Leverage Emerging Technologies For DPA-Resilient Block Cipher Design

Yu Bi*, Kaveh Shamsi*, Jiann-Shiun Yuan*, Francois-Xavier Standaert†, and Yier Jin*
*Department of Electrical Engineering and Computer Science, University of Central Florida
†Universite Catholique de Louvain (UCL) - Belgium

***Abstract*—Emerging devices have been designed and fabricated to extend Moore's Law. While the benefits over 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 tunneling FETs (TFET) and silicon nanowire FETs (SiNW FETs) could offer superior protection to integrated circuits and embedded systems that are subject to hardware-level attacks – e.g., differential power analysis (DPA). Experimental results on SiNW FET and TFET CML gates are presented. In addition, simulation results of utilizing TFET CML 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), Differential Power Analysis (DPA), Emerging Technologies**

I. Introduction

Modern cryptography systems are facing new challenges with the advent of the Internet of Things (IoT). The energy constrained IoT devices may not be able to afford the energy/area/timing requirements of conventional cryptography such as the Advanced Encryption Standard (AES) [1]. As a results, research on developing light-weight cryptographic systems and algorithms has intensified recently [2]–[4]. Furthermore, distributed IoT devices allow for an easier physical access for an adversary. Therefore, securing cryptographic systems against physical side-channel attacks such as differential power analysis (DPA) becomes a high priority.

Since the introduction of DPA by Kocher et al. [5], there has been a considerable amount of research on developing low-cost and efficient countermeasures. Countermeasures at the algorithm level and the circuit level have been proposed. Kocher suggested designing cryptographic algorithms that can withstand a side-channel attack simply by frequently changing the keys, preventing the attacker from collecting enough power traces [5]. The authors in [6] discussed masking bits during the internal stages to limit information leakage. A circuit level technique that involves inserting random noise on voltage and frequency channels has also been proposed [7].

Following this trend, the design of logic gates which show the property of input-independent power and timing profile becomes one of the leading research topics in this area including the sense-amplifier based logic (SABL) and the current mode logic (CML) [8]. These differential logic styles rely on symmetric branches to deliver voltage difference on their double-terminal output based on a pair of differential input voltages. The drawback with these logic designs, mostly CMOS-based, is their large area and power consumption when compared to static single ended logic, thus trading-off power efficiency for security. For the same reason, the differential logic based circuits are not suitable for resource constraint applications.

In this paper, we study how the DPA resistant circuits can benefit from emerging technologies by replacing CMOS transistors with emerging transistors to achieve the goals of high security and low power consumption. Emerging memory and transistor technologies have already shown their potentials in hardware security applications relying on their unique and unconventional properties [9], [10]. Similar to the previous efforts, we will show that differential logic styles, if combined with emerging transistors, can present significant improvements towards circuit security and power consumption compared to their CMOS counterparts. Our findings also lead to the construction of an emerging transistor-based DPA resistant differential logic library. This library becomes an appealing option for high-performance and high-security cryptographic systems under resource constraint implementations. The contributions of this paper include:

- Silicon nanowire FET (SiNW FET) based CML gates are presented in the paper. We also develop the standard cell design of both tunnel FET (TFET) and SiNW FET based CML with the simulated power and delay information.
- Standard cells of TFET-based CML gates are formalized. The 32-bit lightweight KATAN using TFET-based CML is employed for the evaluation. To our knowledge, this is also the first attempt to use emerging technology based CML gates for the implementation of lightweight cryptography.
- The correlation power analysis on TFET CML based KATAN cipher is performed to show the circuit resilience to side-channel attacks in addition to its much lower power consumption.

The rest of the paper is organized as follows: Section II provides the device overviews of two emerging technologies, TFET and SiNW FET. Section III discusses the design of current mode logic gates using emerging transistors and provides a detailed performance evaluation. Section IV provides a case study of TFET based CML gates application in implementing a lightweight, 32-bit KATAN cipher. Correlation power analysis is also presented. We conclude with Sections V and VI which represents a summary discussion and plans for future work.

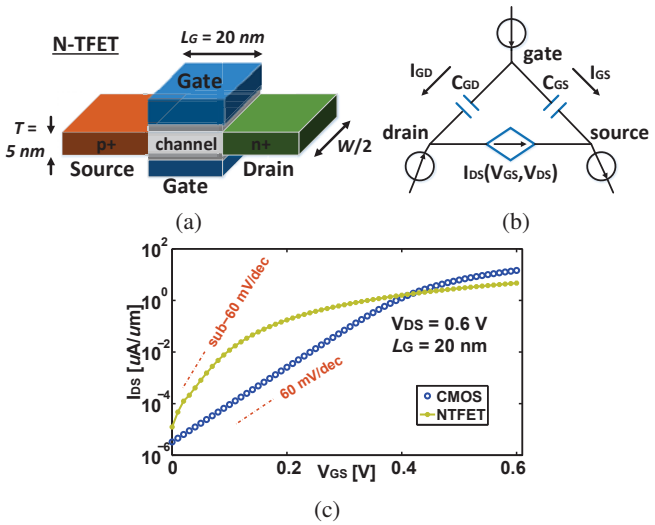


Fig. 1: TFET device modeling: (a) 3-D physical structure of N-type Tunneling FET (b) TFET Verilog-A Model (c) I_{DS} vs. V_{GS} [12] [13].

II. Emerging Devices

A. Tunneling FET

Among different types of proposed tunneling FETs, III-V TFETs appear more promising due to their higher conduction current. GaSb-InAs hetero-junction [11] and InAs homo-junction [12] are two major research directions. Given that InAs homo-junction is more mature in those two devices, we use it as our TFET transistor model in this work. Figure 1a depicts the 3-D physical structure of homo-junction N-type TFET. Compared to conventional CMOS technology, the TFET has asymmetric doping where the source and drain are p-type or n-type doped, respectively[1]. The applied gate voltage can induce a band-to-band tunnel to drive a tunneling current. The high energy carriers in TFET are filtered by the tunneling channel such that a sub-60 $mV/decade$ slope can be achievable at the room temperature [13]. With the steep slope characteristic, TFET can enable the supply voltage scaling to further address conventional CMOS challenges such as oxide breakdown.

As seen in Figure 1b, a look-up table based Verilog-A model has been derived from TCAD Sentaurus for circuit- and system-level simulation [14]. The Verilog-A model is composed of three parts: gate-source capacitance C_{GS}, gate-drain capacitance C_{GD} and the transfer characteristic $I_{DS}(V_{GS}, V_{DS})$. The gate-source current is represented as $I_{GD} = d(C_{GD} * V_{GD})/dt$, while the gate-drain current is expressed as $I_{GS} = d(C_{GS} * V_{GS})/dt$. The pre-measured look-up table that contains a range of fine-step voltage and capacitance values can be referred to calculate the three current models. With the given Verilog-A module, the DC performance of an N-type TFET is presented in Figure 1c, 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. Notably, when the gate-source voltage is less than 0.4 V, the conducting current of TFETs outperforms the CMOS counterpart.

[1]P-type TFET shares the same physical structure with opposite layout of source and drain.

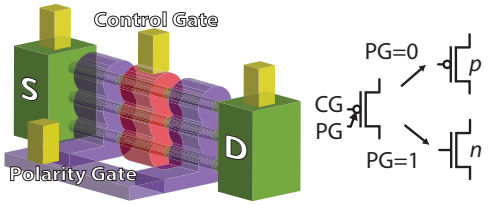


Fig. 2: 3D sketch of the SiNW FETs featuring two independent gates and its associated symbol [15].

B. Silicon NanoWire FET

With the trend towards nano-scale intrinsic material in transistor channels, ambipolar conduction is observed as an undesirable phenomena. However, using dynamic biasing of source and drain Schottky Barrier heights, polarity-controllable FETs have been fabricated using both silicon [15] and carbon nanotubes [16].

In this work we focus on silicon based controllable polarity schottky barrier FETs (SBFETs) that operate in a symmetric logic-range. An illustration of a silicon nano-wire structure firstly fabricated in [15] is depicted in Figure 2. Gate-All-Around (GAA) structures wrap around a number of vertically stacked silicon nano-wires. The GAA gate structure is an evolution of tri-gate FinFET structures with improved leakage characteristics. The polarity gate (PG) regions closer to the drain and source contacts adjust the schottky barrier heights deciding the channel's carrier type and thereby configuring the device's polarity. The control gate provides conventional gate control over the device. Schottky D/S devices have recently been exploited for achieving steep subthreshold in FinFET-like structures [17]. For our SiNW-FET gates circuit simulation we use a model from [15].

III. Current Mode Logic Gates Evaluations

A. Current Mode Logic Introduction

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 [18]–[20]. A "genuine" CML gate is shown in Figure 3. The schematic is mainly divided into two parts: a pull-up network (PUN) and a pull-down network (PDN).

In CML the pull-up network mainly works as the load device to manage the DC voltage drop on the output. Thus, the pull-up network is constructed by either two resistors or P-type FETs (PFETs). In fact, FETs based PUN dominates the design due to its physical advantage over resistors. By simply tuning the gate bias of a PFET, the on-resistance of PFET can be adjusted, thereby altering output voltage accordingly. At

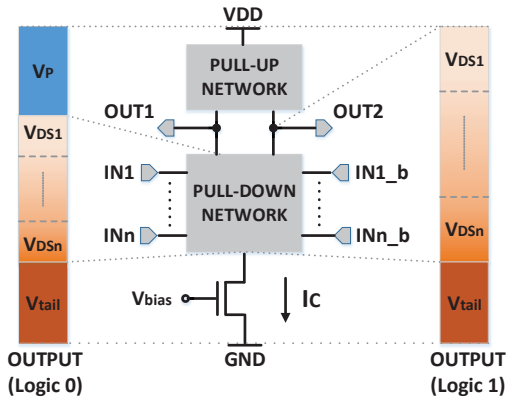
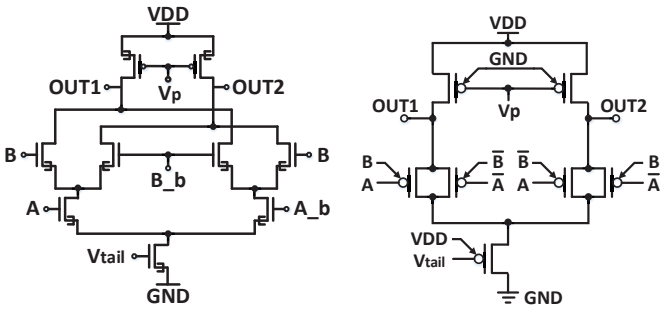


Fig. 3: The universal diagram of CML gate.



(a) (b)

Fig. 4: Two CML XOR schematics using (a) TFET (b) SiNW FET.

the bottom of Figure 3, one N-type FET (NFET) is included to work as a current source, which can determine the value of output voltage swing. The pull-down network that is composed of NFETs 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 NFETs. Due to the differential structure of CML gate, when OUTPUT is logic-1, the voltage level is close to the supply voltage (VDD). When OUTPUT is logic-0, the voltage level is derived as $VDD - R_{on} \times I_C$, where R_{on} is PFET on-resistance and I_C is the constant current controlled by the current source.

B. CML Standard Cells with Two Emerging Devices

The above CML introduction suggests that different layouts of the pull-down network can perform different logic functions. In fact, authors [21] formalized the CML implementation into three levels and multiple differential pairs. Figure 4 depicts two CML examples of exclusive-OR (XOR) gate using TFET and SiNW FET, respectively. The two-input TFET CML XOR gate includes two level and three differential pairs, similar to the conventional CMOS counterpart. On the other hand, the SiNW FET CML XOR gate is enabled by only one level and two differential pairs. The polarity-controllable feature of SiNW FET can further lower the area consumption of circuit implementation, especially for the cryptographic system, where the XOR gates are heavily adopted.

For other CML standard gate designs, it is critical to firstly determine the supply voltage and the voltage optimized swing.

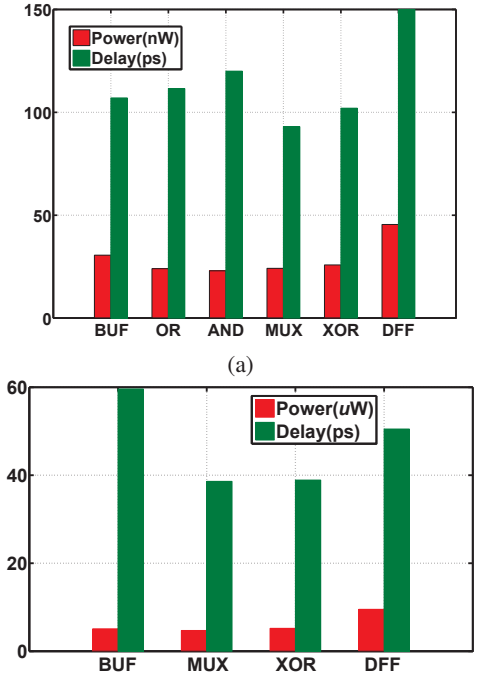


Fig. 5: Power and delay profiles of CML standard cells using (a) TFET (b) SiNW FET.

As analyzed in [14], the TFET threashold voltage is considered as 0.15 V due to the sub-60 $mV/decade$. Therefore, the supply voltage for TFET can be scaled to 0.3 V accordingly. To fairly compare TFET with CMOS, given that the driving current for the TFET with $V_{GS} = 0.15V$ is close to the CMOS with $V_{GS} = 0.3V$, the supply voltage for CMOS is cosidered as 0.6 V. Meanwhile, due to the similar layout shared between SiNW FET and CMOS, we consider the same supply voltage ($VDD = 0.9V$) and voltage swing ($Vsw = 0.45V$) for those two technologies. The configuration of the supply voltage and voltage swing sets the baseline for other parameters such as transistor size and biasing voltages. Here, we configure the widths of three devices to be close to the technology length. Consequently, TFET based CML gates are able to perform the correct functions When $V_{bise} = 0.18V$ and $V_P = 0.14V$, while SiNW FET based CML gates function correctly when $V_{bise} = 0.5V$ and $V_P = 0.2V$. Figure 5 presents the simulated results among two technologies in terms of power and delay profiles. With the scaling supply voltage ($VDD = 0.3V$), the TFET based CML gates trade a higher delay for an overwhelming power advantage. For SiNW FET based CML, it indicates that the performance is becoming better with the increased complexity of functionality.

C. Gate-level Security Analysis

It is worth noting that the difference of the gate-level behaviour between static and CML gates before our implementation of light-weight cipher. It is well known that the key idea of differential power analysis is based on the power consumption during the voltage transition. In static CMOS

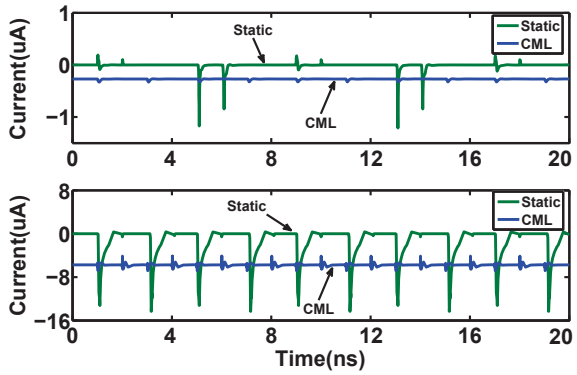


Fig. 6: The power traces between static XOR and CML XOR using TFET (top) and SiNW FET (bottom).

logic, the major power consumption happens when the output of logic undergoes a 0→1 (or 1→0) transition. On the contrary, the CML logic is naturally resistant to a DPA attack given that constant power consumption in almost any transitions.

Figure 6 shows the power traces of four XOR gate implementations using TFET and SiNW FET. The upper two power profiles are the TFET static XOR gate and TFET CML XOR gate, while the lower two traces are the SiNW FET static XOR gate and the SiNW FET CML XOR gate. The simulation results using two devices share the same characteristic that CML XOR gate stays at an constant power consumption compared with the significant power glitch of the static XOR gate. In other words, the power profile of static XOR gate gives away more significant information for the attacker to identify the internal activity of the cryptographic system.

IV. Implementation of Lightweight Cryptographic System

Due to the large area and high power consumption, employing CML gates for cryptographic hardware is not popular. To protect cryptographic circuits against DPA attacks, researchers often adopt other signal processing techniques [22], [23]. However, these solutions incur significant computation cost where the cryptography already involves massive computation and consumes large power and area. As such, lower power, TFET-based CML could be especially valuable when considering devices for the Internet of Things (IoT) and wireless sensor network (WSN) nodes. To address these challenges, in the following sections, we consider the impact of TFET-based CML on a 32-bit KATAN cipher.

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 [4]. 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 7, this 32-bit block is made of 32 registers divided into two parts

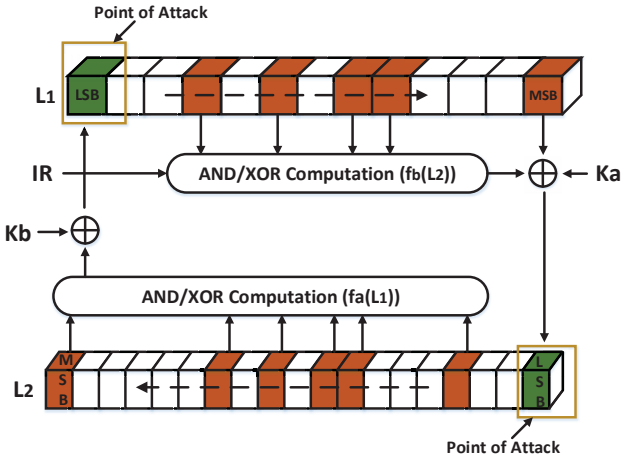


Fig. 7: The abstract schematic of the KATAN ciphers.

– 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 $f_a(L_1)$ and $f_b(L_2)$, can be identified as a combination of AND/XOR calculation in conjunction with different keys (K_a and K_b), and non-linear irregular factor (IR). When the IR counts down 254 rounds from 254 to 0, the KATAN cipher finishes the entire encryption procedure and reads out the ciphertext from 32 registers.

B. CML Implementation on KATAN32

We now discuss how different transistor technologies could impact the power/performance of KATAN32 by using the Synopsys Design Compiler with both 20 nm InAs Homojunction TFET [14] and the PTM 20 nm CMOS technology [24]. 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 HSPICE simulator. The operating frequency of KATAN32 is set as 100 MHz to make sure its functional correctness.

TABLE I: Power Consumption Comparison Among Different Implementations on KATAN32

Technology	Gate Equivalent[#]	Area [μm^2]	Power [μW]
CMOS(Static)	1013	3.534	9.96
CMOS(CML)	393	1.415	170.19
TFET(Static)	1013	3.536	1.89
TFET(CML)	393	1.441	9.76

Area and power data are summarized in Table I, where four different implementations are listed for comparison: two static implementations and CMOS CML employ 0.6 V for the voltage supply, while TFET CML uses 0.3 V. A two-input NAND gate is represented as the gate equivalent. It is worth noting that the number of the synthesized static gate equivalent (GEs) is more than what is reported in [4], 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. With the steep slope feature and scaling supply voltage, both TFET based static and CML implementations lead to a big advantage over the CMOS counterparts. It can fully enable the application of CML based block cipher design with comparable power consumption.

C. Correlation Power Analysis on KATAN32

Although TFET based CML KATAN32 has a better performance, it is still essential to further verify its security, especially the resistance to DPA attack. When considering differential power analysis [5], we first need to identify what intermediate values are a function of plaintext/ciphertext and what intermediate values are a portion of the keys. By observing the KATAN algorithm, it is apparent that the two nonlinear functions $f_a(L_1)$ and $f_b(L_2)$ 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, highlighting in yellow in Figure 7.

Four selected plaintexts are loaded into the two registers as given in Equation (1) and the 80-bit keys are set as all zeros.

$$\begin{aligned} &1: \text{x00000000} \rightarrow p[18]=0, p[31]=0 \\ &2: \text{x80000000} \rightarrow p[18]=0, p[31]=1 \\ &3: \text{x00040000} \rightarrow p[18]=1, p[31]=0 \\ &4: \text{x80040000} \rightarrow p[18]=1, p[31]=1 \end{aligned} \tag{1}$$

However, the chosen input values are not constrained to Expression (1), as long as the plaintext interacts mostly with the subkeys. We use the Hamming weight model as our power model. Based on our chosen plaintexts, the matrix of hypothetical power consumption is listed in Equation (2):

$$\text{Hamming Weight} = \begin{bmatrix} 0 & 1 & 1 & 2 \\ 1 & 0 & 2 & 1 \\ 1 & 2 & 0 & 1 \\ 2 & 1 & 1 & 0 \end{bmatrix} \tag{2}$$

$$\text{Coefficient} = \frac{\sum_{i=1}^{4}(t_i - \overline{t}) \cdot (h_i - \overline{h})}{\sqrt{\sum_{i=1}^{4}(t_i - \overline{t})^2 \cdot \sum_{i=1}^{4}(h_i - \overline{h})^2}} \tag{3}$$

The predicted power consumption is then compared with the measured real power consumption by the correlation coefficient formula as given in Equation (3), where t_i is the measured power trace and h_i is the hypothetical power consumption. The highest correlation coefficient result stands for the correctly guessed keys. In this case, the keys '00' reflect the largest correlation coefficient value. Figure 8 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 of TFET static KATAN32 reaches its highest when the correct keys are applied as shown in Figure 8a. By comparison, the correlation coefficient of TFET CML KATAN32 is much more scattered and all four hypothetical keys are equally distributed as shown in Figure 8b. As a result, it indicates that TFET based CML KATAN32 is more resilient when countering the DPA attacks.

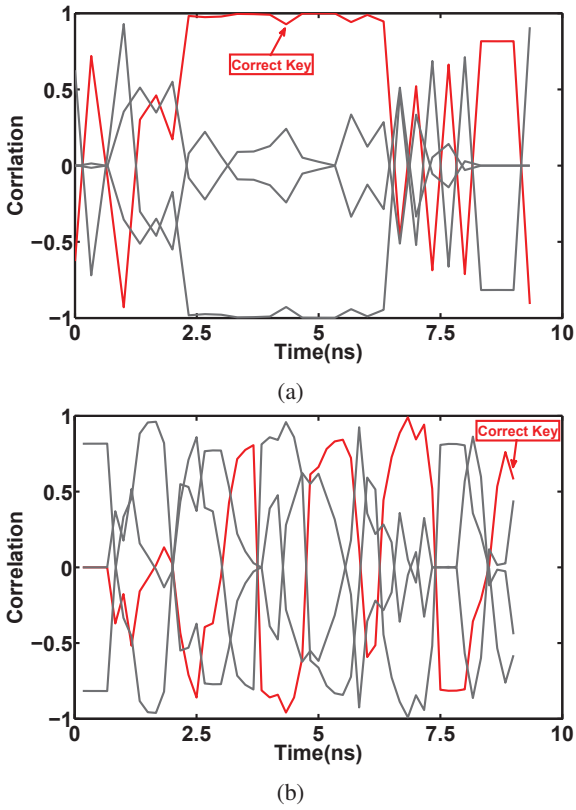


Fig. 8: CPA attack on one clock cycle (a) TFET static KATAN32 vs. (b) TFET CML KATAN32.

V. Discussion and Future Work

In this work, we introduced CML design using two emerging devices (TFET and SiNW FET) and implement TFET based CML KATAN cipher as a case study proving benefits of using emerging transistors balancing circuit performance and security. Besides the discussed two devices, other emerging technologies can also be applied in CML circuit to achieve similar results, e.g, the recently developed negative-capacitance FET (NCFET) [25]. The added ferroelectric layer at the gate in NCFET can generate the negative capacitive effect that enables characteristics of the steep slope subthreashold and tunable hysteresis loop. With the steeper slope feature, the NCFET can further lead to ultra low power application that potentially helps the implementation of CML gates with even lower energy consumption.

Also, the authors in [26] applied sleep technique for the dynamic CML implementation using SiNW FET. Putting CML

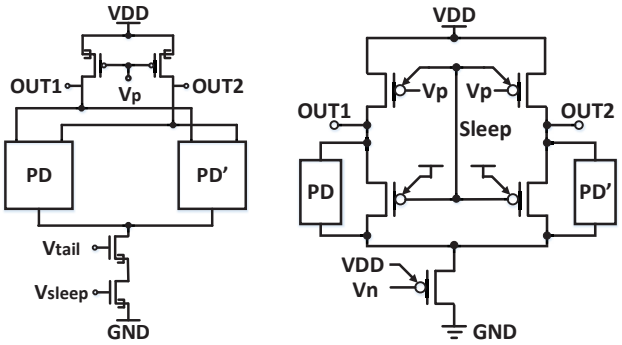


Fig. 9: Power gating techniques on (a) TFET (b) SiNW FET.

circuits into sleep mode can lead to further power saving. Figure 9 depicts new power gating technique employing onto TFET and SiNW FET based CML designs. For the TEFT based CML, a sleep transistor is incorporated at the bottom of the schematic. However, no extra sleep transistor is needed for the SiNW FET based CML. Based on the applied power gating technique, the cryptographic system can work into two modes, standby mode and operation mode, respectively. The cryptographic system is only turned on when the encryption enable signal is on. In our future work, we would like to include both the other emerging technologies and power gating methods into our study to achieve a secure cryptography with even better performance.

VI. Conclusion

In this paper, we have demonstrated that the usage of emerging transistors, i.e. TFETs and SiNW FETs, 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 pros and cons of any 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 circuit security.

References

[1] *Advanced Encryption Standard (AES) FIPS Pub 197 (2001, Nov.).*, [Online]. 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 *Proceedings of the 9th International Workshop on Cryptographic Hardware and Embedded Systems*, 2007.

[3] 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, Report 2013/404, 2013.

[4] C. Cannière, O. Dunkelman, and M. Knežević, "Katan and ktantan – a family of small and efficient hardware-oriented block ciphers," in *Proceedings of the 11th International Workshop on Cryptographic Hardware and Embedded Systems*, 2009.

[5] P. C. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology*, 1999.

[6] M.-L. Akkar and C. Giraud, "An implementation of DES and AES, secure against some attacks," in *Cryptographic Hardware and Embedded Systems — CHES 2001*, 2001.

[7] S. Yang, W. Wolf, N. Vijaykrishnan, D. Serpanos, and Y. Xie, "Power attack resistant cryptosystem design: a dynamic voltage and frequency switching approach," in *Design, Automation and Test in Europe, 2005. Proceedings*, March 2005.

[8] 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 *Solid-State Circuits Conference, 2002. Proceedings of the 28th European*, Sept 2002, pp. 403–406.

[9] 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 *Test Symposium (ATS), 2014 IEEE 23rd Asian*, Nov 2014.

[10] Y. Bi, S. Kaveh, J.-S. Yuan, P.-E. Gaillardon, G. de Micheli, X. Yin, X. Hu, M. Niemier, and Y. Jin, "Emerging technology based design of primitives for hardware security," *J. Emerg. Technol. Comput. Syst., ACM*, Dec. 2015.

[11] G. Zhou, R. Li, T. Vasen, M. Qi, S. Chae, Y. Lu, Q. Zhang, H. Zhu, J.-M. Kuo, T. Kosel, M. Wistey, P. Fay, A. Seabaugh, and H. Xing, "Novel gate-recessed vertical inas/gasb tfets with record high ion of 180 $\mu a/\mu m$ at vds=0.5 v," in *Electron Devices Meeting (IEDM), 2012 IEEE International*, Dec 2012.

[12] 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 *VLSI Technology, 2011 Symposium on*, June 2011.

[13] A. C. Seabaugh and Q. Zhang, "Low-voltage tunnel transistors for beyond cmos logic," *Proceedings of the IEEE*, Dec 2010.

[14] W.-Y. Tsai, H. Liu, X. Li, and V. Narayanan, "Low-power high-speed current mode logic using tunnel-fets," in *Very Large Scale Integration (VLSI-SoC), 2014 22nd International Conference on*, Oct 2014.

[15] M. De Marchi, D. Sacchetto, S. Frache, J. Zhang, P.-E. Gaillardon, Y. Leblebici, and G. De Micheli, "Polarity control in double-gate, gate-all-around vertically stacked silicon nanowire fets," in *Electron Devices Meeting (IEDM), 2012 IEEE International*, Dec. 2012.

[16] Y.-M. Lin, J. Appenzeller, J. Knoch, and P. Avouris, "High-performance carbon nanotube field-effect transistor with tunable polarities," *Nanotechnology, IEEE Transactions on*, 2005.

[17] J. Zhang, M. De Marchi, P.-E. Gaillardon, and G. De Micheli, "A schottky-barrier silicon finfet with 6.0 mv/dec subthreshold slope over 5 decades of current," in *Proceedings of the International Electron Devices Meeting*, 2014.

[18] K. Baddam and M. Zwolinski, "Evaluation of dynamic voltage and frequency scaling as a differential power analysis countermeasure," in *VLSI Design, 2007. Held jointly with 6th International Conference on Embedded Systems., 20th International Conference on*, Jan 2007.

[19] 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 *Design, Automation and Test in Europe, 2008.*, March 2008.

[20] 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 *Design Automation Conference, 2011 ACM/IEEE*, June 2011.

[21] S. Badel, I. Hatirnaz, and Y. Leblebici, "Semi-automated design of a mos current mode logic standard cell library from generic components," in *Research in Microelectronics and Electronics, 2005 PhD*, July 2005.

[22] N. Debande, Y. Souissi, M. A. E. Aabid, S. Guilley, and J.-L. Danger, "Wavelet transform based pre-processing for side channel analysis," in *Proceedings of the 2012 45th Annual IEEE/ACM MICRO*, 2012.

[23] J. G. J. van Woudenberg, M. F. Witteman, and B. Bakker, "Improving differential power analysis by elastic alignment," in *Proceedings of the 11th International Conference on Topics in Cryptology*, 2011.

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

[25] A. Khan, C. Yeung, C. Hu, and S. Salahuddin, "Ferroelectric negative capacitance mosfet: Capacitance tuning amp; antiferroelectric operation," in *Electron Devices Meeting, 2011 IEEE International*, Dec 2011.

[26] L. Amaru, P.-E. Gaillardon, J. Zhang, and G. De Micheli, "Power-gated differential logic style based on double-gate controllable-polarity transistors," *Circuits and Systems II: Express Briefs, IEEE Transactions on*, Oct 2013.