Design Integrated Circuits and Systems*, 2003, pp. 621–625.

[18] U. Ruhrmair, F. Sehnke, J. Solter, G. Dror, S. Devadas, and J. Schmidhuber, "Modeling attacks on physical unclonable functions," in *Proceedings of Conference on RFID Security*, 2010, pp. 237–249.

[19] Y. Lao and K. K. Parhi, "Novel reconfigurable silicon physical unclonable functions," in *Proceedings of Workshop on Foundations of Dependable and Secure Cyber-Physical Systems (FDSCPS)*, 2011, pp. 30–36.

[20] ——, "Reconfigurable architectures for silicon physical unclonable functions," in *Proceedings of IEEE International Conference on Electro Information Technology*, 2011.

[21] M. Majzoobi, F. Koushanfar, and M. Potkonjak, "Techniques for design and implementation of secure reconfigurable PUFs," *ACM Transactions on Reconfigurable Technology and Systems*, vol. 2, no. 1, pp. 1–33, 2009.

[22] Y. A. Prudnikov, A. P. Brychkov, and O. L. Marichev, "Integrals and series, vol. 2: Special functions," *Gordon and Breach Science Publishers*, 1990.

[23] H. Chang and S. Sapatnekar, "Statistical timing analysis under spatial correlations," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 24, no. 9, pp. 1467–1482, 2005.