IEEE TRANSACTIONS ON
EMERGING TOPICS
IN COMPUTING

Received 6 October 2015; revised 4 February 2016; accepted 22 March 2016.
Date of publication 27 April 2016; date of current version 6 September 2017.

Digital Object Identifier 10.1109/TETC.2016.2559159

Tunnel FET Current Mode Logic for DPA-Resilient Circuit Designs

YU BI, (Student Member, IEEE), KAVEH SHAMSI, (Student Member, IEEE), JIANN-SHIUN YUAN, (Senior Member, IEEE), YIER JIN, (Member, IEEE), MICHAEL NIEMIER, (Senior Member, IEEE), AND XIAOBO SHARON HU, (Fellow, IEEE)

Y. Bi, K. Shamsi, J.-S. Yuan, and Y. Jin are with the Department of Electrical and Computer Engineering, University of Central Florida, Orlando FL 32816, M. Niemier and X.S. Hu are with the Department of Computer Science and Engineering, Notre Dame University, Notre Dame IN 46556,

CORRESPONDING AUTHOR: Y. JIN (yier.jin@eecs.ucf.edu)

ABSTRACT Emerging devices have been designed and fabricated to extend Moore's Law. While traditional metrics such as power, energy, delay, and area certainly apply to emerging device technologies, new devices may offer additional benefits in addition to improvements in the aforementioned metrics. In this sense, we consider how new transistor technologies could also have a positive impact on hardware security. More specifically, we consider how tunnel transistors (TFETs) could offer superior protection to integrated circuits and embedded systems that are subjected to hardware-level attacks – e.g., differential power analysis (DPA). Experimental results on a light-weight cryptographic circuit, KATAN32, show that TFET-based current mode logic (CML) can both improve DPA resilience and preserve low power consumption in the target design. Compared to the CMOS-based CML designs, the TFET CML circuit consumes 15 times less power while achieving a similar level of DPA resistance.

INDEX TERMS Current mode logic (CML), correlation power analysis (CPA), hardware security, emerging technology

I. INTRODUCTION

The Internet of Things (IoT) is certain to impose new demands on modern cryptographic systems. As many IoT nodes and remote sensors are driven by batteries, power consumption is a critical design constraint. As a result, conventional encryption algorithms such as Advanced Encryption Standard (AES) [1] may not be suitable for these resource constrained applications because of the high power and area associated with the hardware implementations. As such, the development of light-weight cryptographic algorithms has become a high priority, with various light-weight encryption algorithms being developed [2]–[5]. Meanwhile, the wide distribution of IoT devices gives attackers physical access to these devices, making side-channel attacks easier to apply. Therefore, countering side-channel attacks, such as differential power analysis, is an important design consideration even in these resource-constrained designs.

Ever since differential power analysis was first proposed by Kocher *et al.* [6], researchers have been working to develop solutions to counter DPA attacks. Countermeasures are generally classified into two categories: (i) hardware level solutions and (ii) algorithm level solutions. Kocher suggested that the cryptographic algorithm should be designed in a way that withstands a certain amount of information leakage [7]. For example, when using a hashing algorithm for generating new keys, the frequently changing keys will make it difficult for attackers to capture a sufficient amount of a power trace to mount a successful DPA attack. Another technique was presented by adding a transformed mask to S-box, where the masking methods can be applied to the non-linear part of encryption algorithm [8]. After the substitution operation, the multiplicative mask is replaced with the original mask. Yang *et al.* proposed randomly varying voltage and frequency to prevent side-channel attacks at the gate level [9]. Therefore, the time and power consumption of the intermediate operations are more random, which minimizes the leakage of information through the side channels. A more practical circuit-level method on preventing DPA attack leveraged a sense amplifier-based logic style (SABL) for cryptographic algorithm implementations [10]. The strength of this approach is the constant power consumption of differential logic which can counter power-based attacks as operation

power is independent of processed data. However, traditional circuit level protection schemes such as current mode logic (CML) trade power efficiency for security. When considering the IoT applications, embedded system designers are presented with a dilemma in which they can choose either high security or low power consumption.

Orthogonal to current approaches of circuit level optimization, in this paper we consider how emerging transistor technologies could help mitigate risks of side channel attacks while maintaining low power consumption. Emerging devices have been proven to have unique applications in the hardware security domain [11], [12]. In this work, we further extend research in this direction to use emerging devices to preserve low power consumption but achieve the goal of DPA-resilience. More specifically, we will demonstrate that by implementing CML with emerging tunnel transistors (TFETs) for lightweight encryption algorithms, one can significantly improve the circuit security at a fraction of the power when compared to CMOS equivalents. Our contributions are as follows:

- We first introduce a library of TFET-based current mode logic components that cover all basic logic gates. This is the first work to introduce a full set of designs and measurements of TFET-based CML gates.
- We then use the TFET based CML gates to design a 32-bit, lightweight KATAN cipher. To the best of our knowledge, this is also the first attempt to use CML gates based on emerging technologies for lightweight cryptography implementations.
- Finally, we present correlation power analysis on the TFET CML KATAN cipher, which shows that TFET CML is better than MOS CML in terms of the power consumption and area usage when achieving similar security levels.

The rest of the paper is organized as follows: Section II provides an overview of existing work related to CML and DPA-resilient designs. Section III provides a brief introduction to TFETs. Device modeling is also discussed. Section IV discusses the concept of TFET-based current mode logic gates and provides detailed performance simulations and evaluation of standard TFET-based CML gates. In Section V, TFET based CML gates are used to implement a lightweight, 32-bit KATAN cipher. Correlation power analysis is also presented. We conclude with Sections VI and VII, which respectively represent a summary discussion and plans for future work with TFET based CML.

II. RELATED WORK

In this section, we briefly introduce frequently employed lightweight ciphers as well as current mode logic. Both form the underlying basis of this work.

A. LIGHT-WEIGHT CIPHER

Conventional encryption algorithms such as Advanced Encryption Standard may not be suitable for applications where power and area are strictly limited. For example, devices used in components for the Internet of Things, wireless sensor networks (WSN), etc. consist of various low-power and low-cost nodes to support communication over wireless channels. Furthermore, many IoT devices and wireless sensor nodes support military applications where security is a critical request to be addressed. Understanding how to secure communication channels at a lower cost is an important question for the security community. Thus, the development of light-weight cryptographic algorithms has become an important research area [2]–[5]. Two important design principles guide lightweight cipher design:

i) *Security:* in general, light-weight ciphers are resistant to typical attacks such as algebraic attacks and brute force attacks.
ii) *Implementation Efficiency:* light-weight ciphers are small in terms of area and power consumption, compared to hardware required for standard cryptography algorithms.

One main difference distinguishing the light-weight from the conventional block cipher is that the block size of light-weight ciphers is usually less than 64 bits – when compared to at least 128 bits for conventional block ciphers. As examples:

- The DESL and DESXL ciphers represent the first attempt at light-weight encryption [3]. Since the algorithm is a derivative of DES, the key idea is to replace the DES round function by only one S-box and to remove the initial and final permutation.
- The PRESENT cipher is one of the most popular light weight ciphers proposed in 2007 [2]. It is executed in 31 rounds, and composed of a 64-bit length block and keys of 80-bit or 128-bits. A simple substitution-permutation network (SPN) is adopted for the round function.
- Beaulieu *et al.* proposed a new cryptographic algorithm – the SIMON block cipher – where the block size covers a wide range from 32 to 128 bits as well as key sizes ranging from 64 to 256 bits [4]. Different key schedules can lead to different rounds of encryption varying from 32 to 72 rounds. The SIMON cipher uses the conventional Feistel network with a further reduction of hardware cost.
- Aiming to further lower the gate equivalent (GE, a measure of hardware complexity) of the block cipher, the KATAN and KTANTAN ciphers were proposed in 2009 [5]. The design of the KATAN cipher is a block cipher based on stream cipher design, which iterates 254 rounds to output the ciphertexts. The 80-bit keys can be applied for three different variants, 32, 48 and 64 bits.

B. CURRENT MODE LOGIC

Current mode logic represents a differential digital logic family [10], [13]–[16]. A CML gate includes a tail current source, a current steering core and a differential load. The working mechanism of a CML gate is to switch the constant current through the differential network of input transistors, utilizing the reduced voltage swing on the two load devices as the output.

Although current mode logic is not widely used in mainstream circuit design, its unique features, namely low latency and stable power consumption, can be leveraged for specific applications, such as DPA countermeasures – i.e., serving as a countermeasure against a DPA attack.

To some extent, employing CML primitives may be more efficient than other gate-level DPA countermeasures, such as gate masking [17] and dynamic management of voltage and frequency [9], [14]. For example:

- Badel *et al.* formalized the generic standard cells for differential logic styles, including layout characterization and library generation methodologies [15].
- In order to further reduce the power of CML gates, Cevrero *et al.* leveraged the power gating technique for the differential logic design, where a standard cell was generated, and DPA analysis was lauched on the power-gated CML AES design [16]. The implementation achieved both goals of reduced power consumption and DPA resilience.
- Macé *et al.* raised a potential connection between binary decision diagram (BDD) and the current mode logic for cryptography [18]. It is promising since BDD is applied to optimize the Boolean representation and CML gates tend to be energy-hungry. The exploited isomorphism between CML and BDD can help design very efficient differential logic gates that optimize the performance in terms of power and area.
- Furthermore, the authors of [19] proposed a subthreshold CMOS CML design to reduce the power consumption associated with conventional MOS CML. Not surprisingly, a large PMOS load device and low drive currents ($I_{SD} = 1\,\mathrm{n}A$) lead to a design with a large area and low speed. These drawbacks limit the application of block ciphers, especially lightweight block ciphers, where both area and speed are two critical criteria.

TFET-based CML gates have also recently been introduced [20], [21]. Initial CML gate designs based on the newly developed GaSb-InAs heterojunction TFET, which has improved on-state current with hetero-band alignment. Two logic gates, a buffer and a multiplexer were studied and evaluated [20]. TFET-based CML design exhibited lower power consumption when compared to CMOS equivalents. However, (i) only two TFET CML gates were presented, and (ii) the authors of [20] did not discuss how to leverage TFET CML gates for circuit-level designs, and (iii) TFET CML was not applied at all in the hardware security domain. In order to fully evaluate TFET-based logic – not only from the perspective of traditional metrics such as delay and power, but also with respect to new metrics such as security – in this paper, we will construct a TFET CML gate library using a systematic approach and will demonstrate its applications in the hardware security area.

III. TUNNEL FET TECHNOLOGY

In this section, we briefly discuss the underlying technology (TFET devices) and modeling assumptions which are used to build the TFET CML gate library in this paper.

A. DEVICE DESCRIPTION

Different types of tunneling FETs (TFETs) have been developed and fabricated [22], [23]. Among them, III-V

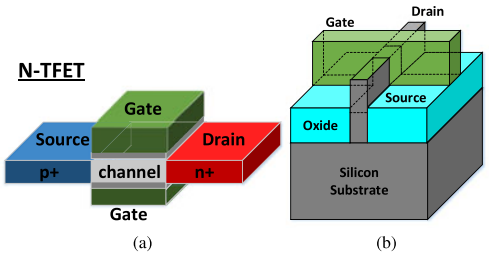


FIGURE 1. 3-D physical structure of (a) a tunnel FET [26] versus (b) a FinFET [27].

TFETs appear more promising due to their higher conduction current. More specifically, InAs homo-junction TFETs [24] and GaSb-InAs hetero-junction TFETs [25] have been the subject of much study. Considering that the InAs homo-junction is more mature among these two devices, we will employ it as our TFET transistor model. FinFET 20 nm technology is also adopted for comparison. The physical structures (used in Synopsys TCAD simulation) of both the homo-junction TFET and FinFET are depicted in Figure 1 [26], [27].

It is apparent that TFETs have asymmetrical doping where source and drain are p-type and n-type doping, respectively. A gate voltage can induce band-to-band tunneling at the channel to control the tunneling current. In contrast, in a conventional CMOS transistor, current conduction occurs via electron carriers with enough energy to surmount the channel thermal barrier. The Fermi-Dirac distribution limits the subthreshold slope (SS) to 60 mV/decade. However, the high energy carriers in TFETs can be filtered by the gate-voltage-controlled tunnel such that a sub-60 mV/decade subthreshold swing is achievable at the room temperature [22]. With improved steep slope and high on-current at a low supply voltage, TFETs could enable supply voltage scaling to further address challenges such as undesirable leakage currents, threshold voltage reduction, etc.

The device parameters assumed for the InAs homo-junction TFET (that we will employ in our circuit simulations) are listed in Table 1. A Si FinFET is also included as the baseline.

B. DEVICE MODELING

While a compact SPICE model has been recently developed for TFETs [28], [29], in this work, we employ a look-up table based Verilog-A model derived from TCAD Sentaurus for our simulations as this model has been widely used and validated [20]. Figure 2a depicts the structure of the TFET Verilog-A model [30]. It is composed of three parts: gate-drain capacitance C_{GD}, gate-source capacitance C_{GS} and the transfer characterisitics $I_{DS}(V_{GS}, V_{DS})$. The current models of different paths are also listed in Equation (1). The calculation of three current models refers to the look-up table that includes a range of fine-step voltage bias and capacitance,

$$\text{Look Up Table} = \begin{cases} I_{GD} = \frac{d}{dt}(C_{GD} * V_{GD}) \\ I_{GS} = \frac{d}{dt}(C_{GS} * V_{GS}) \\ I_{DS} \rightarrow (V_{GD}, V_{GS}). \end{cases} \quad (1)$$

TABLE 1. InAs homo-junction TFET device parameters [24].

Gate Length (L_G)	20 nm
Body Thickness (T_{ch})	5 nm
Dielectric Thickness (HfO_2)	5 nm
Source Doping (p+)	4×10^{19} cm^{-3}
Drain Doping (n+)	6×10^{17} cm^{-3}
Si FinFET S/D Doping	1×10^{20} cm^{-3}

By employing the TFET Verilog-A model, we evaluate the DC performance of an N-type TFET as shown in Figure 2b, where the on-current I_{DS} varies with gate-source voltage V_{GS}. CMOS data is also included for comparison. Both CMOS and TFET devices assume 20 nm technology with V_{DS} = 0.6 V. A TFET's sub-threshold slope is improved when compared to CMOS. Notably, when the gate-source voltage is less than 0.4 V, the conducting current of TFETs outperforms the CMOS counterpart. (However, when $V_{GS} > 0.4$ V, the CMOS device exhibits a better on-current.) As a result, TFETs represent promising ultra low-power features that provide further V_{DD} scaling in integrated circuit designs.

IV. TUNNEL FET CIRCUIT EVALUATION

Here, we discuss our TFET CML standard cell designs. We begin by discussing a "generic" TFET-based CML circuit. We then present design specific criteria for TFET-based CML (i.e., required supply voltage values, etc.). After reviewing the power/performance of other TFET CML standard cells, we conclude this section with an initial evaluation of how resilient a TFET CML design might be to DPA.

A. TFET-BASED CURRENT MODE LOGIC

One major difference between CML circuits and single-ended circuits is that the voltage swing of CML is smaller than that of static logic. Thus, differential logic styles were originally designed for high speed communication. Due to invariant power consumption, researchers adopted this circuit-level method as a countermeasure against differential power analysis [14]–[16]. A "generic" TFET-based CML

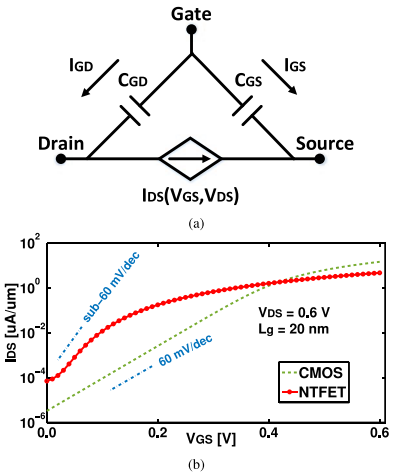


FIGURE 2. TFET device modeling: (a) TFET verilog-A model (b) I_{DS} versus V_{GS} [30].

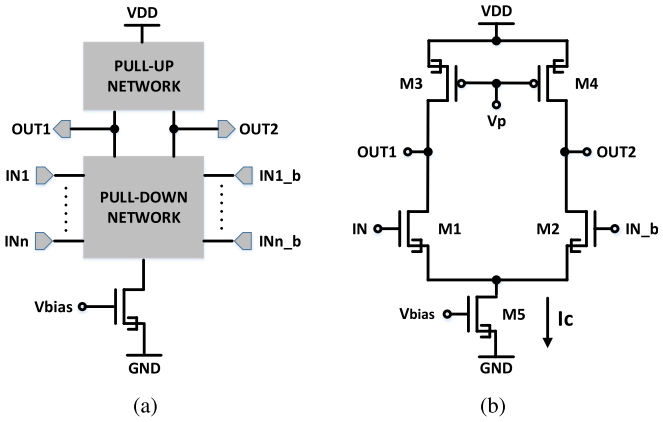


FIGURE 3. (a) The universal diagram of CML circuits (b) Schematic of the TFET-based CML inverter.

circuit is shown in Figure 3a. The schematic is divided into two parts: a pull-up network and pull-down network.

For TFET CML, the pull-up network is constructed by either two resistors or two P-type TFETs (PTFETs). Since the consumption of power and area of the resistor is dramatically larger than a FET using modern technology, the FET-based pull-up network dominates. In CML the pull-up network mainly works as the load device to manage the DC voltage drop on the output. By simply tuning the gate bias of a P-type FET, the on-resistance of PTFETs can be adjusted, thereby altering output voltage accordingly. At the bottom of Figure 3a, one N-type FET (NTFET) is included to serve as a current source, which can determine the value of output voltage swing. On the other hand, the pull-down network that is composed of NTFETs mainly serves as the major functional unit in the CML circuit. The different logic functions can be achieved by distinct combinations of a group of NTFETs. Note that the inputs of the pull-down network are required to be differential pairs.

Figure 3b shows a schematic of a TFET-based current mode inverter/buffer. One pair of transistors is controlled by the differential inputs, IN and IN_b, respectively. The constant driving current is provided by the transistor M5, which is also tunable by the gate bias voltage V_{bias}. Together with M5, transistors M3 and M4 are employed to charge and discharge the output pair, OUT1 and OUT2. When IN is logic 1, M1 is turned on, and the constant current I_C flows through the left-handed path. Thus, OUT1 discharges to a certain value between VDD and GND, and OUT2 alternatively charges to quasi VDD. Note that in the CML design, logic 0 is commonly defined as half VDD, and logic 1 is close to VDD. In this case, OUT1 voltage is less than logic 1, which is treated as logic 0. If OUT1 is extracted as the output pin and the inverted OUT2 is extracted as complementary output pin, the schematic achieves the inverter function. On the contrary, if OUT1 is treated as the complementary output pin and OUT2 is treated as the output pin, the circuit performs the buffer function.

B. DESIGN OPTIMIZATION

In traditional CML design, the biggest challenge is the larger amount of power consumption than static logic, even though

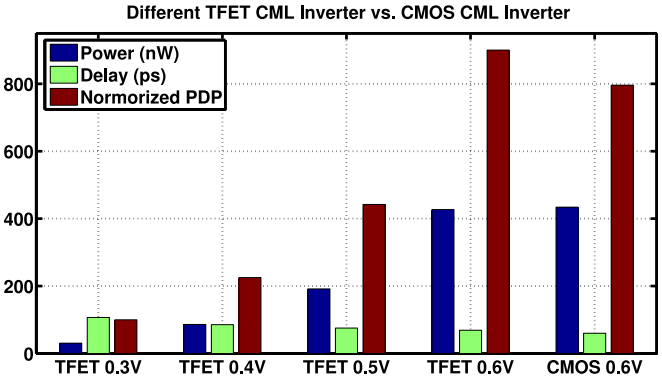


FIGURE 4. Different configurations of TFET CML inverter versus CMOS CML inverter.

researchers have proposed different techniques to minimize the power consumption of CML [16], [31]. One common method is to decrease the supply voltage. However, because of scaling issues with CMOS technology, the voltage source must surpass the threshold value to turn on the transistor at a certain point (V_{th} is approximately 0.27 V for 20 nm technology). Also, the decreased supply voltage can dramatically increase the switching time of CMOS gates, and consequently increase the power-delay product (PDP).

As discussed in Section III, TFETs are promising for low-power applications due to sub-60 mV/decade sub-threshold slopes. In [20], the authors considered the threshold of TFET as 0.15 V, thus the lowest possible supply voltage for TFET is 0.3 V. On the other hand (and again following an approach in [20]), to fairly compare TFETs with CMOS, as the corresponding current for a TFET at V_{GS} = 0.15 V is similar to CMOS at V_{GS} = 0.3 V, the minimum supply for CMOS is set to be 0.6 V. As a result, given the minimum requirement, the input/output voltage swing sits between 0.15 and 0.3 V for TFET, while the voltage swing is between 0.3 and 0.6 V for CMOS.

Figure 4 illustrates the delay and the power-delay product of the CML inverter with different supply voltages for TFETs when compared to a 20 nm FinFET equivalent assuming a VDD of 0.6 V. The voltage swing for all five cases is set as one half of the value of VDD. At the same supply voltage (VDD = 0.6 V), the power consumption of a TFET CML inverter is comparable to a CMOS CML inverter (426.9 nW for TFET versus 434.3 nW for CMOS) – although the TFET CML inverter is slightly slower than the CMOS CML inverter (69 ps for TFET versus 60 ps for CMOS). The driving current of the TFET CML inverter is 711.6 nA compared to CMOS CML inverter of 723.8 nA at $VDD = 0.6V$. When VDD is lowered to 0.3 V, although the switching time of the TFET CML inverter increases accordingly, the power consumption and power-delay product are dramatically reduced when compared to a CMOS CML inverter. This suggests that TFET-based CML gates could offer significant improvements over CMOS CML gates in ultra low power applications. Moreover, because other more complex logic gates (e.g., multiplexers) can be naturally implemented in differential mode style, TFET based CML gates should offer

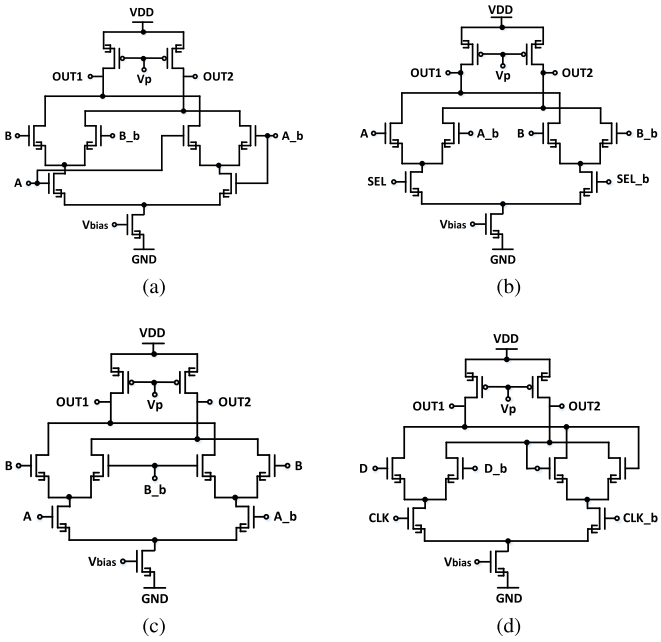


FIGURE 5. The universal schematics structure of four different CML circuits: (a) AND (b) Multiplexer (MUX) (c) Exclusive-OR (XOR) (d) D latch.

additional benefits compared to CMOS CML gates. For instance, a CML based multiplexer composed of nine transistors is more area efficient than a static multiplexer with fourteen transistors (three NANDs and one inverter). It is worth noting that the symmetry property can be better accomplished in CML based multiplexer compared to other CML based logic gates, such as AND/OR gates.

C. TFET-BASED CML STANDARD CELLS

The above analysis suggests that CML can perform various functions based on different configurations. In fact, three levels of CML implementations are introduced in [32]. By observing the stacked levels and different pairs, the delay of a gate with more than three-levels exceeds the delay of an equivalent three-level, static multiplexer. That is, the level of differential pairs is limited to three for the optimization in the CML implementation. Figure 5 depicts four two-input TFET-based CML functions with a two-level structure. Each of the gates has three differential pairs as inputs. A set of four functions (including AND, NAND, OR and NOR) can be derived from Figure 5a with different input/output configurations. The MUX, XOR/XNOR and D latch are also distinguished by wiring and the input/output selection shown in Figures 5b, 5c, 5d, respectively.

As discussed in the previous section, we attempt to maintain the voltage swing of input and output between 0.15 and 0.3 V for TFET CML gates. The configuration of the supply voltage and voltage swing sets the baseline for the other parameters, such as transistor size and biasing voltages. Here, we configure the TFET width to be the same size as the technology length to minimize the area. The 20 nm technology nodes are used for our evaluations. Consequently, it is

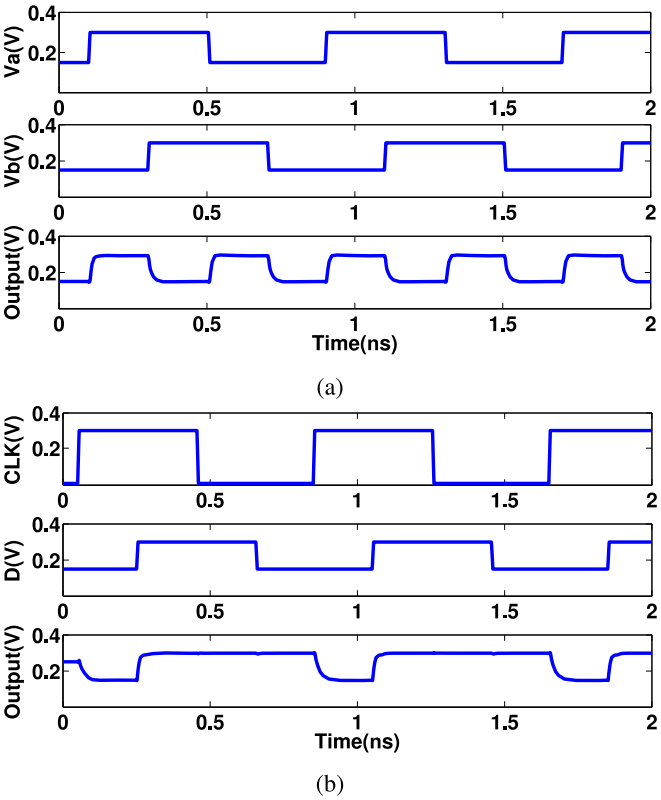


FIGURE 6. **(a) XOR simulation results (b) D Latch simulation results.**

important to tune V_{bias} and V_p to achieve the necessary voltage swing for the entire standard logic cells. After voltage sweeping, the basic CML logic gates functions best when V_{bias} = 0.18 V and V_p = 0.14 V. Figure 6 presents the transient simulations for the exclusive-OR and D latch, where both the inputs and outputs are between 0.15 and 0.3 V.

The other standard cells are also characterized and simulated under the same biasing condition. Table 2 shows the area, delay and power for the standard cells of TFET-based CML. Only ten cells are described, but more CML logic functions can be derived from the standard cells proposed in Table 2. For instance, if we define OUT1 as the output pin, then a CML-based inversion function is possible per Figure 3a. However, if we choose OUT2 as the output pin, the CML

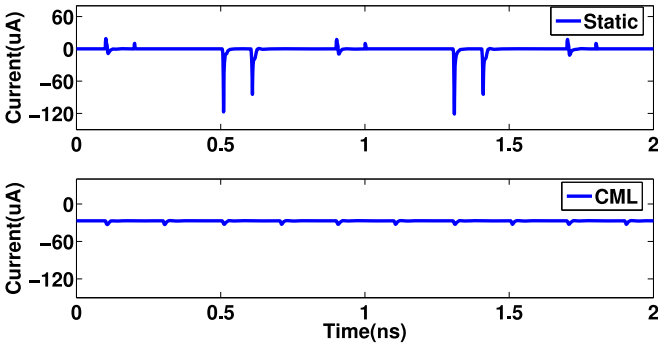


FIGURE 7. **The power traces between static XOR and CML XOR.**

schematic works as a buffer. Moreover, a standard cell library usually accounts for the different driving strengths of each individual function. In CML gates, a simple solution is to increase the constant current by the tail biasing transistor [15].

The area of CML and static TFET gates is also provided in Table 2. With the exception of a CML buffer and a four-input AND gate, all other CML standard cells consume less area compared to static counterparts. This feature may also be a major advantage for cryptographic systems, especially lightweight ciphers such as KATAN, where majority of the hardware is composed of D flip flops and multiplexers.

D. SECURITY EVALUATION OF TFET-BASED CML GATES

Before we consider implementations of lightweight ciphers with TFET CML gates, we first consider TFET CML in more detail from the hardware security perspective. It is well known that the key idea of differential power analysis is based on the power consumption during circuit transition. In static CMOS logic, the major power consumption happens when the output of logic undergoes a 0→1 (or 1→0) transition. Because of this symbolic characteristic of static logic, the genuine cryptographic algorithm is vulnerable to the DPA attack. On the contrary, the CML structure is naturally resistant to a DPA attack considering the relatively constant power consumption for almost any transitions.

Figure 7 depicts the power traces for the TFET static XOR gate and the TFET differential style XOR gate. Obviously, the TFET CML XOR gate dissipates almost constant power in

TABLE 2. **Area, delay and power of the TFET-based CML standard cells.**

Cells	Transistor Counts	Area [μm^2]	Rising Delay [ps]	Falling Delay [ps]	Avg Delay [ps]	Power [nW]	PDP [nW × ps]	CML area/ Static area
Buffer	5	0.0022	90	124	107	30.588	3272.916	1.833
OR2	9	0.0036	99	124	111.5	24.032	2679.568	1
AND2	9	0.0036	75	165	120	22.97	2756.52	0.818
AND4	27	0.011	476	644	560	70.828	39663.68	1.8
MUX2	9	0.0036	71	115	93	24.183	2249.019	0.5
XOR2	9	0.0039	99	105	102	25.848	2636.496	0.817
D-Latch	9	0.0037	102	168	135	23.122	3121.47	0.341
DFF	18	0.0074	100	200	150	45.500	6825	0.341
1-bit FA	45	0.0186	416	591	503.5	233.928	1.178×10^6	0.847
4-bit FA	180	0.744	654	591	622.5	939.150	5.846×10^6	0.847

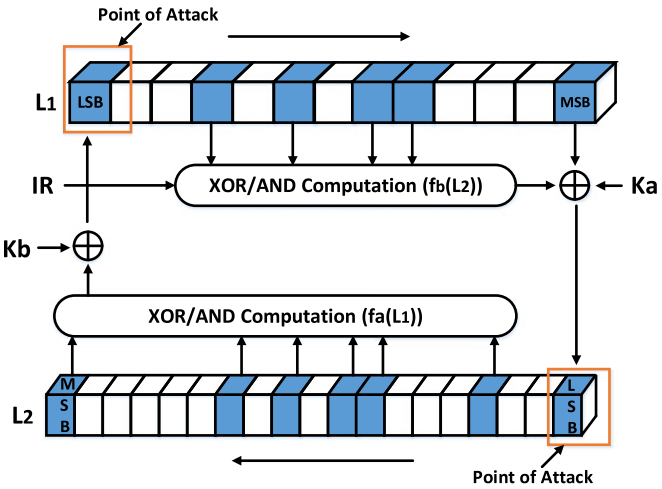


FIGURE 8. **The abstract schematic of the KATAN cipher.**

contrast to the significant power overshoot of the static XOR gate. That is, the power profile of the TFET static XOR gate leaks more information for the attacker to identify the internal activity of the cryptographic system. However, the almost constant power consumption of a TFET CML XOR gate provides essentially no information about data transitions. Moreover, as we have discussed in previous section that the 0→1 transition is essentially mirrored to 1→0 transition in the CML gates, even though attackers may retrieve some information through the power glitches, it is very challenging for them to identify what the processing logic value is.

V. IMPLEMENTATION OF CRYPTOGRAPHIC SYSTEM

Due to large area and high power consumption, using CML to implement cryptographic hardware is not common – especially in lightweight cryptographic systems. To protect cryptographic circuits against DPA attacks, researchers often employ other techniques [33], [34]. These solutions incur significant computation cost where the cryptography already involves massive computation and consumes relatively large power and area. As such, lower power, TFET-based CML could be especially valuable when considering devices for the IoT, WSN nodes, etc. Lacking an effective defense mechanism, hardware in these spaces can be substantially more vulnerable/susceptible to hardware attacks such as DPA.

To address these challenges, in the following sections, we consider the impact of TFET-based CML on a 32-bit KATAN cipher. More specifically, (a) the KATAN cipher is a hardware-oriented block cipher with a low GE – even among other lightweight ciphers, (b) applications that employ lightweight ciphers are typically power constrained – and thus could benefit from TFET technology, and (c) the limit for the application of CML on conventional block ciphers is the large power overhead, but power consumption in a lightweight cipher is typically much less. In subsequent sections, we will briefly discuss the working mechanism of the KATAN cipher. Implementations of the 32-bit KATAN cipher are provided in different circuit-level structures, where a table is presented to compare the TFET based implementation with the CMOS

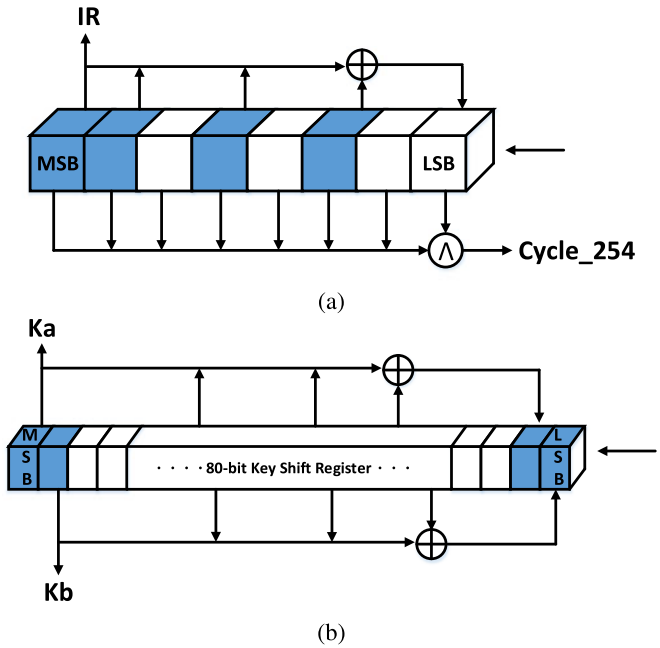


FIGURE 9. **Two additional hardware blocks: (a) IR (counting cycles) and (b) the key schedule.**

implementation. We will then present the correlation power analysis on KATAN32 with experimental results through design simulations.

A. OVERVIEW OF THE KATAN CIPHER

The KATAN ciphers are a family of light-weight block ciphers, consisting of three variants with 32-bit, 48-bit and 64-bit blocks. All KATAN ciphers share the same key schedule with the key size of 80 bits as well as the 254-round iteration with the same non-linear function units [5]. Considering that different variants use the same hardware – except for a small difference in register count – we only focus on the smallest variant of KATAN with 32-bit blocks. As depicted in Figure 8, this 32-bit block is made of 32 registers divided into two parts – L_1 and L_2 – with corresponding sizes of 13 bits and 19 bits respectively. Both L_1 and L_2 are coded as a linear feedback shift register (LFSR), in which it shifts every clock cycle. The two registers are utilized by both plaintext and cipher text for the inputs and outputs. Meanwhile, all the computation of non-linear functions, namely f_a and f_b, can be identified as a combination of AND/XOR calculation in conjunction with different keys (k_a and k_b), and a non-linear irregular factor (IR).

The encryption procedure is described as follows: the plaintext is loaded into two registers L_1 and L_2 such that the lower 19 bits of the plaintext are loaded into register L_2, while the higher 13 bits of the plaintext are loaded into register L_1. In Figure 8 the least significant bits (LSBs) and the most significant bits (MSBs) are specifically noted. Both L_1 and L_2 perform left-shift operations every clock cycle when the start signal is on. During each round, IR and two keys are also generated by two additional blocks. The IR block is shown in Figure 9a, where 8 registers compose an 8-bit LFSR. This block has two functions: first, it generates the

TABLE 3. Power consumption comparison among different implementations on KATAN32.

	Voltage Supply[V]	Gate Equivalent[#]	Area [μm^2]	Average Current[μA]	Power [μW]	Area Change[%]	Power Change[%]
CMOS Static	0.6	1,013	3.534	16.09	9.96	–	–
CMOS CML	0.6	393	1.415	283.65	170.19	– 59.96%	+ 1608.73%
TFET Static	0.6	1,013	3.536	3.14	1.89	+ 0.057%	– 81.02%
TFET CML	0.3	393	1.441	32.53	9.76	– 59.22%	– 2.01%

irregular update value for the non-linear operations, and second, it counts down the 254 rounds (i.e., when the signal *cycle_254* is logic 1, KATAN has completed the entire encryption).

The key schedule block is illustrated in Figure 9b. Similar to the IR, the key schedule block is an 80-bit LFSR. Before the encryption, the keys are stored in the registers. The LFSR shifts one bit to generate one roundkey. The two most significant bits are exported as k_a and k_b for KATAN every two clock cycles. The feedback polynomial with a minimal hamming weight of 5 is selected for the 80-bit shift register as derived in Equation (2). As a result, the subkey of round i can be defined in Equation (3), where the key is denoted as capital K,

$$f(x) = x^{80} + x^{61} + x^{50} + x^{13} + 1 \tag{2}$$

$$k_i = \begin{cases} K_i & i = 0...79 \\ k_{i-80} \oplus k_{i-61} \oplus k_{i-50} \oplus k_{i-13} & i > 79. \end{cases} \tag{3}$$

Two nonlinear functions f_a and f_b are defined in Equations (4) and (5), which represent the two abstract blocks (XOR/AND computation) in Figure 8. Here, considering that the 32-bit KATAN cipher is adopted, we have already located which bits of L_1 and L_2 are selected for the computation. For the other variants, the positions of bits can be different because of a different number of registers [5],

$$f_a(L_1) = L_1[12] + L_1[7] + (L_1[8] \cdot L_1[5]) + (L_1[3] \cdot IR) + k_a \tag{4}$$

$$f_b(L_2) = L_2[18] + L_2[7] + (L_2[12] \cdot L_2[10]) + (L_2[8] \cdot L_2[3]) + k_b. \tag{5}$$

B. CML IMPLEMENTATION ON KATAN

We now discuss how different transistor technologies could impact the power/performance of KATAN32 by using the Synopsys Design Compiler using 20 nm InAs Homojunction TFET [35] and the Predictive Technology Model (PTM) 20 nm FinFET technology [36]. In order to minimize the area consumption of KATAN32, the driving-strength-one library is employed for the synthesis. The synthesized transistor-level netlist is further converted into both the single-ended and differential modes. Synopsys Finesim is adopted for the gate-level simulation with less simulation time compared to the HSPICE simulator. The operating frequency of KATAN32 is set to 100 MHz to ensure its functional correctness.

Area and power data for four different implementations is summarized in Table 3. More specifically, we consider TFET and CMOS static implementations as well as CMOS CML with a 0.6 V supply, as well as TFET CML with a 0.3 V supply. A 2-input NAND gate is assumed when comparing equivalent gate numbers. It is worth noting that the number of the synthesized static GEs is more than what is reported in [5], mainly because we simplify our library for both TFET and CMOS by using our own driving-strength-one and two-input standard cells. Complex logic gates such as D flip flops and multiplexers, are not fully optimized and consume a relatively larger number of gates. (Future work will be performed to further optimize all TFET CML based logic gates.)

Notably, it is not difficult to see that two CML implementations consume fewer gate equivalents and area compared to the two static counterparts given that KATAN32 is largely comprised of D flip flops, as we discussed in Section IV-C. The area of TFET CML KATAN32 is 1.441 μm^2, which is about 59 percent less than the static TFET KATAN32. Note that the area of TFET based static and CML KATAN32 is similar to their CMOS counterparts as comparable 20 nm technologies are used. The power consumption of *TFET CML* (9.76 μW) even outperforms *static CMOS* (9.96 μW) with slightly lower power consumptions. Figure 10 shows the power trace of the KATAN32 implementation for static and CML TFETs, respectively. The zoom-in subfigure displays the large current overshoot of TFET static KATAN32 compared to the constant current of TFET CML KATAN32.

C. POWER MODEL AND ATTACK MECHANISM

When considering differential power analysis [6], we first need to identify the intermediate values that are a function of

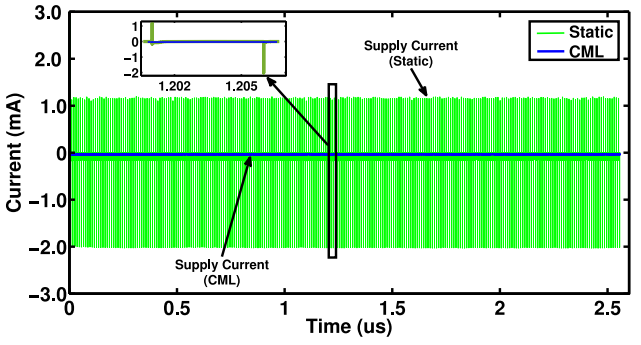


FIGURE 10. KATAN32 power measurements CML TFET versus static TFET.

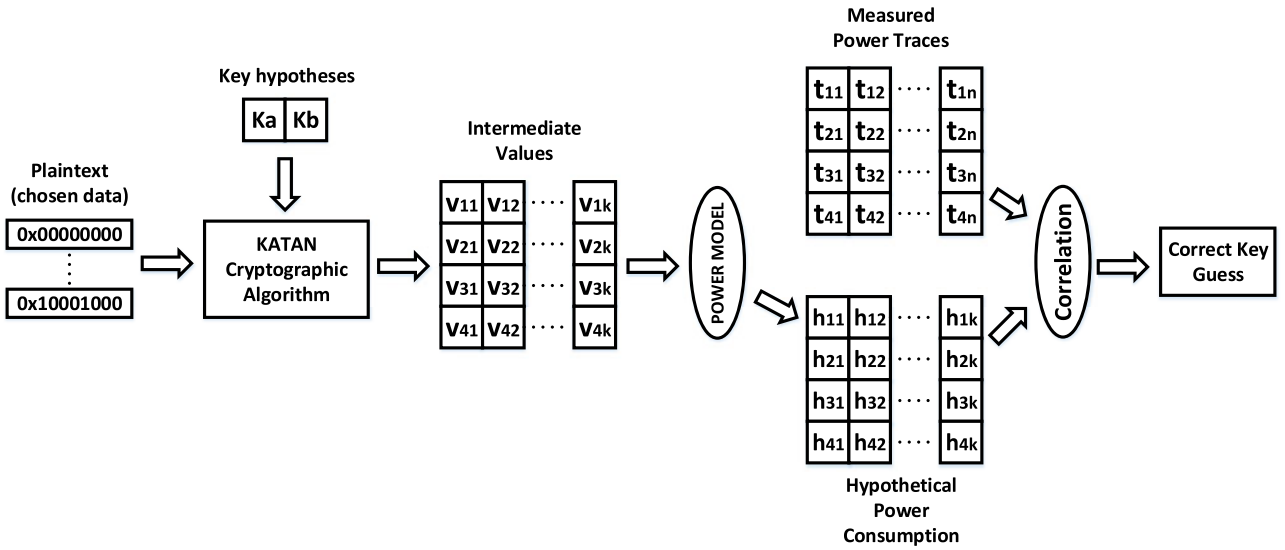


FIGURE 11. The correlation power analysis flow on KATAN cipher.

plaintext/ciphertext, and that are a portion of the keys. Given that when launching a DPA attack, the round keys are part of complete keys, the complexity of DPA computation can be further reduced with the smaller size of round keys. Therefore, the portion of the keys must be as small as possible compared with the complete keys, thereby reducing the complexity of key analysis. The key-dependent intermediate values are further calculated by a group of hypothetical key guesses and are utilized as the inputs of the selection function. Subsequently, the selection function differentiates the power traces into two sets, where they are processed to show a peak for the right key hypothesis.

Correlation power analysis, on the other hand, is an extension of DPA where a model of the power consumption is created for use in the analysis phase of an attack. A power model is needed to approximate the power consumption of the target cryptographic device during an encryption operation. The resulting power predicted by the model will then be correlated to the actual measured power consumption using a key hypothesis. It employs the Hamming weight model (different from the Hamming distance model which is mostly adopted in DPA attack) to hypothesize the intermediate output result and evaluate the relation between the hypothesis values and power traces in a statistical way. Bard *et al.* proposed the security evaluation on the KATAN family, including algebraic and cube attacks [37]. They also pointed out the side channel analysis on KATAN but with only a high-level overview of possible vulnerabilities. To the best of our knowledge, there are not any detailed discussions in existing work about power analysis on the KATAN family. In this paper, we will introduce the power analysis attack on KATAN, as well as the countermeasures – i.e., a TFET CML implementation of KATAN32.

By observing the KATAN algorithm, it is apparent that the two nonlinear functions f_a and f_b are able to connect the plaintext/ciphertext with partial keys (or more precisely, subkeys). We can then select the two bits each round generated by the nonlinear functions as our intermediate values or points of attack as highlighted in red in Figure 8. Besides those two arithmetic functions, the majority of KATAN32 hardware is made up of D flip flops such that the overall power consumption mainly depends on the operation of shifting registers. As a result, it is important to come up with an attack mechanism that maximizes the power profile of two nonlinear operations.

In single-ended logic gates, power consumption only occurs during state transitions, either $0 \rightarrow 1$ or $1 \rightarrow 0$. If we configure the plaintext in a way that for certain clock cycles the power consumption of functions f_a and f_b contributes most, then the power information extracted from the supply current can be maximally related to the key information. More specifically, we can selectively configure the plaintext to be consecutive zeros or ones. Therefore, the power consumption of KATAN32 highly depends on functions f_a and f_b, because the power cost of the left-shift operation is negligible in each clock cycle.

D. CORRELATION POWER ANALYSIS ON KATAN32

In this section, a case study of CPA on KATAN32 is described to disclose the two key values (K [79] and K [78]). Initially, four selected plaintexts are loaded into the two registers as given in Equation (6) and the 80-bit keys are set to all zeros. Note that in real cases, the key is the attackers' target and is unknown to attackers,

$$\begin{aligned} P1 &= \text{x00000000} \Rightarrow p[18] = 0, p[31] = 0 \\ P2 &= \text{x80000000} \Rightarrow p[18] = 0, p[31] = 1 \\ P3 &= \text{x00040000} \Rightarrow p[18] = 1, p[31] = 0 \\ P4 &= \text{x80040000} \Rightarrow p[18] = 1, p[31] = 1. \end{aligned} \tag{6}$$

However, the chosen input values are not constrained to Expression (6), as long as the plaintext interacts mostly with the subkeys. When the start signal is received, KATAN32 begins encryption. Figure 11 shows the proposed CPA attack flow on KATAN32. Each selected plaintext and the

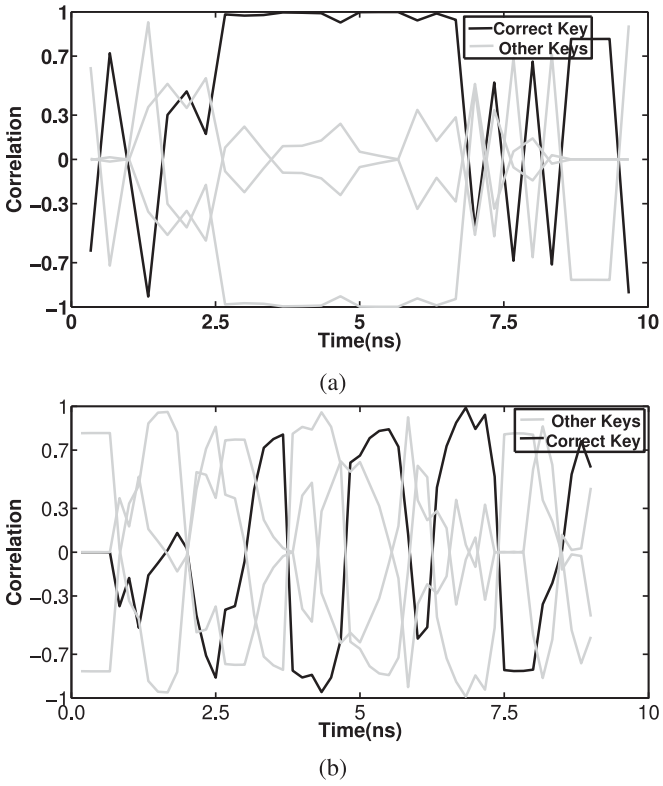


FIGURE 12. CPA attack on one clock cycle (a) TFET static KATAN32 versus (b) TFET CML KATAN32.

hypothetical subkeys K_a and K_b are calculated to achieve the intermediate values "v" matrix. Then, intermediate results are further calculated by the power model, which is defined as the Hamming weight model. The results from the Hamming weight model are defined as the hypothetical power consumption. Based on our chosen plaintexts, the matrix of hypothetical power consumption is given in Equation (7):

$$\text{hypothetical power consumption} = \begin{bmatrix} 0 & 1 & 1 & 2 \\ 1 & 0 & 2 & 1 \\ 1 & 2 & 0 & 1 \\ 2 & 1 & 1 & 0 \end{bmatrix} \quad (7)$$

$$\text{Corr. Coef.} = \frac{\sum_{i=1}^{4}(t_i - \overline{t}) \cdot (h_i - \overline{h})}{\sqrt{\sum_{i=1}^{4}(t_i - \overline{t})^2 \cdot \sum_{i=1}^{4}(h_i - \overline{h})^2}}. \quad (8)$$

The predicted power consumption is then compared with the measured real power consumption by the correlation coefficient formula as given in Equation (8). The highest correlation coefficient result stands for the correctly guessed keys. In this case, the keys '00' reflect the largest correlation coefficient value. The next round follows the same mechanism, but with slightly different ciphertext, which is generated by the last round. Figure 12 shows the detailed correlation power analysis for the respective TFET static KATAN32 and TFET CML KATAN32 on one clock cycle. The black line describes the correct key value for subkeys K_a and K_b (='00'), which are the two most significant bits of the key. It is apparent that the correlation coefficient is largest for a static, TFET-based KATAN32 implementation when the correct keys are applied as shown in Figure 12a. By comparison, the correlation coefficient of TFET CML KATAN32 is more significant, and all four hypothetical keys are similarly distributed as shown in Figure 12b. Consequently, the TFET CML KATAN32 implementation is capable of successfully counteracting the correlation power analysis. Because the power consumption is mainly determined by AND/XOR logic gates of two nonlinear functions – and the effect of CPA is maximized – the correlation coefficients for KATAN32 are higher on average than other block ciphers, e.g., CPA on S-box [16].

As the key schedule of KATAN32 suggests, the key generator block exports two subkeys and does a left-shift operation every clock cycle. Therefore, the 80-bit keys can be continuously output as subkeys in 80 clock cycles, which can be easily attacked by CPA using the chosen plaintexts. The pseudo code for Algorithm 1 describes the abstract CPA attack mechanism on the 80-bit keys of KATAN32. The criteria of choosing the plaintext is to ensure that power consumption is highly dependent on the power cost of intermediate values in certain clock cycles. Moreover, the selected plaintext may be capable of discovering more than one key in different periods.

To launch the complete CPA on KATAN32, the attacker should first select plaintext values that are able to achieve a situation where $\text{Power}_{\text{KATAN32}} = \text{Power}_{\text{intermediate values}}$. Then, after 80 clock cycles, the attacker can calculate the correlation coefficients. If the correlation coefficients are significant at certain periods, the key can be discovered and Algorithm 1 can then be rerun for the next chosen plaintext. If there are not any significant correlation coefficients in the first 80 rounds, the selected plaintexts are not desired for the CPA attack on KATAN32. Because our goal is to leverage the TFET CML implementation on KATAN32 to counter the CPA attack, the completed 80-bit key evaluation will not be discussed in detail.

Algorithm 1. CPA on recovering of 80-bit keys of KATAN.

```
Data: plaintext and measured power
Result: correlation results (correct keys)
while uncovered keys ≤ 80 do
  select the plaintext;
  if Power(KATAN) ≃ Power(Intermediates) then
    while # of rounds ≤ 80 do
      run correlation coefficient;
      correct keys ++;
    end
  else
    unsuccessful plaintext ++ and go back to
    select the plaintext;
  end
end
```

VI. DISCUSSION

Here, we briefly discuss the next steps for this work. Potential circuit-level optimizations as well as algorithmic considerations are highlighted.

A. CIRCUIT-LEVEL OPTIMIZATION

In this work, we use TFET based CML gates to realize lightweight ciphers with both high security and low power consumption. As an initial effort we have constructed generic current mode gates (without applying any circuit improvement techniques). However, this will be considered in our future work, and additional improvements with respect to power are expected. For example, the sleeping transistor in [16] can lead to additional energy improvements.

Considering the power advantage of TFET based CML gates, it is also promising that we continue to optimize our circuit specifications and develop the CML standard library. As we have mentioned, the good thing about building a current mode standard cell library is that the standard logic gates can be used to derive additional logic gates by following the pattern of the CML design template. Also, different driving strength designs of one logic gate can be accomplished through the modification of the tail current source.

Binary decision diagrams have also proven to be a practical way to capture the behavior of CML [18]. The core of the differential cell is its pull down network, which manages the functionality of the CML gate. The PDN can be represented using BDDs where each node of the BDD is a differential pair. Each branch of the BDD is a connection between one drain and the source of another differential pair or an output.

B. ENCRYPTION ALGORITHM CONSIDERATION

Besides the optimization of the CML circuit, another goal is to extend the TFET-based CML for more complicated and popular block ciphers, such as AES. Given that a significant amount of work has been done in protecting conventional block ciphers, a concrete analysis is necessary to evaluate the amelioration using a TFET based CML implementation. Among the techniques, composite field S-boxes are widely applied [38]. Polynomial, normal, and mixed basis composite fields will also be analyzed and one of three bases will be chosen for the TFET-based implementation to counter DPA attack. Although a DPA-based attack is mostly employed in attacking block ciphers, other emerging attacks are also worthy of being covered in the future work, such as fault analysis attacks [39]–[43]. Employing the existing techniques, we will study whether TFET-based CML designs are resistant to fault analysis based attacks.

Besides block ciphers, other encryption and authentication algorithms can also be protected using TFET CML. For example, Galois Counter Mode (GCM) is an authenticated encryption mode that simultaneously generates ciphertext and an authentication tag [44]. It can be implemented in hardware to achieve high speeds with low cost and low latency [45]. To incorporate the GCM into our TFET based block cipher implementation, two scenarios are taken into consideration: TFET static and TFET CML implementation. To our knowledge, no work has been done to implement GCM using CML style implementation. We will conduct a detailed theoretical analysis on how to incorporate GCM operation into CML-based cipher design.

VII. CONCLUSION

In this paper, we have demonstrated that the usage of emerging transistors, i.e., TFETs, can help improve circuit design resilience against CPA attacks while still preserving low power consumption compared to their CMOS counterparts. Additionally, besides the traditional criteria for emerging devices such as area, power, delay and non-volatility, security may serve as a new criterion to thoroughly judge the advantages and disadvantages of emerging devices. Using this new standard, we plan to revisit existing emerging transistors to have a full comparison between emerging technologies and CMOS technology. Meanwhile, we believe that more research outcomes are expected in this area where unique properties of emerging transistors can help enhance the security of circuit designs.

ACKNOWLEDGMENTS

X.S. Hu and M. Niemier were supported in part by the Center for Low Energy Systems Technology (LEAST), one of six centers of STARnet, a Semiconductor Research Corporation program sponsored by MARCO and DARPA.

REFERENCES

[1] *Adv. Encryption Standard (AES) FIPS Pub 197.* (2001, Nov.) [Online]. Available: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[2] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. Robshaw, Y. Seurin, and C. Vikkelsoe, "Present: An ultra-lightweight block cipher," in *Proc. 9th Int. Workshop Cryptographic Hardw. Embedded Syst.*, 2007, pp. 450–466.

[3] G. Leander, C. Paar, A. Poschmann, and K. Schramm, "New lightweight des variants," in *Proc. Fast Softw. Encryption*, vol. 4593, pp. 196–210, 2007.

[4] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, and L. Wingers, "The simon and speck families of lightweight block ciphers," Cryptology ePrint Archive, Rep. 2013/404, 2013.

[5] C. Cannière, O. Dunkelman, and M. Knežević, "Katan and ktantan – a family of small and efficient hardware-oriented block ciphers," in *Proc. 11th Int. Workshop Cryptographic Hardw. Embedded Syst.*, 2009, pp. 272–288.

[6] P. C. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Proc. 19th Annu. Int. Cryptol. Conf. Adv. Cryptol.*, 1999, pp. 388–397.

[7] P. Kocher, "Design and validation strategies for obtaining assurance in countermeasures to power analysis and related," in *Proc. Attacks, NIST Phys. Security Workshop*, 2005.

[8] M.-L. Akkar and C. Giraud, "An implementation of DES and AES, secure against some attacks," in *Proc. 3rd Int. Workshop Cryptographic Hardw. Embedded Syst.*, 2001, vol. 2162, pp. 309–318.

[9] S. Yang, W. Wolf, N. Vijaykrishnan, D. Serpanos, and Y. Xie, "Power attack resistant cryptosystem design: A dynamic voltage and frequency switching approach," in *Proc. Des., Autom. Test Eur.*, vol. 3, pp. 64–69 Mar. 2005.

[10] K. Tiri, M. Akmal, and I. Verbauwhede, "A dynamic and differential CMOS logic with signal independent power consumption to withstand differential power analysis on smart cards," in *Proc. 28th Eur. Solid-State Circuits Conf.*, Sep. 2002, pp. 403–406.

[11] Y. Bi, P.-E. Gaillardon, X. Hu, M. Niemier, J.-S. Yuan, and Y. Jin, "Leveraging emerging technology for hardware security—Case study on silicon nanowire FETs and graphene Symfets," in *Proc. IEEE 23rd Asian Test Symp.*, Nov. 2014, pp. 342–347.

[12] Y. Bi, K. Shamsi, J.-S. Yuan, P.-E. Gaillardon, G. D. Micheli, X. Yin, X. S. Hu, M. Niemier, and Y. Jin, "Emerging technology-based design of primitives for hardware security," *J. Emerg. Technol. Comput. Syst.*, vol. 13, no. 1, pp. 3:1–3:19, Apr. 2016.

[13] M. Yamashina and H. Yamada, "MOS current mode logic MCML circuit for low-power GHZ processors," *NEC Res. Develop.*, vol. 36, pp. 54–63, Jan. 1995.

[14] K. Baddam and M. Zwolinski, "Evaluation of dynamic voltage and frequency scaling as a differential power analysis countermeasure," in *Proc. 20th Int. Conf. VLSI Des. Held Jointly 6th Int. Conf. Embedded Syst.*, Jan. 2007, pp. 854–862.

[15] S. Badel, E. Guleyupoglu, O. Inac, A. Martinez, P. Vietti, F. Gurkaynak, and Y. Leblebici, "A generic standard cell design methodology for differential circuit styles," in *Proc. Des., Autom. Test Eur.*, Mar. 2008, pp. 843–848.

[16] A. Cevrero, F. Regazzoni, M. Schwander, S. Badel, P. Ienne, and Y. Leblebici, "Power-gated MOS current mode logic (PG-MCML): A power aware DPA-resistant standard cell library," in *Proc. 48th ACM/EDAC/IEEE Des. Autom. Conf.*, Jun. 2011, pp. 1014–1019.

[17] E. Trichina, T. Korkishko, and K. Lee, "Small size, low power, side channel-immune AES coprocessor: Design and synthesis results," in *Proc. 4th Int. Conf. Adv. Encryption Standard*, 2005, vol. 3373, pp. 113–127.

[18] F. Macé, F.-X. Standaert, J.-J. Quisquater, and J.-D. Legat, "A design methodology for secured ICS using dynamic current mode logic," in *Proc. 15th Int. Workshop Integr. Circuit Syst. Des. Power Timing Model., Optimization Simul.*, 2005, vol. 3728, pp. 550–560.

[19] A. Tajalli, E. Vittoz, Y. Leblebici, and E. Brauer, "Ultra low power subthreshold MOS current mode logic circuits using a novel load device concept," in *Proc. 33rd Eur. Solid State Circuits Conf.*, Sep. 2007, pp. 304–307.

[20] W.-Y. Tsai, H. Liu, X. Li, and V. Narayanan, "Low-power high-speed current mode logic using tunnel-fets," in *Proc. 22nd Int. Conf. Very Large Scale Integr.*, Oct. 2014, pp. 1–6.

[21] Y. Bi, K. Shamsi, J.-S. Yuan, F.-X. Standaert, and Y. Jin, "Leverage emerging technologies for DPA-resilient block cipher design," in *Proc. Des., Autom. Test Eur. Conf. Exhib.*, 2016, pp. 1538–1543.

[22] A. C. Seabaugh and Q. Zhang, "Low-voltage tunnel transistors for beyond CMOS logic," *Proc. IEEE*, vol. 98, no. 12, pp. 2095–2110, Dec. 2010.

[23] H. Lu and A. Seabaugh, "Tunnel field-effect transistors: State-of-the-art," *IEEE J. Electron Devices Soc.*, vol. 2, no. 4, pp. 44–49, Jul. 2014.

[24] U. Avci, R. Rios, K. Kuhn, and I. Young, "Comparison of performance, switching energy and process variations for the TFET and MOSFET in logic," in *Proc. Symp. VLSI Technol.*, Jun. 2011, pp. 124–125.

[25] G. Zhou et al. "Novel gate-recessed vertical INAS/GASB TFETS with record high ion of 180 $\mu a/\mu m$ at vds=0.5 v," in *Proc. IEEE Int. Electron Devices Meet.*, Dec. 2012, pp. 32.6.1–32.6.4.

[26] B. Sedighi, X. Hu, H. Liu, J. Nahas, and M. Niemier, "Analog circuit design using tunnel-fets," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 62, no. 1, pp. 39–48, Jan. 2015.

[27] D. Hisamoto et al."Finfet-a self-aligned double-gate MOSFET scalable to 20 nm," *IEEE Trans. Electron Devices*, vol. 47, no. 12, pp. 2320–2325, Dec. 2000.

[28] H. Lu, J. W. Kim, D. Esseni, and A. Seabaugh, "Continuous semiempirical model for the current-voltage characteristics of tunnel fets," in *Proc. 15th Int. Conf. Ultimate Integr. Silicon*, 2014, pp. 25–28.

[29] H. Lu, D. Esseni, and A. Seabaugh, "Universal analytic model for tunnel {FET} circuit simulation," *Solid-State Electron.*, vol. 108, pp. 110–117, 2015.

[30] V. Saripalli, G. Sun, A. Mishra, Y. Xie, S. Datta, and V. Narayanan, "Exploiting heterogeneity for energy efficiency in chip multiprocessors," *IEEE J. Emerging Select. Topics Circuits Syst.*, vol. 1, no. 2, pp. 109–119, Jun. 2011.

[31] M. Elmasry and M. Allam, "Dynamic current mode logic family," U.S. Patent 6,028,454, Feb. 22, 2000.

[32] S. Badel, I. Hatirnaz, and Y. Leblebici, "Semi-automated design of a MOS current mode logic standard cell library from generic components," in *Proc. Res. Microelectron. Electron., 2005 PhD*, vol. 2, pp. 155–158, Jul. 2005.

[33] N. Debande, Y. Souissi, M. A. E. Aabid, S. Guilley, and J.-L. Danger, "Wavelet transform based pre-processing for side channel analysis," in *Proc. 45th Annu. IEEE/ACM Int. Symp. Microarchit. Workshops*, 2012, pp. 32–38.

[34] J. G. J. van Woudenberg, M. F. Witteman, and B. Bakker, "Improving differential power analysis by elastic alignment," in *Proc. 11th Int. Conf. Topics Cryptol.*, 2011, pp. 104–119.

[35] H. Liu, V. Saripalli, V. Narayanan, and S. Datta, "III-V tunnel FET model," Apr. 2015. [Online]. Available: https://nanohub.org/publications/12/2.

[36] Arizona State University, "PTM model," 2014. [Online]. Available: http://ptm.asu.edu/

[37] G. V. Bard, N. Courtois, J. N. Jr, P. Sepehrdad, and B. Zhang, "Algebraic, aida/cube and side channel analysis of KATAN family of block ciphers," in *Proc. 11th Int. Conf. Cryptol. Progress Cryptol.*, 2010, pp. 176–196.

[38] Y. Nogami, K. Nekado, T. Toyota, N. Hongo, and Y. Morikawa, "Mixed bases for efficient inversion in f((22)2)2 and conversion matrices of subbytes of AES," in *Proc. 12th Int. Conf. Cryptographic Hardw. Embedded Syst.*, 2010, pp. 234–247.

[39] X. Guo, D. Mukhopadhyay, C. Jin, and R. Karri, "Security analysis of concurrent error detection against differential fault analysis," *J. Cryptographic Eng.*, vol. 5, no. 3, pp. 153–169, 2015.

[40] X. Guo, D. Mukhopadhyay, C. Jin, and R. Karri, "NREPO: Normal basis recomputing with permuted operands," in *Proc. IEEE Int. Symp. Hardw.-Oriented Security Trust*, May 2014, pp. 118–123.

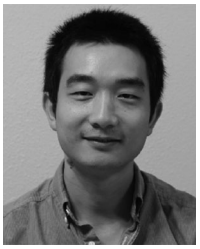
[41] M. Mozaffari-Kermani and A. Reyhani-Masoleh, "A lightweight high-performance fault detection scheme for the advanced encryption standard using composite fields," *IEEE Trans. Very Large Scale Integr. Syst.*, vol. 19, no. 1, pp. 85–91, Jan. 2011.

[42] G. Bertoni, L. Breveglieri, I. Koren, P. Maistri, and V. Piuri, "Error analysis and detection procedures for a hardware implementation of the advanced encryption standard," *IEEE Trans. Comput.*, vol. 52, no. 4, pp. 492–505, Apr. 2003.

[43] S. Bayat-Sarmadi, M. Mozaffari-Kermani, and A. Reyhani-Masoleh, "Efficient and concurrent reliable realization of the secure cryptographic SHA-3 algorithm," *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.*, vol. 33, no. 7, pp. 1105–1109, Jul. 2014.

[44] D. McGrew and J. Viega, "The Galois counter mode of operation," *NIST*, May 2005. [Online]. Available: http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/proposedmodes/gcm/ gcm-spec.pdf

[45] A. Satoh, T. Sugawara, and T. Aoki, "High-performance hardware architectures for Galois counter mode," *IEEE Trans. Comput.*, vol. 58, no. 7, pp. 917–930, Jul. 2009.



YU BI (S'13) received the BSc degree in electronic and information engineering from Xidian University, Xian, China, and the MSc degree in electrical engineering from New York University, New York, NY, in 2010 and 2012, respectively. He is currently working toward the PhD degree in electrical engineering at the University of Central Florida, Orlando, FL. His research focuses on the areas of trusted hardware intellectual property cores, hardware reverse engineering countermeasures, secure and energy-efficient cryptographic systems using emerging transistors, and reliable memory architecture with emerging nonvolatile devices. He is also interested in reliability and optimization of VLSI, analog, and RF circuits. He is a student member of the IEEE.

KAVEH SHAMSI (S'15) received the BS degree in electrical engineering from the Sharif University of Technology, Tehran, Iran, in 2014. He is currently working toward the PhD degree in computer engineering at the University of Central Florida, Orlando, FL. He has been part of the Security in Silicon lab lead by Dr. Yier Jin since 2014. His research experience and expertise include analog and digital circuit design, novel logic design with emerging transistors and memory technologies, hardware security with beyond-CMOS technologies, computer architecture, and IP/IC protection.

JIANN-SHIUN YUAN (S'85-M'88-SM'92) received the MS and PhD degrees from the University of Florida, Gainesville, FL, in 1984 and 1988, respectively. In 1988 and 1989, he was with Texas Instruments Incorporated for CMOS DRAM design. Since 1990, he has been with the faculty of the University of Central Florida, Orlando, FL, where he is currently a professor and the director of US National Science Foundation Multi-functional Integrated System Technology Center. His current research interests include ultra-low power ADC design, hardware security using emerging technology devices, superjunction silicon and GaN power semiconductor devices, RF energy harvesting, and brain-inspired neuromorphic computing. He is a member of Eta Kappa Nu and Tau Beta Pi. He is a founding editor of the *IEEE Transactions on Device and Materials Reliability* and a distinguished lecturer for the IEEE Electron Devices Society. He received the 1995, 2004, 2010, and 2015 Teaching Award, UCF; the 2003 Research Award, UCF; the 2003 Outstanding Engineering Award, IEEE Orlando Section; the Excellence in Research Award at the full professor level of the College of Engineering and Computer Science in 2015; and the Pegasus Professor Award, highest academic honor of excellence at UCF, in 2016.

YIER JIN (S'07-M'12) received the BS and MS degrees in electrical engineering from Zhejiang University, China, in 2005 and 2007, respectively and the PhD degree in electrical engineering in 2012 from Yale University. He is currently an assistant professor in the EECS Department at the University of Central Florida. . His research focuses on the areas of trusted embedded systems, trusted hardware intellectual property (IP) cores, and hardware-software coprotection on computer systems. He proposed various approaches in the area of hardware security, including the hardware Trojan detection methodology relying on local side-channel information, the post-deployment hardware trust assessment framework, and the proof-carrying hardware IP protection scheme. He is also interested in the security analysis on Internet of Things (IoT) and wearable devices with particular emphasis on information integrity and privacy protection in the IoT era. He received the Best Paper Award DAC'15 and ASP-DAC'16.

MICHAEL NIEMIER (S'00-M'03-SM'11) received the BS, MS, and PhD degrees in computer engineering from the University of Notre Dame, IN, in 1998, 2000, and 2004, respectively. While working toward the Ph.D. degree, he was a National Science Foundation graduate research fellow. He is currently an associate professor at the University of Notre Dame. He was a faculty member at the Georgia Institute of Technology, Atlanta, GA, before returning to Notre Dame. His research interests include designing, facilitating, evaluating architectures for emerging technologies with a current emphasis on emerging transistor technologies. He is an active member of the program committees for DAC, DATE, ICCAD, etc. – and has frequently served as the chair of the emerging technologies track at said conferences. He received the IBM Faculty Award and the Best Paper Award at the IEEE Symposium on Nanoscale Architectures, 2009. He also received a Joyce Award for Excellence in Teaching at the University of Notre Dame in 2014. He is a senior member of the IEEE.

XIAOBO SHARON HU (S'85-M'89-SM'02-F'16) received the BS degree from Tianjin University, China, the MS degree from the Polytechnic Institute of New York, and the PhD from Purdue University, West Lafayette, IN. She is a professor in the Department of Computer Science and Engineering at the University of Notre Dame. Her research interests include real-time embedded systems, low-power system design, and computing with emerging technologies. She has published more than 250 papers in the related areas. She served as an associate editor for *IEEE Transactions on VLSI*, *ACM Transactions on Design Automation of Electronic Systems*, and *ACM Transactions on Embedded Computing*. She is the program chair of 2016 Design Automation Conference (DAC) and the TPC cochair of 2014 and 2015 DAC. She received the US National Science Foundation CAREER Award in 1997, the Best Paper Award from Design Automation Conference, 2001, and IEEE Symposium on Nanoscale Architectures, 2009. She is a fellow of the IEEE.