TVD-PB logic circuit based on camouflaging circuit for IoT security

Yuejun Zhang | Qiufeng Wu | Pengjun Wang | Liang Wen | Zhicun Luan | Chongyan Gu

1Faculty of Electrical Engineering and Computer Science, Ningbo University, Ningbo, Zhejiang, China
2College of Electrical and Electronic Engineering, Wenzhou University, Wenzhou, China
3Department of Electronic Technology, China Coast Guard Academy, Ningbo, Zhejiang, China
4Centre for Secure Information Technologies, Institute of Electronics, Communications, and Information Technology, Queen's University Belfast, Belfast, UK

Abstract

Internet of Things (IoT) devices are vulnerable to many physical attacks, including reverse engineering and side-channel analysis because the sensitive information of circuits may be leaked through the physical characteristics of the device. A logic camouflaging circuit is proposed that uses a balanced power consumption and threshold voltage-defined technique to provide an antiphysical attack scheme to protect the hardware security for IoT devices. The proposed circuit uses a symmetric differential pull-down network in implementing the different logic functions through the threshold voltage reconfiguration circuit. As a result, the power consumption of the circuit attains balance and stability between two different logical operations. The proposed threshold voltage-defined power-balance (TVD-PB) design is fabricated using a 65-nm CMOS technology, and the core area occupies approximately 0.0044 mm², composed of NAND, NOR, XOR, and INV components and multiplier gates of the proposed TVD-PB circuit. The entire chip passed the logic function tests. The measured results show that the average similarity of the TVD-PB universal gate is 99.68%. In addition, the current margin is higher than 55 μA and power consumption of 0.455 mW during each clock cycle at 1.2 V derives 0.1072% of the normalized energy deviation and 0.0453% of the normalized standard deviation. Compared with other state-of-the-art techniques, the power dependency against power attacks is improved effectively.

This is an open access article under the terms of the Creative Commons Attribution License, which permits use, distribution and reproduction in any medium, provided the original work is properly cited.

© 2021 The Authors. IET Circuits Devices & Systems published by John Wiley & Sons Ltd on behalf of The Institution of Engineering and Technology.
1 | INTRODUCTION

The Internet of Things (IoT) has been dramatically and increasingly revolutionised our daily lives, such as in smart cities, smart cars, smart buildings, and home automation [1–3]. With the rapid development of IoT applications without the proper consideration of security challenges, it becomes increasingly difficult to ensure the security of IoT systems [4–6]. As shown in Figure 1, it opens the door to a myriad of security threats, such as communication, life-cycle, software, and physical attacks. Because the nature of IoT may require the deployment of devices in hostile environments, such devices are susceptible to information leaks. These lead to physical attacks, including reverse engineering (RE) [7, 8] and side-channel analysis (SCA) [9–11]. Physical attacks have been used against IoT devices, in which sensitive information of the circuit may be leaked through the physical characteristics of the device. Applying physical attacks on an IoT chip, an attacker can obtain precious cryptographic information, alter the operating system, and damage the circuit, all of which may result in long-term destruction. As a result, it is crucial to develop new countermeasures against physical attacks. Protection of the hardware IP core protects the integrated circuit industry and the electronic information industry, including communications, industry, medical care, and education.

In the era of the IoT, security is an issue of particular concern. Full connectivity provides opportunities for accidental or malicious data corruption and contamination. The decision facing system designers is between software-based or hardware-based security solutions. Security [12] requirements highly overtake functional and performance requirements for the software system. Software-based security approaches are also important for securing computing systems. However, conventional cryptographic methods are usually heavyweight and IoT devices normally have limited hardware resources in which it is difficult to implement computationally conventional cryptographic algorithms. Hence, we use a pure, hardware-based, lightweight camouflaging method to protect hardware circuits.

The rest of this work is organised specifically as follows. The Introduction is outlined in Section 1. Related work is presented in Section 2. Section 3 presents the proposed threshold voltage-defined power-balance (TVD-PB) logic gate and its characteristic analysis. Section 4 presents the very large scale Integration (VLSI) implementation of the proposed TVD-PB logic gates. The characteristics and security evaluation of threshold voltage-defined logic gates and chips are discussed in Section 5. The discussion is concluded in Section 6.

2 | RELATED WORK AND OUR CONTRIBUTIONS

2.1 | Related work

Hardware-based security uses an application-specific integrated circuit (IC) or a processor with dedicated security hardware that is specifically used to provide encryption functions and prevent attacks. Security operations such as encryption or decryption and authentication occur at the IC hardware level, in which encryption algorithm performance is optimised. In addition, sensitive information (such as keys and critical final application parameters) is protected within the electrical boundaries of the encryption hardware. Previous literature reported on different types of countermeasures for physical attacks, including protection of customer data and the intellectual property of designers, to provide security for an IoT system. Many RE countermeasures, such as circuit level [13–16] and algorithm level [17–19], have been proposed to tackle the challenges of RE and prevent IP infringements. At a circuit level, camouflaging technique proposed in Rajendran et al. [13] hampers the image processing–based extraction of a gate-level netlist by concealing gates [14] or dummy contacts in the layout. Another technique to prevent IP piracy is logic locking [15]. Additional encryption blocks are inserted to hide the functionality and implementation of an IC using XOR/NXOR gates, MUXES, and a combination of these elements. Hence, a design delivers accurate functions only if a correct key applies. By combining obfuscation cells and physical unclonable function circuits, a licence can be generated to improve the security of hardware circuits [16]. Unfortunately, the on-chip storage of various data is inherently vulnerable to attacks, including SCA, imaging, and fault analysis. At an algorithm level, Dofe et al. [17] proposed protect all states with an obfuscation method based on low-cost state-deflection, which dynamically deflected state transitions from the original

![Figure 1](image-url) Four different types of security attacks
transition path to a black hole cluster if a wrong key was applied. Koteshwara et al. [18] proposed a dynamic technique, resulting in the change of obfuscating signals with time. Sen-gupta [19] proposed a hologram-based obfuscation, which integrated two digital signal processing (DSP) kernel architectures in a camouflaged manner without changing the functionality of each DSP kernel. However, the introduction of an additional code requires more hardware overhead and is also vulnerable to SCA. Field programmable gate array (FPGA)-based approaches mainly protect device security through algorithms for IoT protection [20, 21], applying algorithms to register transfer level (RTL) codes to realize RTL obfuscation, and mainly defending against hardware Trojan horses, side channel attacks, and so forth. The proposed scheme works from the bottom unit circuit and realizes the unit library. At the bottom layer, the proposed scheme could defend against RE and side channel attacks. Moreover, at the top layer, it can also use algorithms to achieve multilevel obfuscation and further improve the security of the circuit.

In cryptography, an SCA is any attack based on information obtained from the physical implementation of an IoT device. In recent years, many SCA resistant methods have been reported at both the gate and architectural level. A countermeasure based on sense amplifier-based logic (SABL) [22], which has a single switching event per cycle, achieves independent input signals and has constant capacitance charging and discharging at an SCA cell level. Wave dynamic differential logic [23] uses a combination of complementary logic gates to balance activity in the circuit. Multithreshold dual-spacer dual-rail delay-insensitive logic [24] provides security by balancing the side channels both in general and between the dual-rail signals themselves. The differential logic style is effectively limited owing to the unbalanced nature of the parasitic capacitance of the complementary wires. Although all of these symmetrical and deterministic approaches are theoretically resistant to power attacks, they are still vulnerable.

The goal of an IC RE is to uncover the gate netlist, circuit schematic, layout, and manufacturing process details of the chip. With this knowledge, an attacker can more efficiently mount various attacks (e.g., fault injection, side channel), clone or counterfeit the design possibly with hardware Trojans inserted, and discover trade secrets. A few commercial entities such as ChipWorks [25] and TAEUS [26] offer IC RE services and routinely reverse engineer chips on even the most advanced process technologies. For instance, Intel’s 22-nm Xeon processor has been successfully reverse-engineered. However, current approaches such as logic locking or obfuscation have been proposed by industry-relevant researchers [15, 16, 27]. However, they have challenges, such as boolean satisfiability attacks and SCA attacks [23, 24].

2.2 | Our contributions

An anti-RE technique is proposed to tackle the challenge of RE and SCA attacks. The main contributions are described here:

1. A TVD-PB circuit, which requires no special layers, structures, or processes, is proposed and implemented on a standard TSMC 65-nm CMOS processor. A set of experimental results is presented, and the features of the implemented TVD-PB circuit design are discussed.

2. The proposed TVD-PB design, which reduces the relation between power consumption and signals, effectively prevents the image processing-based extraction of a gate-level netlist from the layout. The universal logic gates of the proposed TVD-PB design, which have an identical circuit topology and physical layout, use only different threshold voltages to determine the logic function.

3. An anti-RE evaluation method is presented to obtain similar data of the gate layout using image processing technology. A normalized energy deviation (NED) and normalized standard deviation (NSD) technique are used to evaluate the security of anti-SCAs.

3 | THRESHOLD VOLTAGE-DEFINED POWER-BALANCE STRATEGY

We use the programmable switch that turns ON/OFF based on the voltage transistor (VT) asserted on it to implement the camouflaging technique (Figure 2a). The switch is realized using conventional NMOS transistors with the gate biased at the midpoint between nominal NMOS and PMOS threshold voltages: that is, \(0.5(V_{TN} + V_{TP})\) (Figure 2b). Therefore, the switch conducts when low VT (LVT) is assigned during manufacturing. This is because \(V_{GS} = 0.5(V_{TN} + V_{TP}) > LVT\). The switch stops conducting when high VT (HVT) is assigned \((V_{GS} < HVT)\). A good VT defined switch should offer high ON current and low OFF current. The gate voltage, HVT, LVT values, and transistor sizes are tuned to maximise the \(I_{ON}/I_{OFF}\) ratio. For an NMOS switch, higher HVT values and lower gate voltage are better for \(I_{OFF}\), whereas lower LVT and higher gate voltage are good for \(I_{ON}\). To achieve an antiphysical attack for IoT devices, a TVD-PB is proposed. It prevents the image processing-based extraction of a gate-level netlist from the layout by reducing the relation between power and data. The proposed TVD-PB circuit design consists of a sense amplifier, a differential pull-down network, precharge transistors, an evaluation transistor, and a discharge transistor, as shown in Figure 3. The proposed circuit’s operation is controlled using two differential current paths \((I_1, I_2)\). The left and right input signals of the transistor are symmetrical, and different thresholds are used to generate a current difference \((\Delta I > 0 \text{ or } < 0)\). Under the precharge voltage, the LVT generates a strong current, whereas the high-voltage transistors (HVT) generate a weak current. The unbalanced current determines the final output of the circuit. For example, if \(I_1 > I_2\), the output \(\overline{out} = 1\) rises to \(V_{DD}\), and \(\overline{eval} = 0\) pulls down to \(V_{SS}\).

The timing operation of the proposed TVD-PB logic circuit is shown in Figure 4. First, the test circuit is charged to \(V_{DD}\) with the control signals \(charge\), \(discharge\), and \(eval\) set to low. After a delay, as \(charge\) and \(eval\) are pulled high and the...
**FIGURE 2** (a) Voltage transistor programmable switch. High-voltage transistor (HVT): OFF, low-voltage transistor (LVT): ON. (b) Drawing of I-V curves of NVT, HVT, and LVT transistors. NVT, normal-threshold voltage transistors

**FIGURE 3** Proposed threshold voltage-defined power-balance circuit design

discharge remains uncharged, the circuit continues in an evaluation phase. Furthermore, the circuit performs logic operations to obtain the correct output value. Finally, when the signal eval is set to a low logic and the signal discharge is set to a high logic, the operational logic remains in the discharge phase. The circuit discharges to $V_{GS}$ and prepares for the next logic operation. The proposed logic camouflaging circuit that uses a threshold voltage-defined technique can configure into eight different logic functions. Hence, this approach hides the true nature of the circuit to an adversary. In addition, power dependency against power attacks has been improved effectively by balancing power consumption. The TVD logic gate [27] is based on SABL, which uses a strong-arm flip-flop topology. It replaces the input differential pair with a differential pull-down network determined by the logic function desired. Hence, the TVD logic circuit is vulnerable to SCA attacks.

**FIGURE 4** Proposed threshold voltage-defined power-balance timing operation

However, the proposed TVD-PB circuit with an additional discharge phase achieves logic insensitive to unbalanced routing capacitance. The experimental results show that power consumption is almost constant from cycle to cycle [28, 29]. This drastically reduces the need to balance the output load, because each output transits every cycle. Hence, the main difference between the proposed TVD-PB and baseline TVD is that the proposed TVB-PB technique can balance the power under unbalanced load capacitances.

### 4 ARCHITECTURE OF THRESHOLD VOLTAGEN-DEFINED POWER-BALANCE UNIVERSAL GATES AND MULTIPLIER

#### 4.1 Threshold voltage-defined power-balance universal gates

A schematic diagram of the two-input TVD-PB XOR logic gate is shown in Figure 5a. Unlike conventional CMOS gates, the circuit operation is divided into three phases: precharging, evaluation, and discharging. During the precharge phase, the control signals charge, discharge and eval are set to low, transistors P1, P2, P5 are turned on, and the out and out nodes are charged to $V_{DD}$. Because both the signal eval and charge have a high logic, the circuit enters the evaluation phase, in which transistors P2 and P5 are turned off and transistor N21 is turned on. At this time, if the input combination $AB = 11$, and transistors N5, N6, N19, and N20 in the pull-down network are turned on, the gate voltages of transistors N2 and N3 are charged to a high level. Thus, the two branches have currents $I_1$ and $I_2$ flowing through, and $I_1 < I_2$ because N5 and N6 are LVTs. When the sense amplifier amplifies the current difference, the signal out quickly becomes low. The transistor P4 will be turned on. The signal out makes a small dip and remains high. When the signal eval is set to low logic and the signal discharge is set to high logic, the logic is set to be at discharge phase, in which transistor N21 is turned off, both
transistors N1 and N4 are turned on, and both signal \( \overline{out} \) and \( out \) are discharged to \( V_{ss} \). Hence, the working cycle realizes XOR logic functions.

Figure 5b–d illustrates the NAND/AND, NOR/OR and INV/BUFF gates. Compared with the XOR, they are identical except for the configuration of the high- and low-threshold transistors in the differential pull-down network. Therefore, the mode of the operation of the TVD-PB NAND, NOR and INV circuits follows the TVD-PB XOR circuit.

The layout of the TVD-PB XOR circuit after full customisation is shown in Figure 6. It uses two layers of metal (M1 and M2) wiring, in which M1 is used for internal signal interconnection and power supply wiring (line width of 90 nm) and M2 is a part of the internal signal connection (line width of 100 nm). In addition, the layout area is reduced by minimising the size, layout symmetry, source-drain sharing, and power sharing. Finally, the area of the proposed TVD-PB logic camouflaging circuit is \( 6.595 \times 1.8 \mu m^2 \). Table 1 shows
the configuration of the HVTs and LVTs for different gate circuits. The layout of the TVD-PB XOR, NAND, and NOR is the same. Moreover, the layout of the VTL_N and VTH_N layers can be realized by configuring the threshold VTs. Owing to a certain layout, it can effectively prevent RE attacks.

4.2 Threshold voltage-defined power balance–based multiplier circuit

Figure 8 shows a 4 × 4-bit array multiplier. The proposed multiplier circuit includes 16 multiplications (MULs) and several inverters and buffers, and operates with a supply voltage of 1.2 V implemented in each logical gate to characterise the worst-case delay and power consumption. The structure circuit of MUL is as shown in Figure 7, which consists of a TVD-PB NAND gate and a full adder. The multipliers were implemented using the previously described universal gates, as well as full adders designed in each logic family. An array multiplier not only implements a regular layout structure, which makes it particularly suitable for VLSI implementations, it constructs a longer critical path delay and consumes a greater amount of power compared with other multipliers such as a carry-save multiplier, Wallace-tree multiplier, and Booth multiplier. The propagation delay is measured on the critical path, which is between the signal eval of the input and the most significant bit of the multiplier output. The layout of the multiplier is fully customised using a TSMC 65-nm multi-threshold CMOS process. Figure 8 shows the layout of a 4 × 4-bit multiplier with a core area of 110 × 20 µm². Four metal layers (M1, M2, M3, and M4) were selected, among which M1, M2, and M3 are used for internal signal interconnection, whereas M3 and M4 are used for the power supply ring.

The design of the TVD-PB standard cell is applied to the s-box measurement circuit, and the corresponding physical database needs to be built. As shown in Figure 9, the process [30] involves three phases: (a) Stage I: This stage is mainly focussed on creating the timing library for the logic synthesis of the circuit. Stage II: To recognise the layout information of the standard cell by the ICC tools, the LEF file is extracted through the Abstract Generator tool. Taking the standard cell as an example, physical information extraction of the layout is completed by three steps: Pin Step, Extract and Abstract. Stage III: This stage gives the key flow of converting LEF to the Milkyway format physical library. (b) Based on the unit, we
Thirteen-six I/O pads, consisting of 21 signal pads and 15 power supply pads, are in a mould. To test the chip's function automatically, a test platform was built, as shown in Figure 12. The test platform consists of a PC, Altera DE2-115 FPGA Development Board, Keysight E3649A dual-output DC power supply, a Fluke 8845A digit precision multimeter, a Keysight 33600A series waveform generator, a Rigol DSO9064C digital oscilloscope, and others.

An FPGA is used to generate test vectors, and the oscilloscope is used to observe the output waveform. Figure 13 shows the functional test waveform of gate circuits, such as TVD-PB XOR, NAND, and NOR. Figure 14 shows a functional test waveform of an MUL circuit with eight cycles, where X and Y are the inputs of the MUL, and Z is the product output. Therefore, these test results indicate that the proposed circuit has a correct logic function.

5 | RESULTS AND DISCUSSION

A multiplier test chip was fabricated using a TSMC 65-nm low-power CMOS process. The test chip consists of a TVD-PB multiplier, PADS, DFFs, and a parallel-to-serial circuit. The characteristics of the manufactured chip are summarised in Figure 11. Five-six I/O pads, consisting of 21 signal pads and 15 power supply pads, are in a mould. To test the chip's function automatically, a test platform was built, as shown in Figure 12. The test platform consists of a PC, Altera DE2-115 FPGA Development Board, Keysight E3649A dual-output DC power supply, a Fluke 8845A digit precision multimeter, a Keysight 33600A series waveform generator, and others.

An FPGA is used to generate test vectors, and the oscilloscope is used to observe the output waveform. Figure 13 shows the functional test waveform of gate circuits, such as TVD-PB XOR, NAND, and NOR. Figure 14 shows a functional test waveform of an MUL circuit with eight cycles, where X and Y are the inputs of the MUL, and Z is the product output. Therefore, these test results indicate that the proposed circuit has a correct logic function.

5.1 | Characterisation of power consumption

Characterisation of power consumption is equivalent to the case of the current based on a constant supply voltage. In this section, the TVD-PB XOR current curve was taken as a case study for analysis. As shown in Figure 15a, the TVD-PB XOR unit circuit generates three spike pulses in three working phases, where the current generated by the discharge is the largest and the generated power consumption is the largest. Moreover, each current static XOR gate evaluation will be different based on different input signals. Generally, the
circuit’s resistance to differential power analysis (DPA) attacks can be reflected based on the difference of circuit power consumptions in different clock cycles. As can be seen from Figure 15b, the power consumption of the static XOR gate depends on the input signal, and different input signals will generate different amounts of power consumption. However, the proposed TVD-PB logic camouflaging circuit has the same power consumption curve in different clock cycles without considering the input signal, and it has the power consumption characteristics independent of the input signal, which can be effectively used to resist DPA attacks.

Table 2 compares the proposed TVD-PB technique with other works. Delay of the proposed TVD-PB gate outperforms the PMP-TVD [31]. More power consumption is consumed owing to the additional introduction of the discharge phase.

Power consumption and the frequency of the MUL chip are measured at different voltages and temperatures. Figure 16 shows that the minimum operating voltage of the test chip is 1.0 V, the total power consumption of the chip is 0.308 mW, and the leakage power consumption is 0.0825 mW. As the voltage increases, the proportion of leakage power to total power also increases. At $V_{DD} = 1.8$ V, the maximum frequency and power consumption are 389 MHz and 1.140 mW, respectively, and the leakage power consumption is 0.653 mW.

Figure 17 shows the energy consumption diagram of the test chip. The figure shows that as the power supply voltage increases, the dynamic energy consumption gradually decreases. As the integration of static power becomes longer, static energy consumption replaces dynamic energy consumption and becomes the main energy consumption. The best energy efficiency point of the test chip is 1.1 V, and the minimum energy consumption at this time is 1.99 pJ.

Figure 18 shows the frequency and power consumption test results at different temperatures. The change in total power consumption is not obvious and the leak in power consumption increases with the temperature. From the energy in Figure 19, all energy consumption increases with an increase in
temperature, mainly because the delay of the chip increases with an increase in temperature, and the power integration time becomes ever longer.

5.2 | Characterisation of reliability

Operation of the TVD-PB logic is based on the threshold voltage of the transistors in the differential pull-down network. Therefore, the correct logic operation of the TVD-PB logic gate must be guaranteed in the event of process variations, particularly threshold voltage variations. To evaluate the robustness of the TVD-PB logic to process variations, 5000 samples Monte Carlo (MC) simulations were performed on TVD-PB XOR, and the gate functionality was verified for every possible input combination. The earlier analysis shows that $I_1 - I_2$ ($\Delta I$) determines the final signal output ($out$) is high when $\Delta I > 0$; otherwise, it is low. Therefore, MC simulations are performed to determine the effect of process variability on $\Delta I$ at the gate output. First, the $\Delta I$ that determines the gate output was calculated, and then the distribution of $\Delta I$ in all MC simulations was analysed. If $out$ is high (low) for a particular input combination, $\Delta I > 0$ ($<0$) will ensure the correct output. Therefore, this study uses the $\Delta I$ value $3\sigma$ of the distribution.
mean to determine the robustness of the TVD-PB logic in terms of current. As shown in Figure 20, the TVD-PB logic is fully functional and robust for process variations, with current margins above 55 μA for all possible input combinations. To evaluate the influence of environmental change factors on the TVD-PB logic operation, a noise margin simulation was performed on the TVD-PB XOR gate, and the frequency, temperature and voltage scan was performed in the noise analysis. According to the noise simulation, the TVD-PB circuit is similar to the noise margin of a static CMOS standard cell. Therefore, we contend that TVD-PB logic gates are as reliable as their static CMOS standard cell counterparts in terms of the input noise margin.

5.3 | Security analysis

The TVD-PB camouflaging unit circuit implements different logic functions through different configurations of HVTs and LVTs in a differential pull-down network. Therefore, a similarity index is proposed to characterise the security performance of the camouflaged unit circuit layout. In the similarity calculation, the image is converted into a corresponding identity according to its format, and the degree of similarity of the image is determined by comparing the identification. The grey histogram is one of the most used algorithms. The grey histogram of the image represents the grey distribution of the image, reflecting the relation between the frequencies of the pixels of each grey level. As shown in Figure 21, MATLAB software is used to calculate the grey values of the layout among XOR, NAND and NOR, and these three-histogram data almost completely coincide. The average similarity of the three gate layouts is as high as 99.87%. Hence, it is difficult for the attacker to obtain the gate-level netlist by reverse-engineering a GDSII layout file. The proposed TVD-PB logic circuit can effectively prevent both RE attacks. In addition, an important problem is the portion of the circuit that would be replaced with this family. In this work, we use an interference graph method [7] to drive the selection of replaced gates.

The fabricated chips were tested for power consumption, as depicted in Figure 22. The tested power of the circuit includes the multiplier core and some signal buffers. As can be seen in Figure 22, the multiplier maintains good power consumption for a period of time with almost no difference. For conventional multipliers and traditional multipliers, power consumption depends on the input signal, and different input signals will produce different power consumption. The TVD-PB logic camouflaging circuit designed here has the same power consumption curve in different clock cycles regardless of the input signal; its power consumption is independent of characteristics of the input signal, and thus it can effectively resist DPA attacks.

The simulation results of the DPA attack are shown in Figure 23. The proposed method is evaluated using a DPA attack on an 8-bit SBOX circuit used by an AES-128 cryptographic algorithm. The test circuit was constructed in a Cadence Virtuoso environment using both CMOS and TVD-PB logic styles. The Figure 23a shows that when a CMOS implementation is used, for the correct key guess (161)10, the correlation is close to unity (0.75). In contrast to the CMOS implementation, when implementing the test circuit using TVD-PB logic gates, the correct key showed a low correlation coefficient, as displayed in Figure 23b.

To assess the dependence between data and energy consumption, NED and NSD are generally used to measure the performance of the circuit's resistance to DPA attacks, as defined by Equations (1) and (2):

\[
NED = \frac{E_{\text{max}} - E_{\text{min}}}{E_{\text{max}}} \tag{1}
\]

\[
NSD = \frac{\sigma_E}{E} \tag{2}
\]

where \(E\) is the energy consumed by the circuit in a single clock cycle, as defined by Equation (3):
where $E_{\text{max}}$ is the maximum energy consumption of the circuit in different clock cycles, $E_{\text{min}}$ is the minimum power consumption of the circuit in different clock cycles, and $E$ is the average power consumption of the circuit over multiple clock cycles, as defined by Equation (4):

$$E = V_{DD} \int_0^T I_{DD}(t) dt$$

$$E = \left( \frac{\sum E_i}{n} \right)$$

**Figure 20** Distribution of current difference between the two differential branches for a threshold voltage-defined power-balance XOR logic gate: (a) $AB = 00$, (b) $AB = 01$, (c) $AB = 10$, (d) $AB = 11$.

**Figure 21** Threshold voltage-defined power-balance XOR-NAND-NOR histogram data.
\( \sigma_E \) is the standard deviation between the energy consumption of circuits with different clock cycles, as defined by Equation (5):

\[
\sigma_E = \sqrt{\frac{\sum_{i=1}^{n} (E_i - \bar{E})}{n}}
\]

Table 3 compares TVD-PB gates in terms of independent energy performance, overhead, and security against other previously proposed circuit structures. The NED of the TVD-PB XOR logic camouflaged circuit is less than 0.01%, and the NSD is less than 0.01%. Compared with the state of the art, the NED and NSD are effectively reduced by 1.29% and 0.42%, respectively. The proposed circuit improves resistance to the SCA performance.

6 | CONCLUSION

Based on the power consumption balance and threshold voltage-defined techniques, a novel TVD-PB circuit design is proposed. The proposed camouflaging circuit uses a threshold voltage-defined technique to configure itself to eight different logic functions, thereby hiding the true nature of the circuit from the adversary. In addition, by balancing power consumption, power dependency against power attacks has been improved effectively. The proposed TVD-PB circuit was fabricated using a TSMC 65-nm CMOS low-power process. The area of the test chip is 0.0044 mm², the delay is 0.45 ns, and average power consumption is 0.455 mW under the conditions of a 1.2-V supply and 27°C with 0.03% NED and 0.01% NSD. The average similarity of the TVD-PB universal gates is 99.68%, which ensures complete function and robustness with a current margin exceeding 55 µA. The designed circuit can effectively resist RE and DPA attacks. To present its feasibility in practical applications, area and power consumption are further investigated. The layout of the proposed circuits is full-custom design. Therefore, large-scale

| Reference | Normalized energy deviation (%) | Normalized standard deviation (%) | Reverse engineering | Side-channel analysis | Delay | Power | Transistors |
|-----------|---------------------------------|----------------------------------|---------------------|---------------------|-------|-------|------------|
| ST        | 47.11                           | 21.80                            | No                  | No                  | 1×    | 1×    | 12         |
| DDPL [34] | 0.50                            | 0.20                             | No                  | Yes                 | 0.9×  | 7.2×  | 16         |
| CSSAL [35]| 0.92                            | 0.32                             | No                  | Yes                 | 1.2×  | 0.7×  | 21         |
| SQAL [32] | 0.07                            | 0.01                             | No                  | Yes                 | 0.9×  | 0.2×  | 9          |
| EE-SPFAL [33]| 0.01                          | 0.05                             | No                  | Yes                 | 0.6×  | 0.3×  | 12         |
| Sense amplifier-based logic [22]| 2.63                          | 0.56                             | No                  | Yes                 | 1.6×  | 0.7×  | 18         |
| TDPL [28] | 0.50                            | 0.20                             | No                  | Yes                 | 1.4×  | 4.9×  | 16         |
| Threshold voltage-defined [27]| 1.25                            | 0.32                             | Yes                 | Yes                 | 1.7×  | 1.1×  | 31         |
| PMP-threshold voltage-defined [31]| 1.32                          | 0.43                             | Yes                 | Yes                 | 3.4×  | 1.8×  | 39         |
| This work | 0.03                            | 0.01                             | Yes                 | Yes                 | 1.9×  | 3.4×  | 26         |

*In the table, ST respectively represents TSMC 65 nm Library_LP STD_Cell tcb65gplus_200a XOR2D0.
integration is limited to electronic design automation tools. In future work, design atomisation of the TVD-PB logic gates will be investigated for IoT devices. Moreover, lightweight TVD-PB methods are expected to be developed to provide low-cost hardware security schemes.

ACKNOWLEDGEMENTS
This work was supported by the National Natural Science Foundation of China (Nos. 61871244 and 61871078); the Zhejiang Provincial Natural Science Foundation of China (No. L Y18F040002); China Postdoctoral Science Foundation Funded Project No. 2019M661357; State Key Laboratory of ASIC and System Foundation of Fudan University (No. 2019KF002); the K. C. Wong Magna Fund in Ningbo University, China; and the Fresh Talent Programme for Science and Technology Department of Zhejiang Province (No. 2019R405072).

ORCID
Liang Wen https://orcid.org/0000-0001-5490-4943
Chongyan Gu https://orcid.org/0000-0002-3028-8004

REFERENCES
1. Wu, N., et al: IoT-based smart and complex systems: a guest editorial report. IEEE/CAA J. Autom. Sinica. 5(1), 69–73 (2018)
2. Xu, W., et al: Internet of vehicles in big data era. IEEE/CAA J. Autom. Sinica. 5(1), 19–35 (2018)
3. Stengou, C., et al: Secure integration of IoT and cloud computing. Future Gener. Comput. Syst. 78, 964–975 (2018)
4. Hassija, V., et al: A survey on IoT security: application areas, security threats, and solution architectures. IEEE Access. 7, 2109–3536 (2019)
5. Futstaei, M., et al: Evaluating critical security issues of the IoT world: present and future challenges. IEEE Internet Things J. 5(4), 2483–2495 (2018)
6. Zhou, W., et al: The effect of IoT new features on security and privacy: new threats, existing solutions, and challenges yet to be solved. IEEE Internet Things J. 6(2), 1606–1616 (2019)
7. Li, L., Wang, P., Zhang, Y: Design of anti-key leakage camouflage gate circuit for reverse engineering based on dummy vias. Microelectron. J. 90, 163–168 (2019)
8. Gomez, H., Duran, C., Roa, E: Defeating silicon reverse engineering using a layout-level standard cell camouflage. IEEE Trans. Consum. Electron. 65(1), 109–118 (2019)
9. Singh, A., et al: Improved power/EM side-channel attack resistance of 128-bit AES engines with random fast voltage dithering. IEEE J. Solid-State Circuits. 54(2), 569–583 (2019)
10. Bellizia, D., Scotti, G., Trifiletti, A: TEL logic style as a counter measure against side-channel attacks: secure cells library in 65nm CMOS and experimental results. IEEE Trans. Circuits Syst. 1 Reg. Pap. 65(11), 3874–3884 (2018)
11. Kumar, S.D., Thapliyal, H., Mohammad, A: FinSal: FinFET-based secure adiabatic logic for energy-efficient and DPA resistant IoT devices. IEEE Trans. Comput. Aided Design. Circuits Syst. 37(1), 110–122 (2018)
12. Wieringa, R., Daneva, M: Six strategies for generalising software engineering theories. Sci. Comput. Program. 101, 136–152 (2015)
13. Rajendran, J., et al: Security analysis of integrated circuit camouflage. In: Proc. ACM CCS, Berlin, Germany, pp. 709–720 (2013)
14. Roy, J.A., Koushanfar, F, Markov, L.L: Ending piracy of integrated circuits. Computer. 43(10), 30–38 (2010)
15. Rajendran, J., et al: Fault analysis-based logic encryption. IEEE Trans. Comput. 64(2), 410–424 (2015)
16. Chen, M., et al: Hardware protection via logic locking test points. IEEE Trans. Comput. Aided Design Integr. Circuits Syst. 37(2), 3020–3030 (2018)
17. Dohe, J., Yu, Q: Novel dynamic state-deflection method for gate-level design obfuscation. IEEE Trans. Comput. Aided Des. Integr. Circuits Syst. 37(2), 273–285 (2018)
18. Koteswarar, S., Kim, C.H., Parhi, K.K: Key-based dynamic functional obfuscation of integrated circuits using Sequentially Triggered mode-based design. IEEE Trans. Inf. Forensics Secur. 13(1), 79–93 (2018)
19. Sengupta, A., Rathor, M: Protecting DSP kernels using robust hologram-based obfuscation. IEEE Trans. Consum. Electron. 65(1), 99–108 (2019)
20. Chen, Z., et al: Towards FPGAs security in IoT: a new detection technique for hardware trojans. IEEE Internet Things J. 6(4), 7061–7068 (2019)
21. Kokila, J., Ramaabramaniam, N., Naganathan, N: Resource efficient metering scheme for protecting SoC FPGA device and its in IoT applications. IEEE Trans. VLSI Syst. 27(10), 2284–2295 (2019)
22. Tiri, K., Aalami, M, Verbauwhede, I: A dynamic and differential CMOS logic with signal independent power consumption to withstand differential power analysis on smart cards. Proc. 28th Eur. Solid-State Circuits Conf. (ESSC), Florence, Italy, 403–406 (2002)
23. Hwang, D.D., et al: AES-based secure coprocessor IC in 0.18-μm CMOS with resistance to differential power analysis side-channel attacks. IEEE J. Solid-State Circuits. 41(4), 781–792 (2006)
24. Avital, M., et al: Randomized multipolarity logic against differential power analysis. IEEE Trans. VLSI Syst. 23(4), 702–711 (2015)
25. Chipworks: Intel’s 22nm tri-gate transistors exposed. (2012) http://www.chipworks.com/blog/technologyblog/2012/04/23/intels-22nm-trigate-transistors-exposed/
26. TAEUS. http://www.taues.com/taeus-services/ip-litigation-services/reverse-engineering/
27. Erbagci, B., et al: A secure camouflaged threshold voltage defined logic family. In: IEEE International Symposium on Hardware Oriented Security and Trust (HOST), McLean, USA, pp. 229–235 (2016)
28. Bucci, M., et al: A flip-flop for the DPA resistant three-phase dual-rail pre-charge logic family. IEEE VLSI Syst. 20(11), 2122–2132 (2012)
29. Akkaya, N.E.C., et al: A DPA-resistant self-timed three-phase dual-rail pre-charge logic family. In: IEEE International Symposium on Hardware Oriented Security and Trust (HOST), Washington, USA, pp. 112–117 (2015)
30. Hevner, Alan R., et al: Design science in information systems research. MIS Q. 28(1), 75–105
31. Akkaya, N. E. C., Erbagci, B., Mai, K: A secure camouflaged logic family using post-manufacturing programming with a 3.6GHz adder prototype in 65nm CMOS at 1V nominal VDD. In: IEEE Int. Solid-State Circuits Conf. (ISSCC), San Francisco, USA, pp. 128–130 (2018)
32. Avital, M., et al: DPA-secured quasi-adiabatic logic (SQAL) for low-power passive RFID tags employing S-boxes. IEEE Trans. Circuits Syst. I. 62(1), 149–156 (2015)
33. Kumar, S.D., Thapliyal, H., Mohammad, A: EE-SPEAL: a novel energy-efficient secure positive feedback adiabatic logic for DPA resistant RFID and smart cards. IEEE Trans. Emerg. Topics Comput. 7(2), 281–293 (2019)
34. Bucci, M., et al: Delay-based dual-rail precharge logic. IEEE Trans. VLSI Syst. 19(7), 1147–1153 (2011)
35. Monteiro, C., Takahashi, Y, Sekine, T: Charge-sharing symmetric adiabatic logic in countermeasure against power analysis attacks at cell level. Microelectron J. 44(6), 496–503 (2013)

How to cite this article: Zhang Y, Wu Q, Wang P, Wen I, Luan Z, Gu C. TVD-PB logic circuit based on camouflaging circuit for IoT security. IET Circuits Devices Syst. 2021;1–13. https://doi.org/10.1049/cds.2.12080