Emerging tunnel FET and spintronics-based hardware-secure circuit design with ultra-low energy consumption

Aditya Japa1 · Subhendu K. Sahoo2 · Ramesh Vaddi3 · Manoj Kumar Majumder4

Received: 29 December 2020 / Accepted: 26 September 2022 / Published online: 10 November 2022
© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2022

Abstract

Present complementary metal–oxide–semiconductor (CMOS) technology with scaled channel lengths exhibits higher energy consumption in designing secure electronic circuits against hardware vulnerabilities and breaches. Specifically, CMOS sense amplifier-based secure differential power analysis (DPA) countermeasures at scaled channel lengths show large energy consumption, with increased vulnerability. Additionally, spin-transfer torque magnetic tunnel junction (STT-MTJ) and CMOS-based logic-in-memory (LiM) cells demonstrate high energy consumption due to the large write current requirement of the STT-MTJ and poor MOS device performance at scaled channel lengths. This paper for the first time leverages emerging tunnel field effect transistor (TFET) steep-slope device characteristics and compatible non-volatile STT-MTJ devices for enhanced hardware security with ultra-low energy consumption at lower supply voltages. TFET-based sense amplifier-based logic (SABL) gates are proposed that achieve 3× lower energy consumption than the Si FinFET SABL designs. Further, utilizing TFET SABL gates, a TFET PRIDE S-box is designed that exhibits higher DPA resilience with 3.2× lower energy consumption than the FinFET designs. With the resulting lower static power consumption, TFET SABL-based cryptosystems are thus less vulnerable to static power side-channel attacks. Additionally, the proposed STT-MTJ and TFET LiM gates achieve 4× lower energy consumption than the STT-MTJ and FinFET designs. Lastly, these gates are explored in a logic encryption/locking technique that shows 3.1× lower energy consumption than the STT-MTJ and FinFET-based design.

Keywords Tunnel FET (TFET) · Differential power analysis (DPA) · Sense amplifier-based logic (SABL) · Spin-transfer torque magnetic tunnel junction (STT-MTJ) · Logic-in-memory (LiM) · Logic encryption/locking

1 Introduction

Offshore manufacturing of integrated circuits (ICs) has increased the vulnerability to hardware security attacks in the modern Internet of Things (IoT) era [1, 2]. The National Institute of Standards and Technology, for example, has observed an exponential growth in hardware vulnerabilities in the last few years [3]. Moreover, the hardware-assisted security techniques and systems market is growing rapidly with efforts to prevent the counterfeiting of ICs [4]. Various hardware security attacks have been described in the literature, including hardware reverse engineering, counterfeiting of IC, and side-channel analysis (SCA). Among different hardware security attacks available, SCA is effective in recovering hidden secret information [5]. SCA utilizes side-channel signals such as power consumption, electromagnetic, and photonic signals to reveal the encryption keys of the cryptographic circuits/systems [6]. Differential power analysis (DPA) processes the power consumption...
information of the encryption engine and requires comparatively less effort in recovering secret key information [7]. Additionally, the static complementary metal–oxide–semiconductor (CMOS) logic style shows higher vulnerability to DPA attacks due to the data-dependent power consumption profile [8, 9]. To address this issue, several researchers have explored novel logic styles that show higher DPA resilience [10]. Sense amplifier-based logic (SABL), fin field effect transistor (FinFET)-based secure adiabatic logic (FinSAL), randomized multi-topology logic (RMTL), homogeneous dual-rail logic (HDRL), secure positive-feedback adiabatic logic, and differential symmetric pull-down network gates have been demonstrated to mitigate the data dependence on device power consumption [11–16]. Among the novel logic designs, the SABL style has been proven secure but faces several challenges including higher power and energy consumption overheads [11]. Moreover, at sub-50-nm channel lengths, CMOS SABL has exhibited higher static power consumption that revealed the confidential information against static power SCA [17]. To overcome this issue, emerging hyperFET devices have been leveraged for DPA-resilient SABL logic. However, this technique has exhibited 3x higher energy consumption than CMOS technology [18]. Thus, CMOS SABL logic has demonstrated inherent disadvantages that need to be addressed for DPA-resilient cryptographic circuits with ultra-low energy consumption.

On the other hand, the spin-transfer torque-based magnetic tunnel junction (STT-MTJ) has attracted wide attention due to its lower static power, non-volatility, and higher compatibility with CMOS technology [19, 20]. Moreover, integrating STT-MTJ and CMOS was found to provide flexibility for the construction of logic-in-memory (LiM) architectures for high-speed data transfer [21]. Several researchers have demonstrated logic gates and arithmetic circuits by exploring STT-MTJ-based LiM cells [22, 23]. However, STT-MTJ requires a relatively large write current to change the state, which demands maintaining higher supply voltages [24]. Additionally, CMOS technology scaling leads to serious problems including lower ON current, short-channel effects, high power density, and poor reliability [25]. Consequently, STT-MTJ-based LiM circuits exhibit large energy consumption due to the poor performance of MOS devices at scaled channel lengths (or supply voltages). Recent STT-MTJ LiM cell-based crypto circuits, for example, exhibited increased energy consumption [26].

The recently emerging tunnel FET (TFET), with its band-to-band tunneling mechanism, has exhibited steep-slope characteristics (lower subthreshold swing) and higher ON-/OFF-current ratio ($I_{ON}/I_{OFF}$) [27–29]. As a result, TFET-based digital, analog, and mixed signal circuits/systems can achieve higher energy efficiency at lower supply voltages [30, 31]. Apart from the low energy consumption and higher speed benefits, TFET devices with special characteristics have been leveraged to enhance hardware security [32]. TFET-based current mode logic and adiabatic logic have been proposed for DPA-resistant cryptosystems [33, 34]. TFET-based compact polymorphic logic gates were designed by exploring the onset of tunneling for both positive and negative gate bias [35]. The p-n forward current of the TFET was explored as a favorable feature to design a true random number generator and low area overhead DPA countermeasure [36, 37]. Thus, at scaled supply voltages, emerging TFET devices have been utilized to enhance the hardware security of electronic systems [38]. Therefore, this work leverages TFET device characteristics for hardware security techniques that exhibit lower energy consumption. SABL logic gates were designed by exploring TFET devices to reduce energy consumption. The proposed TFET SABL gates are applied to design the PRIDE substitution box (S-box). DPA attack is performed on the proposed TFET SABL-based S-box, and the performance is also benchmarked with the baseline Si FinFET designs. Additionally, STT-MTJ and TFET-based LiM gates are proposed to reduce the energy consumption. These designs are also benchmarked with STT-MTJ and FinFET-based LiM gates. Moreover, the proposed LiM gates are utilized in logic encryption/locking to obtain enhanced hardware security with ultra-low energy consumption.

The rest of the paper is organized as follows: Section 1 demonstrates the state of the art and the motivation of the proposed work. Section 2 presents the device characteristics of the TFET and STT-MTJ that are explored for circuit design. Section 3 demonstrates TFET SABL-based logic gates and S-box design for DPA analysis. Further, these TFET SABL designs are benchmarked with FinFET designs. Section 4 presents STT-MTJ and TFET-based LiM gates and logic encryption/locking technique. The performance of the STT-MTJ and TFET-based logic encryption circuit is then compared with STT-MTJ and FinFET designs. The fabrication compatibility of the TFET and STT-MTJ technologies is also discussed in this section. Finally, conclusions are drawn in Sect. 5.

## 2 Device characteristics

This section presents device characteristics and Verilog-A models of TFET and STT-MTJ that are required for circuit design. The motivation to introduce TFET into SABL logic and STT-MTJ LiM circuits is also discussed.

### 2.1 TFET technology

TFET devices work based on a band-to-band tunneling mechanism and exhibit a high ON-/OFF-current ratio. Several TFET devices have experimentally demonstrated
lower subthreshold swing, i.e., below 60 mV/dec [28, 29]. This work explores lookup table (LUT)-based 20 nm InAs TFET Verilog-A models for circuit design [39]. The TFET-based circuits are benchmarked with equivalent LUT-based 20 nm Si FinFET designs [39]. The device architecture of the n-channel TFET (N-TFET) and n-channel Si-FinFET (N-FinFET) is shown in Fig. 1. Various device parameters considered in these models are shown in Table 1. TFET and FinFET symbols were created by calling Verilog-A models into the industry-standard Cadence tool. Later, circuits were designed using the device symbols. Figure 2 shows the $I_D-V_{GS}$ characteristics of both N-TFET and N-FinFET by varying the gate-to-source voltage ($V_{GS}$) from 0 to 0.4 V. Initially, when the N-TFET switches OFF, it shows a 2× lower OFF current than the N-FinFET. With sufficiently positive $V_{GS}$ voltage, the N-TFET switches ON, and current through the N-TFET increases abruptly due to the band-to-band tunneling mechanism. It can be observed from Fig. 2a that the N-TFET shows 3.4× and 1.23× higher ON current of 0.3 and 0.4 V at $V_{GS}$, respectively. Further, the N-TFET exhibits lower subthreshold swing (30 mV/dec) than the N-FinFET device, as shown in Fig. 2b. Therefore, it can be concluded that the N-TFET exhibits an abrupt transition from the OFF state to the ON state (steep slope characteristics). TFET-based circuits also achieve lower energy consumption due to the high ON/OFF-current ratio.

It was recently revealed that SABL circuits become secure against DPA with the abrupt transition from the pre-charge to the evaluation phase [18]. This behavior requires abrupt transitions in the device characteristics that are used for circuit design. However, the introduction of emerging steep-slope hyperFET devices in SABL-based cryptosystems exhibited 3× higher energy consumption than CMOS-based designs [18]. To reduce this energy consumption, this paper introduces steep-slope TFET devices in SABL circuits that can achieve ultra-low energy consumption with enhanced security assurance.

### 2.2 STT-MTJ device characteristics

A magnetic tunnel junction (MTJ) is a nano-stacked structure that consists of two ferromagnetic (FM) layers, separated by a thin oxide layer as shown in Fig. 3 [19]. Between the two FM layers, the magnetic orientation of one layer is fixed, called the reference layer, while the magnetic orientation of the other layer varies in the same or opposite direction to that of the reference layer, and is called the free layer. Upon providing sufficient current through the MTJ, the magnetic orientation of the free layer and reference layer point in the same direction, the MTJ exhibits lower resistance ($R_P$), which is called the parallel state. On the other hand, if the magnetic orientation of the free layer and reference layer point in opposite directions, the MTJ exhibits higher resistance ($R_{AP}$), called the antiparallel state. Due to the nonmagnetic layer, the MTJ exhibits variation in resistance, which is defined as tunnel magnetoresistance (TMR) (Eq. 1). The MTJ should exhibit high TMR for faithful reproduction of the stored value.

$$TMR = \frac{R_{AP} - R_P}{R_P}$$  \hspace{1cm} (1)

Among several switching mechanisms available, STT switching exhibits a high TMR suitable for commercialized MTJs [20]. The perpendicular STT-MTJ devices eliminate several challenges exhibited by in-plane devices. As a result, perpendicular STT-MTJ devices have attracted wide attention. This work explores a compact Verilog-A model of CoFeB/MgO perpendicular magnetic anisotropy STT-MTJ [21, 40]. The STT-MTJ described in this model is designed using two FM layers made of CoFeB and a thin oxide layer made of MgO. This model is compatible with an industry-standard Cadence environment, and the parameters used are listed in Table 2. Therefore, the STT-MTJ model is plugged, and the circuits are designed and analyzed.

| Table 1 Device parameters of the InAs TFET and FinFET [30, 39] |
|---------------------------------------------------------------|
| **TFET parameters**                                          |
| Channel length                                               | 20 nm |
| Effective oxide thickness (EOT)                              | 0.7 nm |
| Channel thickness ($T_{ch}$)                                 | 5 nm  |
| Source doping (InAs)                                         | $4 \times 10^{19}$ cm$^{-3}$ |
| Drain doping (InAs)                                          | $6 \times 10^{17}$ cm$^{-3}$ |
| **FinFET Parameters**                                        |
| Channel length                                               | 20 nm |
| Effective oxide thickness (EOT)                              | 0.7 nm |
| Fin width ($W_{Fin}$)                                        | 8 nm  |
| Fin height ($H_{Fin}$)                                       | 25 nm |
| Source/drain doping                                          | $1 \times 10^{20}$ cm$^{-3}$ |

### Fig. 1 Device architectures of a N-TFET, b N-FinFET
The STT-MTJ requires a relatively large write current to change the state (high to low or low to high), which requires higher supply voltage. At scaled channel lengths (scaled supply voltages), MOS devices exhibit lower ON current. As a result, the STT-MTJ exhibits a higher propagation delay to change the state, or the state cannot be changed. Thus, STT-MTJ-based LiM cells exhibit higher energy consumption [25]. To reduce energy consumption, this work explores TFET devices (with higher ON current and lower subthreshold swing) in STT-MTJ-based LiM circuits. TFET and STT-MTJ-based LiM circuits are also explored for logic encryption/locking techniques.

### 3 Energy-efficient and secure TFET SABL-based crypto circuits

This section demonstrates TFET-based SABL gate design and analysis. Additionally, a PRIDE S-box is designed and evaluated by performing a DPA attack on it. The energy consumption of the TFET-based S-box design is also benchmarked with FinFET-based designs.

#### 3.1 TFET-based SABL logic

The proposed TFET SABL architecture that explores the TFET-based differential pull-down network (DPDN) is shown in Fig. 4. The logic gates based on this architecture work in the pre-charge and evaluation phase. In the pre-charge phase (clk = 0), transistors $T_1$ and $T_2$ switch ON, and $T_3$ switches OFF. Consequently, the outputs ($Y$, $Y_b$) discharge to the ground because of inverters. In the evaluation phase (clk = 1), transistor $T_3$ switches ON and connects the TFET DPDN to the ground. Depending upon the inputs applied to TFET-based DPDN, the outputs ($Y$, $Y_b$) of the SABL gates are evaluated. To explore the SABL architecture, TFET AND/NAND, OR/NOR, and XOR/NOR gates were designed. The logic gate designs corresponding to their TFET DPDN circuits are shown in Fig. 5, where $K_1$ and $K_2$ indicate the connection between the pull-up and pull-down networks.
example, consider the TFET XOR gate where input $B$ is at logic “1” and $B_b$ is at logic “0.” As input $A$ is at logic “0” and $A_b$ is at logic “1,” node $N_1$ demonstrates faster discharge (through transistor $T_2$ and $T_3$) than node $N_2$. As a result, the transistor $I_{P1}$ in the inverter design (in the pull-up network) switches ON, and output $Y_b$ discharges to the ground. When $Y_b$ discharges to the ground, $Y$ charges to supply voltage ($V_{DD}$). Figure 6 shows the transient characteristics of the TFET SABL gates at a supply voltage of 0.3 V. It can be observed that TFET SABL gates exhibit proper functionality at an ultra-low supply voltage of 0.3 V with frequency of 100 MHz. Table 3 presents a performance comparison of the TFET SABL logic gates and FinFET SABL gates at a supply voltage of 0.3 V. Due to the high $I_{ON}/I_{OFF}$ ratio, the TFET SABL gates exhibit lower propagation delay than the FinFET SABL logic gates. The TFET SABL gates also show relatively lower power consumption and achieve 3× lower energy consumption than the FinFET gates. Next, the static power consumption of the TFET SABL gates is calculated to test the vulnerability of the SABL gates to static power side-channel attacks. From Fig. 7, it can be observed that the TFET SABL gates achieve approximately 3× lower static power consumption than the FinFET-based SABL at a supply voltage of 0.3 V. Due to the lower static power consumption, the TFET SABL gates are robust against static power side-channel attacks. Therefore, it can be concluded that the TFET SABL gates exhibit better performance than the FinFET designs at lower supply voltages.

3.2 TFET SABL-based PRIDE S-box design

Here, a DPA attack is performed on the TFET SABL-based PRIDE S-box, and the performance of the TFET SABL PRIDE S-box is benchmarked with a FinFET design.

**DPA mechanism on 4-bit PRIDE S-box**

PRIDE is a block cipher based on substitution and permutation networks with a 64-bit input/output and 128-bit key for encryption [18]. The complete encryption of the PRIDE cipher is performed in 20 rounds. One round consists of
three main operations: XOR with round key, 4-bit parallel S-box operations followed by permutations, and linear operations. As it is widely accepted that the S-box is the most vulnerable part of a block cipher, this work considers the 4-bit PRIDE S-box to perform a DPA attack [18]. The 4-input and 4-output PRIDE S-box is a combinational block, and the relation between inputs and outputs is expressed as the Boolean Eqs. (2–5).

\[
y_3 = x_1 \oplus x_2 \cdot x_2 \\
y_2 = x_0 \oplus x_2 \cdot x_1 \\
y_1 = x_3 \oplus y_3 \cdot y_2 \\
y_0 = x_2 \oplus y_1 \cdot y_2
\]

The DPA attack is performed to retrieve the secret key information of the crypto engine. The adversary contains the cryptographic algorithm with the required input patterns to be applied. The DPA attack is performed on the PRIDE S-box design as shown in Fig. 8. Here, XOR operations (as simple encryption) are performed between randomly generated inputs (D) and a 4-bit key (K). This produces the output that is applied to the 4-bit S-box. Finally, the S-box produces output (Y) by performing a substitution operation. The detailed DPA attack mechanism is explained as follows (Fig. 8).

- Firstly, the S-box is designed using the Cadence Virtuoso environment, and the current traces (i_{vdd}) are recorded by applying random inputs (D) with a fixed key (K_i).
- The recorded current traces are sampled with a rate of T (T samples per trace) and arranged in a matrix S of size D \times T.
- In the next step, the S-box algorithm is implemented using Python 3, and the output values are calculated using inputs D (similar inputs as in the first step) and all possible keys K.
- The obtained output values are mapped to hypothetical power consumption values using a Hamming distance (HD) model and represented by a matrix H of dimensions D \times K. The HD of the two successive output values is calculated using Eq. (6).

\[
\text{HD} = \text{Hamming weight}(Y_i \oplus Y_{i-1})
\]

Finally, each column of the H matrix is correlated with all the columns of the current trace matrix S. This results in the correlation matrix (C) of dimensions K \times D. The correct key used for encryption will show the highest value of correlation compared with other keys.

### Security evaluation of TFET SABL-based PRIDE S-box

The PRIDE S-box circuit is designed using the proposed TFET SABL gates. The proposed TFET SABL-based PRIDE S-box is compared with the TFET-based static complementary PRIDE S-box to highlight the security benefits. Both designs are implemented using 20 nm InAs TFET technology. Each

| Gate | TFET | FinFET |
|------|------|--------|
| Power consumption (µW) | Propagation delay (ns) | Energy consumption (fJ) | Power consumption (µW) | Propagation delay (ns) | Energy consumption (fJ) |
| XOR | 1.1  | 0.5   | 0.55  | 1.13 | 2.1  | 2.373 |
| AND | 0.812 | 0.6   | 0.49  | 0.83 | 1.94 | 1.61 |
| OR  | 0.95  | 0.52  | 0.49  | 0.92 | 1.9  | 1.75  |

![Fig. 7 Static power consumption comparison of TFET SABL gates with FinFET designs](image)

![Fig. 8 Proposed TFET-based PRIDE S-box design](image)
design is individually simulated using 100 random inputs with a fixed key (K = 5). The power traces obtained from the TFET static and SABL-based S-box circuits are depicted in Fig. 9. It can be observed that the power traces of the TFET SABL-based S-box circuit are uniform compared with the TFET-based static complementary design. The obtained power traces are sampled with a rate of 1000 and arranged as a matrix S. The resulting power trace matrix S is correlated with the hypothetical power values matrix (H) by following the DPA mechanism. Figure 10a shows the resulting correlation coefficients of the TFET-based static complementary S-box design with all possible keys. It can be seen that the DPA attack performed on this design is successful and shows the highest correlation coefficient for the correct key (K = 5). However, the DPA attack performed on the TFET SABL-based S-box design is unsuccessful, as shown in Fig. 10b. The correlation coefficient of the wrong key (K = 12) is observed to be high compared with the original key (K = 5). Moreover, the correlation coefficient of the original key is hidden in the analysis result and cannot be observed by the adversary. This robustness is obtained from the favorable SABL structure and the sharp switching behavior of the TFET device.

**Performance benchmarking**

The performance of the TFET SABL-based S-box design is benchmarked with an equivalent FinFET SABL-based S-box design as shown in Table 4. At a supply voltage of 0.3 V, the TFET and FinFET-based designs show energy consumption of 13.09 fJ and 41.339 fJ, respectively. Thus, the TFET SABL-based S-box design exhibits 3.15× lower energy consumption than the FinFET design at a supply voltage of 0.3 V. Moreover, the static power consumption of the TFET SABL-based S-box design is observed to be 3.5× lower than that of the FinFET design. Therefore, the TFET SABL-based crypto circuits exhibit lower vulnerability to static power side-channel attacks.

### Table 4

| Parameter                   | TFET SABL-based S-box | FinFET SABL-based S-box |
|-----------------------------|------------------------|--------------------------|
| Power consumption (µW)      | 6.3                    | 6.7                      |
| Static power consumption (nW)| 17.53                  | 61.35                    |
| Propagation delay (ns)      | 2.12                   | 6.17                     |
| Energy consumption (fJ)     | 13.09                  | 41.339                   |

**4 STT-MTJ and TFET LiM cells for logic locking**

This section presents the STT-MTJ and TFET-based LiM gates and benchmarking with the STT-MTJ and FinFET-based designs. Further, these gates are applied to logic
locking/encryption, and the energy consumption is calculated. The fabrication compatibility and challenges of TFET and STT-MTJ are also discussed.

4.1 STT-MTJ and TFET LiM-based logic gates

The proposed STT-MTJ and TFET LiM cells are identical to SABL gates in which STT-MTJ devices are explored to store one-bit input, as shown in Fig. 11. This stored input can be accessed by a logic tree, and the final output of the LiM cell is produced with the help of a pre-charge sense amplifier. An additional writing circuit is used to write the data into STT-MTJ devices. The STT-MTJ and TFET LiM cell works in two phases that are similar to TFET SABL gates. When the clock signal is at logic 0 (clk = 0), the sense amplifier works in the pre-charge phase. In this phase, the logic tree is disconnected from the sense amplifier, and the transistors T1 and T2 switch ON. As a result, outputs Y and Yb of the cell discharge to logic 0. When the clock signal is at logic 1 (clk = 1), the sense amplifier works in the evaluation phase. In this phase, with the resistance difference between the MTJs, and depending upon the input, the charging/discharging speed of the two branches varies. As a result, the sense amplifier evaluates one output to be logic 1 and the other output to be logic 0.

Figure 12 shows the STT-MTJ and TFET-based AND/NAND, OR/NOR, and XOR/XNOR LiM gates corresponding to different logic tree structures, where K1 and K2 show the connection between pull-up and pull-down networks. More specifically, consider the XOR gate in which two MTJ devices are used to store the input B and its complement. For example, consider that MTJ1 (B is at logic 1) and MTJ2 (Bb is at logic 0) are in parallel and antiparallel configurations, respectively. Consequently, the resistance of MTJ1 is lower than that of MTJ2. With relatively lower resistance, the current through MTJ1 is greater than the MTJ2. As a result, the transistor IP2 in the inverter design (pull-up network) switches ON and output node N1 charges to VDD. As a result, Y and Yb result in ground and VDD, respectively. Figure 13 shows the transient characteristics of logic gates at a supply voltage of 0.3 V. From this, it can be observed that STT-MTJ and TFET-based logic gates exhibited proper...
functionality at low supply voltage. Figure 14 shows the energy consumption comparison of STT-MTJ and TFET-based logic gates with equivalent STT-MTJ and FinFET designs at a supply voltage of 0.3 V. The STT-MTJ and TFET-based gates achieved 4× lower energy consumption than the STT-MTJ and FinFET designs. With the higher ON current of the TFET devices, STT-MTJ exhibited a lower propagation delay in changing its state. As a result, the proposed LiM-based gates achieved lower energy consumption. These gates were further explored for energy-efficient logic encryption/locking applications.

4.2 STT-MTJ and TFET LiM cell-based logic locking

Logic locking is a hardware security technique that protects the circuit/design by adding key-based gates into the original design. Consequently, the circuit/system cannot provide proper functionality without the correct key input. Figure 15 shows a block diagram of conventional and proposed LiM-based logic locking in which both input and key will be provided to the design. The original functionality of the system can be achieved upon application of the correct key. In the conventional logic locking technique, a separate non-volatile memory is used to store the key bits. Recent research revealed that fetching the data from external memory results in a large energy overhead [19, 20]. To reduce the energy overhead, this paper explores STT-MTJ and TFET LiM cell-based logic locking, where the STT-MTJ and TFET LiM cells are used to store and process the data. For example, consider the IEEE International Symposium on Circuits and Systems (ISCAS) C17 benchmark (Fig. 16) that is explored for logic locking applications [41]. This design uses six two-input NAND gates wherein two NAND gates are designed using STT-MTJ and TFET LiM cells that are operated by key inputs \( K_1 \) and \( K_2 \) as shown in Fig. 16. As a result, the STT-MTJ stores key bits and the logic is processed using a TFET-based logic tree. The remaining four NAND gates are designed using TFET SABL-based NAND gates as shown in Fig. 16. The Out\(_1\) and Out\(_2\) of the ISCAS C17 circuit are expressed as Eqs. (7 and 8).
For example, the key bits $K_1K_2$ are fixed as 10, and Eqs. (7 and 8) are simplified as Eqs. (9 and 10)

$$Out_1 = A \cdot C + B \cdot \left(\frac{C \cdot K_1}{C} \right)$$ \hspace{1cm} (7)

$$Out_2 = \left(\frac{C \cdot K_1}{C} \right) \cdot (B + K_2)$$ \hspace{1cm} (8)

Figure 17 shows the transient characteristics of the proposed ISCAS C17-based circuit at a supply voltage of 0.3 V. With key bits of $K_1K_2 = 10$, the circuit shows correct functionality as expressed in Eqs. (9 and 10). The energy consumption of the STT-MTJ and TFET LiM cell-based C17 circuit is calculated at a supply voltage of 0.3 V. It can be observed that the STT-MTJ and TFET-based logic encryption circuit achieves lower energy consumption of 6.96 fJ, whereas the STT-MTJ and FinFET-based logic encryption circuit shows energy consumption of 21.64 fJ. Thus, the proposed design shows 3.11× lower energy consumption than the FinFET designs. STT-MTJ and TFET LiM-based logic encryption achieves lower energy consumption due to the higher ON current and low leakage characteristics of the TFET at lower supply voltage.

4.3 Fabrication compatibility of STT-MTJ with TFET

The homojunction TFET and CMOS FinFET devices were fabricated using an identical manufacturing process, since the two devices have similar architecture [28]. It was experimentally confirmed that complementary TFET devices fabricated in a standard CMOS foundry exhibited higher compatibility for commercial production and enhanced flexibility for heterogeneous TFET-CMOS systems [28]. Several research groups have demonstrated the benefits of mixed MOSFET-TFET circuits/systems and corresponding layout rules with both simulations and experimental fabrication [31]. Additionally, the STT-MTJ exhibited higher compatibility with the CMOS process by back-end-of-line fabrication. This encouraged the researchers to explore LiM architectures that achieve low area and energy overheads. Recent research demonstrated the heterogeneous 3D integration for STT-MTJ-based memory-on-logic applications that separate memory and logic blocks, and stack memory tires on top.
of logic blocks [20]. This STT-MTJ-based 3D integration achieved silicon area saving with performance gain.

CMOS exhibited higher compatibility with STT-MTJ and TFET is fabricated using an identical manufacturing process. Therefore, the TFET technology can show the ease of integration and flexibility in manufacturing with STT-MTJ. However, secondary effects including ambipolarity, p-i-n forward current, and enhanced Miller effect still exist in TFET, which makes it unpopular and less suitable for commercialization at this time [31]. More research efforts are needed to make these emerging technology integrations a reality.

5 Conclusion

Existing CMOS SABL-based circuits and CMOS-based STT-MTJ LiM circuits are characterized by high energy consumption, with increased vulnerability to hardware security attacks. To reduce the energy consumption, the emerging TFET is introduced into these circuits, achieving ultra-low energy consumption with enhanced security. TFET SABL-based gates and a PRIDE S-box design achieve approximately $3\times$ lower energy consumption than the FinFET designs while maintaining higher DPA resilience. Moreover, TFET SABL-based cryptosystems with lower static power consumption can show vulnerability to static power side-channel attacks. Additionally, the proposed STT-MTJ and TFET LiM gates achieve $4\times$ lower energy consumption than the STT-MTJ and FinFET designs. The proposed STT-MTJ and TFET LiM gates were explored in a logic encryption/locking technique that shows $3\times$ lower energy consumption than the STT-MTJ and FinFET designs. STT-MTJ and TFET-based circuits exhibited higher compatibility in fabrication. However, STT-MTJ and TFET devices exhibited several second-order effects including low reliability, process variations, and other leakages (ambipolarity and p-i-n forward current) that make commercialization of these devices difficult. Further research efforts from the device circuit community are needed to resolve the existing challenges.

Funding The authors have not disclosed any funding.

Data availability Enquiries about data availability should be directed to the authors.

Declarations

Conflict of interest The authors have not disclosed any competing interests.

References

1. Li, A., Shinde, Y., Shi, J., Ye, X., Li, Y., Song, W.Z.: System statistics learning-based IoT security: feasibility and suitability. IEEE J Internet Things. 6(4), 6396–6403 (2019)
2. The cost of malicious cyber activity to the US economy. W. House. 2018. [Online]. Available:https://www.whitehouse.gov/wpcontent/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf
3. Bartock, M., Souppaya, M., Savino, R., Knoll, T., Shetty, U., Cherfaoui, M., Yeluri, R. and Scarfone, K.: Hardware-enabled security for server platforms: enabling a layered approach to platform security for cloud and edge computing use cases. National Institute of Standards and Technology. (pp. 39–39)
4. Roshanisefat, S., Kamali, H.M., Homayoun, H., Sasan, A.: SAT-hard cyclic logic obfuscation for protecting the IP in the manufacturing supply chain. IEEE Trans. VLSI Syst. 28(4), 954–967 (2020)
5. Prinetto, P., and Roascio, G.: Hardware security, vulnerabilities, and attacks: a comprehensive taxonomy. In ITASEC 177–189 (2020)
6. De, P., Mandal, C., Prampalli, U.: Path-balanced logic design to realize block ciphers resistant to power and timing attacks. IEEE Trans. VLSI Syst. 27(5), 1080–1092 (2019)
7. Wang, W., Standaert, Y.F.X., Liu, J., Guo, Z., Gu, D.: Ridge-based DPA: improvement of differential power analysis for nanoscale chips. IEEE Trans. Inform. Forensic Secur. 13(5), 1301–1316 (2018)
8. Rossi, D., Tenentes, V., Yang, S., Khursheed, S., Al-Hashimi, B.M.: Aging benefits in nanometer CMOS designs. IEEE Trans. Circuits Syst. II Exp. Briefs 64(3), 324–328 (2017)
9. de Cnudde, T., Nikova, S.: Securing the present block cipher against combined side-channel analysis and fault attacks. IEEE Trans. Very Large Scale Integ. Syst. 25(12), 3291–3301 (2017)
10. Shanmugham, S.R., Paramasivam, S.: Survey on power analysis attacks and its impact on intelligent sensor networks. IET Wireless Sensor Syst. 8(6), 295–304 (2018)
11. Tena-Sanchez, E., Castro, J., Acosta, A.J.: A methodology for optimized design of secure differential logic gates for DPA resistant circuits. IEEE J Emerg. Select Topics Circuits Syst. 4(2), 203–215 (2014)
12. Kumar, S.D., Thapliyal, H., Mohammad, A.: FinSAL: a novel FinFET based secure adiabatic logic for energy-efficient and DPA resistant IoT devices. IEEE Trans. Comput Aided Design Integr. Circuits Syst. 37(1), 110 (2017)
13. Avital, M., Dagan, H., Keren, O., Fish, A.: Randomized multi-topology logic against differential power analysis. IEEE Trans. VLSI Syst. 23(4), 702–711 (2015)
14. Tanimura, K., Dutt, N.D.: HDRL: homogeneous dual-rail logic for DPA attack resistant secure circuit design. IEEE Embed. Syst. Lett. 4(3), 57–60 (2012)
15. Kumar, S.D., Thapliyal, H., Mohammad, A.: EE-SPFAL: a novel energy-efficient secure positive feedback adiabatic logic for DPA resistant RFID and smart card. IEEE Trans. Emerg. Topics Comput. 7(2), 281–293 (2019)
16. Saini, H., Gupta, A.: Constant power consumption design of novel differential logic gate for immunity against differential power analysis. IET Circuits Devices Syst. 13(1), 103–109 (2018)
17. Bellizia, D., Bongiovanni, S., Monsurro, P., Scotti, G., Trifiletti, A.: Univariate power analysis attacks exploiting static dissipation of nanometer CMOS VLSI circuits for cryptographic applications. IEEE Trans. Emerg. Topics Comput. 5(3), 329–339 (2017)
18. Delgado-Lozano, I. M., Tena-Sanchez, E., Nunez J., and Acosta, A. J.: Design and analysis of secure emerging crypto-hardware
