IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received April 3, 2018, accepted May 15, 2018, date of publication May 21, 2018, date of current version June 19, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2839363

Ultra-Lightweight and Reconfigurable Tristate Inverter Based Physical Unclonable Function Design

YIJUN CUI[1], CHONGYAN GU[2], (Member, IEEE), CHENGHUA WANG[1], MÁIRE O'NEILL[2], (Senior Member, IEEE), AND WEIQIANG LIU[1], (Senior Member, IEEE)

[1]College of Electronic and Information Engineering, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China
[2]Centre for Secure Information Technologies, ECIT, Queen's University Belfast, Belfast BT3 9DT, U.K.

Corresponding author: Weiqiang Liu (liuweiqiang@ nuaa.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61771239, in part by the Natural Science Foundation of Jiangsu Province under Grant BK20151477, in part by the Fundamental Research Funds for the Central Universities China under Grant NS2017024, in part by the Institute for Information and Communications Technology Promotion through the Korean Government (Study on secure key hiding technology for IoT devices [KeyHAS Project]) under Grant 2016-0-00399, and in part by the Engineering and Physical Sciences Research Council under Grant EP/N508664/-CSIT2.

ABSTRACT A physical unclonable function (PUF) is a promising security primitive which utilizes the manufacturing process variations to generate a unique unclonable digital fingerprint for a chip. It is especially suitable for resource constrained security applications, *e.g.* internet of things (IoT) devices. The ring oscillator (RO) PUF and the static RAM (SRAM) PUF are two of the most extensively studied PUF designs. However, previous RO PUF designs require a lot of hardware resources for ROs to be robust and SRAM PUFs are not suitable for authentication. The previous research by the author proposed a tristate static RAM (TSRAM) PUF which is a highly flexible challenge response pair (CRP) based SRAM PUF design. In this paper, a novel configurable PUF structure based on tristate inverters, namely a tristate configurable ring oscillator (TCRO) PUF is proposed. A configurable delay unit, composed of a tristate matrix, is used to replace the inverters in the RO PUF. The configurable bits are able to select a subset of the tristate inverters in the delay unit. Each tristate inverter is completely utilized by using the configurable delay unit and thus the approach enhances the flexibility and entropy of the proposed PUF design. The proposed PUF design can generate an exponential number of CRPs compared with the conventional RO PUF. Moreover, the proposed design significantly reduces the hardware resource consumption of the RO PUF. Delay models of both the TSRAM PUF and the proposed TCRO PUF designs are presented. A comprehensive evaluation of the TSRAM PUF is proceeded. To validate the proposed TSRAM PUF and TCRO PUF designs, a simulation based on UMC 65nm technology and a hardware implementation on a Xilinx Virtex-II FPGA are presented. The experimental results demonstrate good uniqueness and reliability as well as high efficiency in terms of hardware cost.

INDEX TERMS PUF, lightweight, tristate inverter, uniqueness, reliability.

I. INTRODUCTION

Nowadays non-volatile memory (NVM) based security mechanisms are widely used in conventional security systems, in which binary encrypted keys are stored and authenticated to access stored secret information. However, with the development of attacking techniques, *e.g.* side channel analysis (SCA), the keys stored in NVM are vulnerable to adversaries [1]. To address this issue, PUF designs have been investigated by researchers to improve hardware security [2], [3]. A PUF is a security primitive that utilizes unpredictable fabrication variations to encrypt integrated circuits (ICs) to provide unique identifying information. The random variations in chips that are produced under the same fabrication process can lead to different unique responses when presented with the same input challenge. When an input (challenge) is sent to a PUF circuit, a unique output (response) will be generated. PUFs can use these CRPs to authenticate devices and distinguish genuine devices from fake ones. Hence, PUFs can be applied to key generation [4], [5], radio-frequency identification (RFID) security [6], [7] and IP protection [8], [9]. Commonly, PUFs are categorized into delay-based PUFs and memory-based PUFs [10]. Delay-based PUFs focus on extracting the differences in the propagation delay of signals and memory-based PUFs detect the instability in memory cells when powered up. To date, a number of delay-based PUF designs have been proposed to exploit the various types of fabrication variations in IC, *e.g.* Arbiter PUF [11], [12] and RO PUF [13]. Memory-based PUF designs have been proposed including static RAM (SRAM) PUF [14], [15], Butterfly PUF [8], FPGA ID generator [16], *etc.*.

RO PUF is one of the most promising designs due to its reconfigurability, high uniqueness and reliability. RO PUF is composed of RO pairs based on the basic RO unit [2]. To generate a single bit response of a conventional RO PUF design, two symmetrical and route-balanced ROs are used to produce two different frequencies and one 1-bit response is decided by comparing two frequencies. A counter and a comparator are used to generate one bit output, either '0' or '1'. This architecture incurs large power and area overheads. Configurable RO PUFs have been proposed to improve the reliability and hardware resource usage of RO PUF [13], [17]–[19], where multiplexers (MUXs) are used to select one of two inverters and thus the number of CRPs increased and the hardware consumption is decreased.

A cross-coupled tristate inverter based SRAM PUF, TSRAM PUF, was proposed in our previous work [20]. The tristate inverters introduce a mechanism that can reconfigure the SRAM cell, which produces effective CRPs without using any additional auxiliary processing. In this paper, we propose a novel configurable PUF architecture based on a tristate inverter matrix, which reframes the design of the conventional RO PUF design. A configurable delay unit composed of a tristate inverter matrix is used to replace the ROs in the RO PUF and the memory cell in the SRAM PUF. The configurable bits are able to select a subset of the tristate inverters in the delay unit. By using this strategy, every tristate inverter in the PUF design can be fully used to enhance the flexibility of the PUF design. The new scheme can generate more CRPs at an exponential order compared to the conventional RO PUF designs while significantly reducing the hardware area consumption.

In contrast to current existing improvements that either employ a RO to generate PUF CRPs, the quantity of tristate inverters can be flexibly selected and utilized in a RO. The main advantages of the proposed TCRO PUF design are as follows: 1) high efficiency in term of hardware cost. The proposed design improves the efficiency of every single transistor used to compose the TCRO PUF structure. Due to the tristate inverters, the configurable signal of the TCRO PUF design enables every inverter to contribute to the CRPs. Hence, the proposed TCRO PUF design, based on the same amount of the tristate inverters, has a large number of CRPs; 2) high flexibility. More than two tristate inverters are connected in parallel to form a new architecture whose output is non-linear; 3) low cost and lightweight. The proposed TCRO PUF design achieves the same number of CRPs by using less transistors compared to the previous designs. Hence, the proposed TCRO PUF is very lightweight, and is suitable for resource constrained applications, *e.g.* IoT devices.

To validate the functionality and performance of the proposed TCRO and TSRAM PUF designs, simulations using UMC 65nm technology and practical implementation on a Xilinx Virtex-II field programmable gate array (FPGA) device are evaluated. Experimental results show that the proposed designs use the smallest number of hardware resources compared with previous work. Reliability experiments under temperature and voltage variations demonstrate good robustness of the proposed designs.

The three main contributions of this paper are summarized as follows:

1) A new TCRO PUF design is proposed based on a tristate inverter matrix. The proposed TCRO PUF is ultra-lightweight and reconfigurable compared with conventional RO PUF designs.
2) CMOS simulations and FPGA implementations are conducted to validate the performance of the proposed TCRO PUF. The TCRO PUF achieves good uniqueness results with values of 49.69% and 48.30% on ASIC and FPGA respectively, as well as a good reliability result of 95.27% on FPGA.
3) A comprehensively evaluation of the previously proposed TSRAM PUF is presented in this paper. The experimental results show that the TSRAM PUF achieves good uniqueness results of 49.7% and 43.4% on ASIC and FPGA respectively, as well as a reliability result of 94.66% on FPGA.

The rest of the paper is organized as follows. Section II provides background on related PUF structures. Section III gives the preliminaries of the design. Section IV presents the detailed structure and circuit of the TSRAM PUF and proposed reconfigurable TCRO PUF. Section V evaluates the simulation performance of the proposed PUF in Cadence with UMC 65nm technology. The implementation of the TSRAM PUF and proposed TCRO PUF on FPGA is given in section VI. Finally, a conclusion is provided in Section VII.

II. RELATED RESEARCHES

A. RO PUF

The RO PUF is one of the most widely studied PUF designs due to its high reliability and uniqueness. RO is widely used in IC designs. A typical RO PUF is shown in Figure 1. The RO PUF is composed of RO pairs based on the basic RO unit. A counter is employed to calculate the frequency of each RO and a comparator is used to compare frequencies from n ROs. The resulting 1-bit response is dependent on the output of the comparator, either '1' or '0' [2].

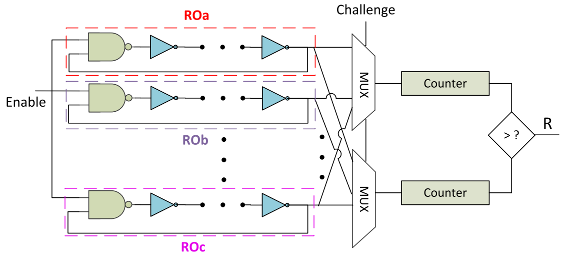


FIGURE 1. Conventional RO PUF by [2].

However, the conventional RO PUF has some limitations. In particular, it has a relatively low entropy due to the relationship of the RO pairs. As shown in Figure 1, if the frequency of RO_a is higher than RO_b, and the frequency of RO_b is higher than RO_c, obviously the frequency of RO_a is higher than RO_c. Due to this relationship, the conventional RO PUF can be attack and the hardware resource usage is high.

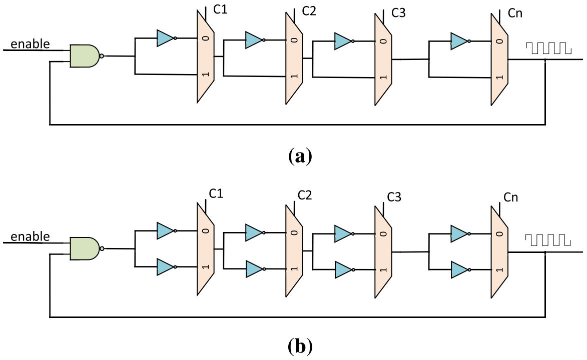


FIGURE 2. Conventional CRO PUF designs. (a) CRO PUF by [17]. (b) CRO PUF by [18].

In order to address these issues, improvements have been developed, *e.g.* CRO PUF [17], [18] as shown in Figure 2(a) and Figure 2(b). In Figure 2(a), a delay unit is composed of a chain of delay elements, where the delay element is constructed using an inverter and a MUX. The challenge bit of each delay element, $\forall C \in (0, 1)$, selects whether the inverter feeds into a RO or not. A similar strategy as shown in Figure 2(a) is applied to construct a delay unit by comprising two inverters and a MUX. One of the inverters in each delay element is chosen to form a RO. Compared to Figure 2(a), the number of the inverters in Figure 2(b) is restricted to a constant. These improvements have increased circuit entropy and reduced the hardware resource usage compared to the conventional RO PUF. However, for its application in low-cost IoT devices, improvements on RO PUF designs by decreasing the hardware area consumption are still desirable.

B. SRAM PUF

The SRAM PUF is one of the most widely known memory-based PUF designs, which evaluates the power-up pattern of a standard 6T SRAM array. Each SRAM cell is composed of two cross-coupled CMOS inverters as shown in Figure 3(a). The predominant mismatch in an SRAM cell determining its power-up state is the difference between the threshold voltages (V_{th}) of both PMOS transistors P1 and P2 as shown in Figure 3(b). Due to the mismatch, the SRAM PUF cell will power up to either a '0' or '1' as a PUF response [14].

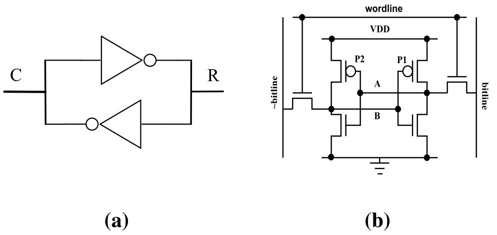


FIGURE 3. Conventional SRAM PUF design by [14]. (a) Gate level. (b) Cell level.

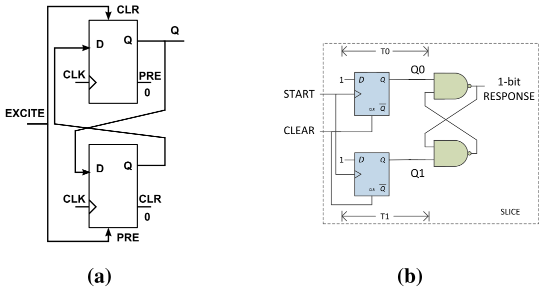


FIGURE 4. Other memory-based PUF designs. (a) Butterfly PUF by [8]. (b) FPGA ID generator by [16].

To address the problems of SRAM PUFs requiring a device power-up operation to generate a response, Kumar *et al.* [8] propose the Butterfly PUF as shown in Figure 4(a) to emulate the behaviour of an SRAM PUF, and implemented their design on a Xilinx Virtex-5 FPGA. For 64 Butterfly PUF cells, 130 slices are consumed, and the area scales linearly with two slices utilized for each cell. Due to the unbalanced routing on FPGA the response is a function of imbalance in wire routing rather than the variability from the cells. To counter this issue, Gu *et al.* [16] proposed a compact FPGA ID generator design, as shown in Figure 4(b), which utilizes only one single slice to generate a 1-bit response and is manually placed and routed to ensure balanced routing. To generate a 64-bit response, 64 slices are used. However, these designs are Weak PUFs since none of these designs have the capability to produce CRPs. This restricts their application to only key generation rather than authentication.

In order to enhance the practical applications of SRAM PUFs, a protocol is introduced by [21], which utilizes the address of the SRAM PUF as a challenge and the SRAM word as a response. A typical authentication protocol is illustrated in Figure 5 for devices equipped with SRAM PUF. When different challenges (SRAM addresses) are applied to the SRAM PUF, responses will be generated automatically.

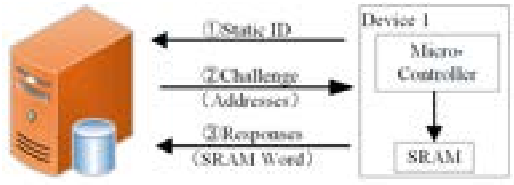


FIGURE 5. Typical protocol for SRAM PUF by [21].

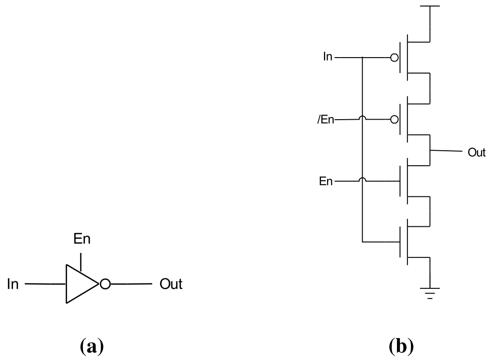


FIGURE 6. A tristate inverter. (a) Gate symbol. (b) Transistor level structure.

III. PRELIMINARIES

A. TRISTATE INVERTER

An inverter is a common component in a PUF structure, *e.g.* inverters are used in conventional RO PUF designs and the SRAM PUF designs. In our proposed designs, a normal inverter is replaced by a tristate inverter. Every tristate inverter, as shown in Figure 6(a), has an enable signal to activate the operation. Figure 6(b) shows the transistor level of a tristate inverter. When the signal *En* is set as '0', both input related transistors are disabled, which leaves the output floating, producing a high impedance output. In contrast, when *En* is '1', both input related transistors are enabled, and the tristate inverter is equivalent to a common inverter.

B. EVALUATION METRICS

To investigate the performance of the proposed PUF designs, two important metrics are evaluated in this work, *i.e.* uniqueness and reliability.

1) UNIQUENESS

As the output response of a PUF will be used for security applications, *e.g.* device authentication and key generation, the response of every chip should be unpredictable. Uniqueness evaluates how easily the responses of different PUF implementations can be differentiated when the same challenge input is used. A percentage measurement for uniqueness based on average inter-chip hamming distance (HD) can be defined according to Equation 1. Two chips i and j among k devices implement the same PUF circuit and derive two $n-$bit responses, R_i and R_j, from the same challenge C.

$$\mathsf{Uniqueness} = \frac{2}{k(k-1)} \sum_{i=1}^{k-1} \sum_{j=i+1}^{k} \frac{\mathsf{HD}(\mathsf{R}_i, \mathsf{R}_j)}{\mathsf{n}} \times 100 \tag{1}$$

Ideally, the uniqueness should be 50%.

2) RELIABILITY

A PUF design should always produce the same response to the same challenge. However, variations in the supply voltage and temperature can affect the response. Reliability assesses the robustness of a PUF design under different environmental conditions. We use the percentage of the number of unstable bits to measure a PUF's reliability, which can be defined by finding the average intra-chip HD of s $n-$bit responses as in Equation 2.

$$\mathsf{HD}_{\mathsf{INTRA}} = \frac{1}{s} \sum_{t=1}^{s} \frac{\mathsf{HD}(\mathsf{R}_i, \mathsf{R}'_{i,t})}{\mathsf{n}} \times 100 \tag{2}$$

where $R(i,t)'$ is the $t-$th sample of R'_i. The percentage figure of merit for reliability can be defined as Equation 3.

$$\mathsf{Reliability} = 100 - \mathsf{HD}_{\mathsf{INTRA}} \tag{3}$$

3) UNIFORMITY

The uniformity of a PUF design measures the proportion of one and zero bits in a response, from which the likelihood of each value can be derived. If a design returns responses that are ideally random, then the distribution of bit values will be equal between ones and zeros. Having this property is essential from a security perspective to prevent an attacker from guessing if a response of a particular device is biased towards a particular value. To estimate the uniformity, it is simply a matter of finding the Hamming weight (HW) of a response, which will give the ratio of ones and zeros, as well any biases in the design of the PUF cell itself as each bit is independent.

For device i and an N-bit response the percentage HW of the $N-$bit response can be calculated as follows:

$$\mathrm{HW}\,(\Phi_i) = \frac{1}{N} \sum_{j=1}^{N} R_{i,j} \times 100 \tag{4}$$

where, $R_{i,j}$ is the j-th bit of the response from the i-th device.

IV. PROPOSED TSRAM PUF AND TCRO PUF DESIGNS

A. TSRAM PUF

The 1-bit TSRAM PUF design proposed in our previous work [20], consists of two identical cross-coupled tristate inverter arrays, is shown in Figure 7. Each array contains n parallel tristate inverters. The enable bits are labeled as *challenge part I*, $C1[i]$, and *challenge part II*, $C2[i]$, $i = 1, 2, \ldots, n$.

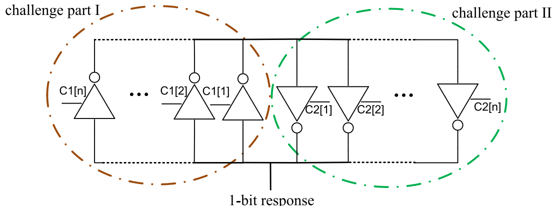


FIGURE 7. An 1-bit TSRAM PUF.

When none of the tristate inverters is enabled, the output of the TSRAM PUF circuit is in a state of high impedance. When the challenge signal contains one or more enable signals, tristate inverters are selected from the two arrays to form an effective SRAM PUF cell, forcing the circuit to settle down to one of the two stable states, *i.e.* ‘0’ or ‘1’. For an identical cross-coupled loop, the same number of tristate inverters, at least one in each array, should be enabled at the same time in each challenge part. When only one tristate inverter is selected from each array, the TSRAM PUF operates like a conventional SRAM PUF. Once the tristate inverters are enabled, the TSRAM PUF cell produces a 1-bit response. Ideally, the TSRAM PUF cell with two physically identical inverters is logically undetermined. Due to the physical mismatch and the electrical noise in a practical implementation, the cell will converge to one of the two stable states. If two or more tristate inverters are selected from each array, the additional current generated could enhance the uniqueness of the response. This is demonstrated in the next section. The number of tristate inverters selected is determined by the challenges. This reconfigurable architecture enables the TSRAM PUF to generate effective CRPs without the need for additional auxiliary processing, such as a one-way function or stream cipher [15], as required by the conventional SRAM PUF aiming to obtain multiple CRPs. The TSRAM PUF can efficiently reduce the hardware resource consumption and the system complexity. A general TSRAM PUF architecture is shown in Figure 8, where C-I, C-II and Rare used to represent challenge part I, challenge part II and the response. The challenge signal determines the number of tristate inverters that are selected to form the metastable loop. The challenge input for each TSRAM PUF cell can be the same or different. If the application demands more CRPs, then different challenges can be applied to C-I and C-II. Otherwise, the challenges for each PUF cell can be the same.

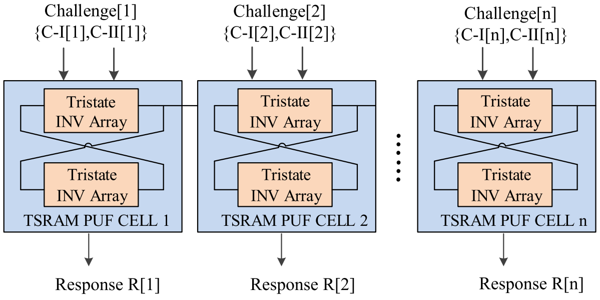


FIGURE 8. n-bit TSRAM PUF architecture.(INV: inverter).

B. PROPOSED TCRO PUF

1) ARCHITECTURE

The proposed 1-bit TCRO PUF architecture, as shown in Figure 9, is composed of two groups of delay paths, constructed using identical tristate inverter matrices. For each group, one tristate inverter matrix is selected to feed into the counter depending on the challenge bits. The frequencies are calculated by the counters and compared using a comparator to generate a 1-bit response, either ‘0’ or ‘1’.

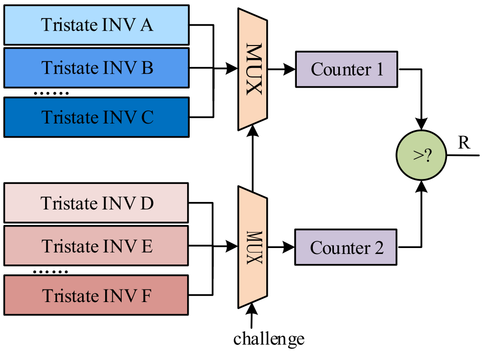


FIGURE 9. The proposed TCRO PUF.

An example of a tristate matrix cell, comprising by an $n \times m$ array of CMOS controlled tristate inverters and a two input AND gate, is illustrated in Figure 10. When the *Enable* signal is activated, the TCRO PUF cell starts to oscillate.

Configurable bits are used to enable the tristate inverter in the proposed design. According to the configurable bits, different tristate inverters of the TCRO PUF cell are selected to feed into the circuit and contribute to the output frequency. The configurable bits of each column in the cell should have at least one bit equal to 1 to ensure the signal can propagate to the final output. Due to the process variations in devices, the responses of each cell will exhibit differences when applying the same configurable bits. When only one tristate inverter is activated in each column, the TCRO PUF cell is equivalent to a conventional RO PUF. In the proposed TCRO PUF design, the activation of a tristate inverter provides an additional charging (discharging) current to the capacitive load to effect the time delay on each column stage. Hence, it introduces a reduction of the oscillation period and thus increases the frequency of the tristate RO, which makes the TCRO PUF more reliable.

2) HARDWARE CONSUMPTION

There are n stages and m rows in a TCRO PUF cell that can be used to generate the frequency as illustrated in Figure 10. Assume that k tristate inverters are selected from the n-*th* stage of the delay matrix, the permutation and combination for selecting the tristate inverters can be represented as $\binom{m}{k}^n$. Hence, all selection possibilities of the tristate inverters in

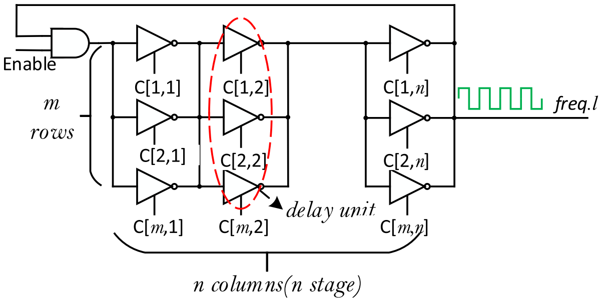


FIGURE 10. A tristate matrix cell for the proposed TCRO PUF.

the *n-th* stage can be derived as $\left(\sum_{k=1}^{m}\binom{m}{k}\right)^{n}$. In order to generate a 1-bit response bit, two identical TCRO matrices over l matrices are utilised and compared. Therefore, the number of selection possibilities of the tristate inverters over n stages can be defined as Equation 5.

$$\mathrm{N_{TCRO}} = \binom{l}{2}\sum_{i=1}^{n}\left(\sum_{k=1}^{m}\binom{m}{k}\right)^{n} \tag{5}$$

The cost efficiency (CE), introduced here to measure the efficiency of the proposed TCRO PUF design, is defined as the number of gates ($\mathrm{N_{gate}}$) per response bit ($\mathrm{N_{bits}}$) as shown in Equation 6.

$$\mathrm{CE} = \frac{\mathrm{N_{gate}}}{\mathrm{N_{bits}}} \tag{6}$$

In the conventional RO PUF [2], the RO is composed of n inverters, and two of m ROs are selected to generate a 1-bit PUF response. Typically, one inverter consists of two transistors. Hence, the CE of a conventional RO PUF can be depicted as Equation 7.

$$\mathrm{CE_{RO}} = \frac{(2n+4)\cdot m}{\binom{m}{2}} = \frac{4n+8}{m-1} \tag{7}$$

For the CRO PUF [17] as shown in Figure 2(a), assuming that it has m CRO cells and n stages on each cell, the number of response bits is calculated as described in $\binom{m}{2}\cdot 2^{n-1}\cdot 2^{n-1}$. Based on this, the CE is computed as described in Equation 8.

$$\mathrm{CE_{CRO1}} = \frac{(6n+4)\cdot m}{\binom{m}{2}\cdot 2^{n-1}\cdot 2^{n-1}} = \frac{6n+4}{(m-1)\cdot 2^{2n-3}} \tag{8}$$

For the CRO PUF [18] as shown in Figure 2(b), based on m CRO cells and n stages on each cell, the CE can be described as Equation 9.

$$\mathrm{CE_{CRO2}} = \frac{(8n+4)\cdot m}{\binom{m}{2}\cdot 2^{n}\cdot 2^{n}} = \frac{8n+4}{(m-1)\cdot 2^{2n-1}} \tag{9}$$

A CE comparison between the conventional RO PUF, the two CRO PUFs and the proposed TCRO PUF designs is shown in Figure 11. The analysis is based on 5 stages ($n = 5$) and 4 RO cells ($m = 4$). It can be seen that the proposed TCRO PUF design achieves the most efficient CE value compared with previous work.

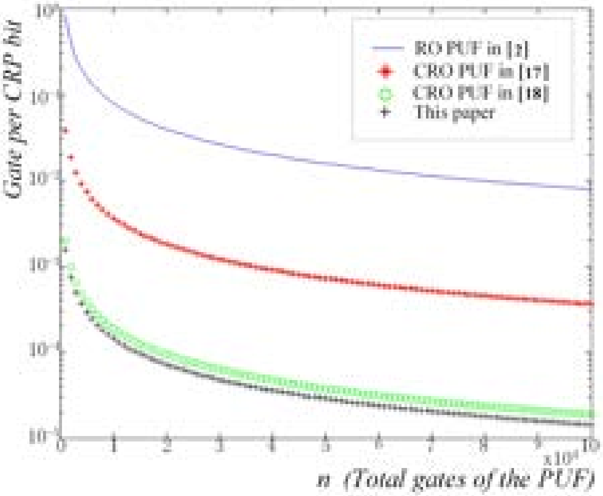


FIGURE 11. A comparison of the CE values on different PUF designs.

V. CMOS SIMULATION RESULTS FOR PROPOSED TSRAM PUF AND TCRO PUF DESIGNS

Tristate inverters are very common in CMOS designs and can be easily implemented in ASIC designs. In order to evaluate the performance of the proposed PUF structure in ASIC, Cadence 6.1 is employed to carry out simulations with UMC 65 nm technology assuming a 1.1V supply voltage. Monte Carlo simulation is utilised to simulate the process variation. The output responses are processed with Matlab to evaluate the PUF metrics, *e.g.* uniqueness. Reliability cannot be evaluated from the simulation results.

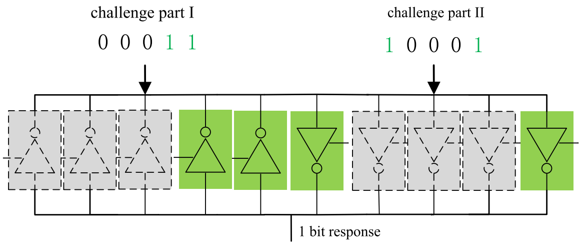


FIGURE 12. An example of the proposed 1-bit TSRAM PUF.

A. TSRAM PUF ON CMOS TECHNOLOGY

1) SIMULATION SETUP

In order to verify the performance of the TSRAM PUF designs, an example of the 1-bit TSRAM PUF cell composed of two groups of 5 tristate inverters, as shown in Figure 12, is designed for simulation. To generate an n-bit TSRAM PUF response, n 1-bit TSRAM PUF cells are created, where $n = 128$ in this work. The number of challenge bits can be flexibly increased depending on the practical application requirement. In this work, 10 challenge bits in each cell is used. Assuming a *challenge part I* of *00011*, and a *challenge part II* of *10001*, the relevant tristate inverters are selected. Every tristate inverter consists of two 1.1V regular threshold voltage PMOS cell and two 1.1V regular threshold voltage NMOS cells.

2) SIMULATION RESULTS FOR TSRAM PUF

Figure 13 shows the Monte Carlo simulation result for the TSRAM PUF design. It can be seen that with the fabrication variations, the PUF circuit settles down to either '0' (0V) or '1' (1.1V) within 40 ps, which demonstrates that the design can generate random response bits from the same challenge inputs.

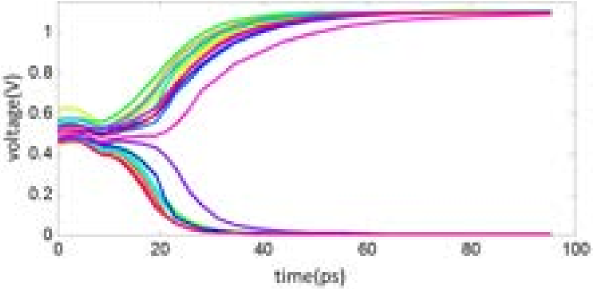


FIGURE 13. Monte Carlo simulation for the TSRAM PUF.

To measure the uniqueness of the TSRAM PUF design, samples are evaluated by sending the same challenge. The uniqueness result is shown in Figure 14. It can be seen that the average uniqueness value is 49.70%, very close to the ideal value of 50%, indicating that the TSRAM PUF performs well in differentiate devices. The uniformity is also calculated based on the simulation data. The value of the uniformity is 51.6%, which is also very close to the ideal value.

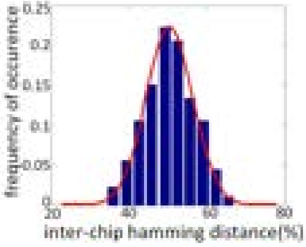


FIGURE 14. Simulation results for the TSRAM PUF.

B. TCRO ON CMOS TECHNOLOGY

1) SIMULATION SETUP

In order to verify the performance of the proposed TCRO PUF designs, a tristate matrix of 5 stages and 4 rows ($m = 4, n = 5$) is built in this simulation. Base on the tristate matrix, 256 tristate RO pairs are used to construct the TCRO PUF. In each tristate matrix, there are 20 bits configurable signals that can dynamically configure the PUF structure. Monte Carlo simulations are employed to simulate the process variations and generate the output frequencies. According to the different output frequencies, the uniqueness of the TCRO PUF is calculated.

2) SIMULATION RESULTS

The transmission delay of a tristate inverter is higher than a normal inverter, and consequently the output frequency of the tristate matrix will be slower compared with a conventional ring oscillator. Figure 15 shows the Monte Carlo simulation for the TCRO PUF, where the output frequency changes with the process variation. It is clear that the frequency of the proposed PUF structure is much slower than a traditional RO. At the same time, the output frequency of the proposed structure will change with the process. After obtain a sufficient number of CRPs, the uniqueness is calculated in Matlab. The uniqueness result is shown in Figure 16. It can be seen that the average uniqueness value is 49.69%, very close to the ideal value of 50%, indicating that the TCRO PUF also performs well in differentiate devices. Based on the simulation responses, the uniformity is calculated and the value is 52.45%.

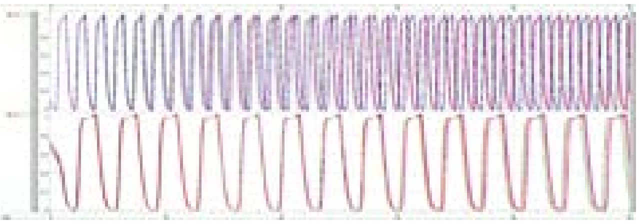


FIGURE 15. Monte Carlo simulation for the TCRO PUF.

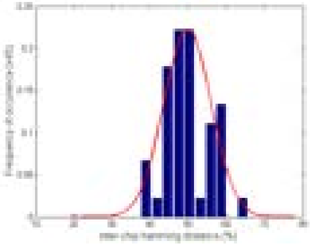


FIGURE 16. Simulation results for the proposed TCRO PUF.

VI. HARDWARE IMPLEMENTATION AND EXPERIMENT

Xilinx FPGAs, including Virtex II, Virtex II Pro and Spartan II, have internal tristate inverters that can be accessed by the user. However, modern FPGAs do not have internal tristate inverters and only have tristate inverters for I/O pins. To comprehensively evaluate the feasibility of the proposed TCRO PUF and TSRAM PUF designs, they are implemented on 10 Xilinx Virtex II XC2VP30 boards. There are two tristate inverters in each CLB, and in total there are 6848 tristate inverters in each XC2VP30 chip. The architecture of the tristate inverter on a Xilinx Virtex II FPGA is shown in Figure 17. To ensure a good performance, the circuit is manually placed and routed to ensure identical delay paths for every TSRAM cell. A hard macro strategy is created by using Xilinx FPGA Editor.

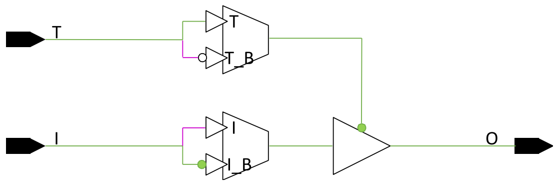


FIGURE 17. A basic tristate inverter on an Xilinx Virtex II FPGA.

The evaluation of the uniqueness and reliability is carried out using the method proposed in [22]. As the core supply voltage of the XC2VP30 chip is 1.5V, the supply voltage is adjusted from 1.3V to 1.7V. The temperature of the chip is adjusted from 0° to 70° using a thermometric cooling and heating plate.

A. TSRAM PUF HARDWARE EXPERIMENT

In this work, a 128-bit response is generated from 128 arrays of tristate inverters. Due to the limited number of tristate inverters on the targeted FPGA, a two-stage ($m = 2$) TSRAM PUF as shown in Figure 18 is implemented based on the internal tristate inverters of the XC2VP30.

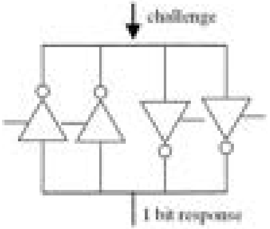
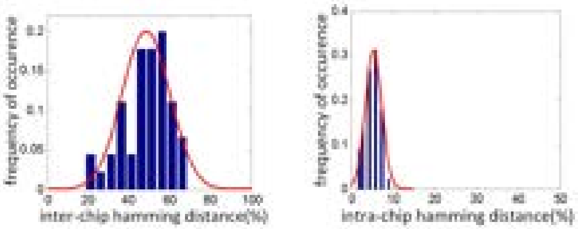


FIGURE 18. 2-stage TSRAM PUF.

Figure 19(a) shows the uniqueness result of 43.4% for the TSRAM PUF on the FPGA. The standard deviation from the FPGA implementation results are higher than the one from the simulation. The reason is that the sample size of the FPGA implementation is smaller than the simulation. The intra-chip HD is 5.34% as illustrated in Figure 19(b), from which the reliability is $100\% - 5.34\% = 94.66\%$, representing the TSRAM PUF design is reliable under environmental variations. The uniformity result is 40.10%, which indicates a good balance between ones and zeros of the responses.



(a)

(b)

FIGURE 19. Experimental results for the TSRAM PUF design. (a) Uniqueness. (b) Intra-chip HD.

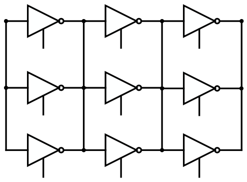
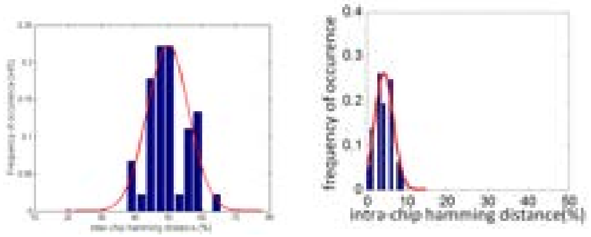


FIGURE 20. Tristate matrix implemented on FPGA.

B. TCRO PUF DESIGN

In order to evaluate the performance of the TCRO PUF in FPGA, a tristate matrix of 3 columns and 3 rows, as shown in Figure 20, is created based on the inverter and the internal tristate gate on a XC2VP30. To avoid routing mismatch, the tristate matrix is well balanced by manual routing. A hard-macro of the tristate matrix is also created using Xilinx FPGA Editor. In each XC2VP30, 128 tristate matrixes are built to generate a 64-bit response. Figure 21 shows the evaluation results of the proposed TCRO PUF, in which Figure 21(a) exhibits the uniqueness result that from the Xilinx Virtex II FPGA. It can be seen that the proposed TCRO PUF achieves the uniqueness result of 48.30%.



(a)

(b)

FIGURE 21. Hardware experimental results for the proposed TCRO PUF design. (a) Uniqueness. (b) Intra-chip HD.

Figure 21(b) shows the reliability of the proposed TCRO PUF design over different operating conditions. It can be seen that the average reliability results of the proposed design are approximately 95.27%. Moreover, the responses also have a good uniformity of 37.43%.

C. COMPARISON WITH OTHER WORK

A comparison of the TSRAM PUF and proposed TCRO PUF with other PUFs is listed in Table 1. The TSRAM and TCRO PUF designs achieve better uniqueness and reliability results from both ASIC simulations and FPGA platforms than previous memory based PUFs and delay based PUFs. Particularly, with the configurable bits, both the TSRAM PUF and TCRO PUF offer numerous configuration options, which increases the number of CRPs exponentially. Also, in term of hardware consumptions, the TSRAM PUF and TCRO PUF use a much lower number of resources to generate a one bit response compared with the previous best PUF designs [18].

TABLE 1. Comparison with conventional memory-based and delay-based PUF designs.

Design	Arbiter PUF [11]	SRAM PUF [14]	CRO PUF [18]	FF-APUF [23]	PUF ID [24]	TSRAM PUF		TCRO PUF	
						ASIC	FPGA	ASIC	FPGA
HDinter	23%	49.9%	47.3%	40%	45.60%	49.7%	43.4%	49.69%	48.30%
HDintra	9%	3.57%	0.06%	2.9%	1.26%	NA	5.34%	NA	4.73%
CRPs	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Gates/Bit	≤ 2	≥ 6	≤ 10	44 slices	1 slice	≥ 1.6	≥ 4	≤ 0.1	≤ 0.1

VII. CONCLUSION

In this paper, a novel and efficient TCRO PUF is proposed and a previous proposed TSRAM PUF is evaluated. A tristate inverter gate is utilized to allow dynamic reconfiguration of the basic cell in both the TCRO PUF and TSRAM PUF designs. The TCRO PUF and TSRAM PUF are desirable for low-cost and low-power security applications. The functionality and performance of the TCRO and TSRAM PUF designs are validated by both simulation using UMC 65nm technology and implementation on a Xilinx Virtex-II FPGA. The experimental results show that the TSRAM PUF achieves good uniqueness and reliability results, which uniqueness results of 49.7% and 43.4% on ASIC and FPGA respectively, as well as a reliability result of 5.34% over a temperature range of $0^{\circ}C \sim 70^{\circ}C$ with 10% fluctuation in supply voltage on FPGA. Furthermore, the TSRAM PUF can provide CRPs that are not available using a conventional SRAM PUF. The TCRO PUF also achieves good uniqueness results of the values of 49.69% and 48.30% on ASIC and FPGA respectively, as well as good reliability results of a value of 4.73% on FPGA. Also, the TSRAM PUF and the proposed TCRO PUF use less hardware resources compared with previous designs, which makes the proposed PUF design very promising in resource-constrained applications.

REFERENCES

[1] A. Moradi, D. Oswald, C. Paar, and P. Swierczynski, "Side-channel attacks on the bitstream encryption mechanism of Altera Stratix II: Facilitating black-box analysis using software reverse-engineering," in *Proc. ACM/SIGDA Int. Symp. Field Programm. Gate Arrays*, 2013, pp. 91–100.

[2] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *Proc. 44th ACM Annu. Des. Autom. Conf.*, 2007, pp. 9–14.

[3] D. Lim, J. W. Lee, B. Gassend, G. E. Suh, M. van Dijk, and S. Devadas, "Extracting secret keys from integrated circuits," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 13, no. 10, pp. 1200–1205, Oct. 2005.

[4] J. Delvaux, D. Gu, D. Schellekens, and I. Verbauwhede, "Helper data algorithms for PUF-based key generation: Overview and analysis," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 34, no. 6, pp. 889–902, Jun. 2015.

[5] M.-D. Yu, R. Sowell, A. Singh, D. M'Raïhi, and S. Devadas, "Performance metrics and empirical results of a PUF cryptographic key generation ASIC," in *Proc. IEEE Int. Symp. Hardw.-Orient. Secur. Trust (HOST)*, Jun. 2012, pp. 108–115.

[6] S. Devadas, E. Suh, S. Paral, R. Sowell, T. Ziola, and V. Khandelwal, "Design and implementation of PUF-based 'unclonable' RFID ICs for anti-counterfeiting and security applications," in *Proc. IEEE Int. Conf. RFID*, Apr. 2008, pp. 58–64.

[7] P. Tuyls and L. Batina, "RFID-tags for anti-counterfeiting," in *Proc. Cryptograph. Track RSA Conf. Topics Cryptol.*, 2006, pp. 115–131.

[8] S. S. Kumar, J. Guajardo, R. Maes, G.-J. Schrijen, and P. Tuyls, "The butterfly PUF protecting IP on every FPGA," in *Proc. IEEE Int. Workshop Hardw.-Orient. Secur. Trust (HOST)*, Jun. 2008, pp. 67–70.

[9] J. Guajardo, S. S. Kumar, G.-J. Schrijen, and P. Tuyls, "FPGA intrinsic PUFs and their use for IP protection," in *Proc. Int. Workshop Cryptograph. Hardw. Embedded Syst.*, 2007, pp. 63–80.

[10] H. Handschuh, G.-J. Schrijen, and P. Tuyls, "Hardware intrinsic security from physically unclonable functions," in *Towards Hardware-Intrinsic Security*. Berlin, Germany: Springer, 2010, pp. 39–53.

[11] Z. Paral and S. Devadas, "Reliable and efficient PUF-based key generation using pattern matching," in *Proc. IEEE Int. Symp. Hardw.-Orient. Secur. Trust (HOST)*, Jun. 2011, pp. 128–133.

[12] K. Fruhashi, M. Shiozaki, A. Fukushima, T. Murayama, and T. Fujino, "The arbiter-PUF with high uniqueness utilizing novel arbiter circuit with delay-time measurement," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, May 2011, pp. 2325–2328.

[13] A. Maiti, J. Casarona, L. McHale, and P. Schaumont, "A large scale characterization of RO-PUF," in *Proc. IEEE Int. Symp. Hardw.-Orient. Secur. Trust (HOST)*, Jun. 2010, pp. 94–99.

[14] D. E. Holcomb, W. P. Burleson, and K. Fu, "Power-up SRAM state as an identifying fingerprint and source of true random numbers," *IEEE Trans. Comput.*, vol. 58, no. 9, pp. 1198–1210, Sep. 2009.

[15] M. Barbareschi, E. Battista, A. Mazzeo, and N. Mazzocca, "Testing 90 nm microcontroller SRAM PUF quality," in *Proc. IEEE Int. Conf. Des., Technol. Integr. Syst. Nanosc. Era (DTIS)*, Apr. 2015, pp. 1–6.

[16] C. Gu, J. Murphy, and M. O'Neill, "A unique and robust single slice fpga identification generator," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, Jun. 2014, pp. 1223–1226.

[17] M. Gao, K. Lai, and G. Qu, "A highly flexible ring oscillator PUF," in *Proc. 51st ACM Annu. Design Autom. Conf.*, 2014, pp. 1–6.

[18] A. Maiti and P. Schaumont, "Improved ring oscillator PUF: An FPGA-friendly secure primitive," *J. Cryptol.*, vol. 24, no. 2, pp. 375–397, 2011.

[19] Y. Cui, C. Wang, W. Liu, Y. Yu, M. O'Neill, and F. Lombardi, "Low-cost configurable ring oscillator PUF with improved uniqueness," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, May 2016, pp. 558–561.

[20] Y. Cui, C. Wang, W. Liu, and M. O'Neill, "A reconfigurable memory PUF based on tristate inverter arrays," in *Proc. IEEE Int. Workshop Signal Process. Syst. (SiPS)*, Oct. 2016, pp. 171–176.

[21] K. Xiao, M. T. Rahman, D. Forte, Y. Huang, M. Su, and M. Tehranipoor, "Bit sselection algorithm suitable for high-volume production of SRAM-PUF," in *Proc. IEEE Int. Symp. Hardw.-Orient. Secur. Trust (HOST)*, May 2014, pp. 101–106.

[22] Y. Cui, C. Wang, W. Liu, and M. O'Neill, "Live demonstration: An automatic evaluation platform for physical unclonable function test," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, May 2016, p. 2377.

[23] C. Gu, Y. Cui, N. Hanley, and M. O'Neill, "Novel lightweight FF-APUF design for FPGA," in *Proc. 29th IEEE Int. Syst.-Chip Conf. (SOCC)*, Sep. 2016, pp. 75–80.

[24] C. Gu, N. Hanley, and M. O'Neill, "Improved reliability of FPGA-based PUF identification generator design," *ACM Trans. Reconfigurable Technol. Syst.*, vol. 10, no. 3, p. 20:1–20:23, May 2017. [Online]. Available: http://doi.acm.org/10.1145/3053681

YIJUN CUI received the B.E. degree in information engineering from the Nanjing University of Aeronautics and Astronautics, Nanjing, China, in 2010, where he is currently pursuing the Ph.D. degree.

He was a Visiting Ph.D. Student with the Data Security System Group, Centre of Secure Information Technologies, Queen's University Belfast, U.K., from 2014 to 2015. His current research interests are mainly in the hardware security.

CHONGYAN GU (S'14–M'16) received the M.Sc. degree (Hons.) in data communications from the University of Sheffield, Sheffield, U.K., in 2006, and the Ph.D. degree from Queen's University Belfast, Belfast, U.K., in 2016. She is currently a Research Fellow with the Center for Secure Information Technologies, Queen's University Belfast, U.K.

Before joining Queen's University Belfast, she was an Electronic Engineer in vehicle security and communication system design of GAC Mitsubishi Corporation, China. Her current research interests include hardware security and trust, physical unclonable functions, true random number generator, hardware Trojan detection, logic obfuscation circuit, and machine learning.

CHENGHUA WANG received the B.Sc. and M.Sc. degrees from Southeast University, Nanjing, China, in 1984 and 1987, respectively. In 1987, he joined the College of Electronic and Information Engineering, Nanjing University of Aeronautics and Astronautics, Nanjing, China, where he became a Full Professor in 2001. He has published six books and over 100 technical papers in journals and conference proceedings. His current research interests include design and test of integrated circuits, circuits and systems for communications, and signal processing. He was a recipient of over 10 teaching and research awards at the national and provincial level.

MÁIRE O'NEILL (M'03–SM'11) is currently the Director of the U.K. Research Institute in Secure Hardware and Embedded Systems. She is also the Chair of information security and the Research Director of data security systems with the Centre for Secure Information Technologies, Queen's University Belfast.

She also leads the EU H2020 SAFEcrypto (Secure Architectures for Future Emerging Cryptography) Project. She was a former holder of a Royal Academy of Engineering Research Fellowship from 2003 to 2008 and previously held an EPSRC Leadership Fellowship from 2008 to 2014.

She has authored two research books and has over 130 peer-reviewed conference and journal publications. Her research interests include hardware cryptographic architectures, lightweight cryptography, side channel analysis, physical unclonable functions, post-quantum cryptography, and quantum-dot cellular automata circuit design. She is also a member of the IET and IACR. She is a member of the Royal Irish Academy and a fellow of the Irish Academy of Engineering. She has received numerous awards for her research work which include a 2014 Royal Academy of Engineering Silver Medal and British Female Inventor in 2007. She is an Associate Editor for IEEE Transactions on Computers and the IEEE Transactions on Emerging Topics in Computing and is an IEEE Circuits and Systems for Communications Technical committee member.

WEIQIANG LIU (M'12–SM'15) received the B.Sc. degree in information engineering from the Nanjing University of Aeronautics and Astronautics (NUAA), Nanjing, China, in 2006, and the Ph.D. degree in electronic engineering from Queen's University Belfast (QUB), Belfast, U.K., in 2012. He was a Research Fellow with the Institute of Electronics, Communications and Information Technology, QUB, from 2012 to 2013. In 2013, he joined the College of Electronic and Information Engineering, NUAA, where he is currently an Associate Professor.

He has published one research book by Artech House and over 60 leading journal and conference papers. His research interests include emerging technologies in computing systems and VLSI design for digital signal processing and cryptography. His paper was finalist in the Best Paper Contest of IEEE ISCAS 2011 and he has co-authored a Best Paper Candidate of ACM GLSVLSI 2015. One of his papers was the Most Popular Article of the IEEE Transactions on Computers in 2017 and one was selected as the Feature Paper of the IEEE TC in the 2017. He serves as a Steering Committee Member of the IEEE Transactions on Multi-Scale Computing Systems, an Associate Editor of the IEEE Transactions on Computers, and the Guest Editors of two special issues of the IEEE Transactions on Emerging Topics in Computing. He has been a technical program committee member for several international conferences including ARITH, ASAP, ISCAS, ISVLSI, NANOARCH, and ICONIP. He is a member of the IEEE Circuits and Systems for Communications Technical Committee.