Received 7 July 2020; revised 2 October 2020; accepted 17 October 2020. Date of publication 20 October 2020; date of current version 10 November 2020.
The review of this article was arranged by Editor S. Vaziri.

Digital Object Identifier 10.1109/JEDS.2020.3032635

Using the MSET Device to Counteract Power-Analysis Attacks

ASSAF PELED (Member, IEEE), LIRON DAVID, OFER AMRANI, YOSSI ROSENWAKS, AND AVISHAI WOOL (Senior Member, IEEE)

Department of Electrical-Engineering–Systems and Physical-Electronics, Tel-Aviv University, Ramat-Aviv 69978, Israel

CORRESPONDING AUTHOR: A. PELED (e-mail: assafpeled@gmail.com)

ABSTRACT One pivotal countermeasure in dealing with side-channel power analysis attacks is to maintain the signal-to-noise ratio of the power readings associated with the target as data-independent and as low as possible, in order to limit the attacker's ability to deduce meaningful information from the target. The following study shows that the MSET (Multiple-State Electrostatically-Formed Nanowire Transistor) device achieves these two desired outcomes by virtue of its low-power characteristics, therefore having an inherent advantage in terms of side channel attacks over prevalent technologies. This advantage is tested with an SRAM cell and a memory register. Using correlation metrics, the correlation coefficient of the Hamming distance to the power dissipation in the register - at the adversary's point of observation - is shown to be close to zero over multiple power traces, when the register is implemented in MSET technology.

INDEX TERMS MSET, power-analysis attacks, side-channel attacks, low-power transistors.

GLOSSARY

MSET	Multiple-State Electrostatically-formed Nanowire transistor.
EFN	Electrostatically-Formed Nanowire
FDSOI	Fully-Depleted Silicon on Insulator
SCA	Side-Channel Attacks
PAA	Power-Analysis Attacks
JG	Junction-Gate.

I. INTRODUCTION

The combined capabilities of the MSET (Multistate Electrostatically-Formed Nanowire Transistor) design and unconventional operation have been subject to recent studies [1], [4] which demonstrated the MSET's pronounced benefits at low-power and low-voltage in a variety of applications. Originally emerging from the EFN device [2], [3], the first MSET prototypes were mainly confined to applications requiring multiplexing [5], [6] or threshold-logic [7], whereas the MSET models that ensued enabled implementation of logic gates [1] and SRAM cells [3].

The double-drain MSET is presented in Fig. 1-top along with its characteristic dimensions. The device follows the principles of operation of a double-gate JFET [8], with the exception of having one source but two or more drain terminals. In Fig. 1 the SOI-based [9] MSET's bulk is surrounded on both sides by two junction-gates which form a one-sided abrupt pn-junction with the bulk (with both JG doped $N_{JG} = 10^{19} cm^{-3}$ and bulk oppositely doped $N_{bulk} = 5 \cdot 10^{17} cm^{-3}$).

By applying a differential bias between the junction gates, the depletion region around the corresponding gate expands or contracts accordingly, allowing to control the conduction channel from the source (denoted 'S') and direct it to either the left or the right drain (denoted 'D1' and 'D2', respectively). The drains are separated by an oxide barrier to suppress current leakage, with the barrier extending all the way down to the SOI-BOX. Shallow trench isolations (STI) are located around the device corners.

The switching mechanism of the MSET's conduction channel depends on the limiting of its dynamic voltage range to $\pm 0.25V$, to prevent excess forward current at the junction-gates during normal operation. This range permits MSET-based logic structures to be realized with fewer devices [1] – compared to other technologies - by integrating multiple drain contacts on a single transistor. The

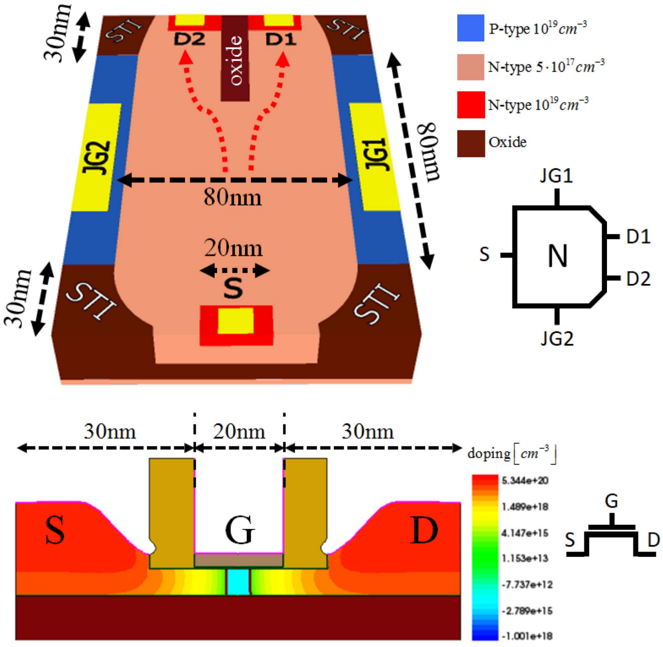

FIGURE 1. Top: MSET device illustration with characteristic dimensions. Bottom: Fully-depleted SOI (FDSOI) MOSFET illustration with characteristic dimensions. Device symbols of N-type MSET and N-type FDSOI appear sideways.

MSET SRAM cell presented in the following section is of no exception in that regard.

When digital functions are embedded in CPU or memory blocks, the information leaking from the devices involved may be exploited by malicious adversaries [10], [11], [12], [13]. As the range of MSET applications continuously grows, when the MSET devices process sensitive information and implements cryptographic calculations, power analysis attacks become an issue to consider with care. In the vast field of side-channel attacks, Power-Analysis Attacks [14], [15], [16], [17] (PAA) are a common practice, and are considered economical due to the relatively inexpensive equipment which is normally required for performance. PAAs are set to interpret the power consumption during cryptographic operations by employing statistical methods to correlate input/output transition with the power consumption at selected observation points across the CMOS circuit. By contrast, PAA countermeasures aim at diminishing the power dependency during these logic transitions.

The literature lists several countermeasure procedures that reduce the physical impact of information leakage. Broadly speaking, these protective measures can be classified as follows; in the algorithmic level, random process within the target device may include the interleaving of “dummy” instructions to avoid sequential execution and detection of the secret algorithm; on the architectural level, random superfluous hardware operations can hinder the attacker’s performance by de-correlating the input data with the device’s power readings. Dual-Rail Pre-charge Logic (DPL) is a widely encountered logic style that aims to provide constant power consumption at each clock cycle by using differential signaling.

The Sense Amplifier Base Logic [18] (SABL) uses a fixed amount of charge for each logic transition, including during the degenerated events when the gate’s logic state retains its current value. Wave-Dynamic Differential Logic [19] (WDDL) emulates the dual-rail pre-charge style and uses complementary logic to balance the circuit activities. Dynamic Mode Logic (DyCML) uses current mode behavior and was originally proposed in [20], [21]. Low-Swing Current Mode Logic [22] (LSCML) follows a similar line of reasoning, in which the current swing is independent of the value of the output load capacitance. Masked Dual Rail Pre-charge Logic [23] (MDPL) was introduced to overcome the routing constraint present in dual-rail gates.

The foregoing solutions entail considerable degree of redundancy in the number of transistors, therefore complicating the overall design flow and inevitably incurring power losses. The study in [24], for example, puts forward the theoretical strengths and weaknesses of the above countermeasure styles by investigating the power consumption of several elementary logic gates with a 130nm CMOS technology. Whereas the average power supply current of a CMOS-AND2 gate is 1.19μA, the WDDL implementation of the same gate uses 8 times as much current, while the MDPL solution reaches 16 times that value. Moreover, the SCA resistive styles are disadvantageous in terms of design complexity and total area covered. To name one example, an SABL implementation of a NAND gate would require 18 transistors, while WDDL and MDPL involve 24 transistors each.

The aim of the remaining paper is twofold; first, we take an SRAM-cell and a memory register as test cases for evaluating the electrical characteristics of the MSET versus a 22nm FDSOI MOSFET (see: Fig. 1) implementation of these circuits; secondly, in light of the MSET low-power characteristics, our study expounds the MSET advantages in greater detail in the context of PAA, and demonstrates the inbuilt potential of this transistor to impede attackers from interpreting power consumption measurements collected during cryptographic operations, thus excluding any need to incorporate redundant transistors to form PAA-resistant variants.

II. MSET POWER ANALYSIS ATTACKS

Figure 2 shows two schematic configurations of an SRAM cell. The right-hand side – implemented with the FDSOI-MOSFET depicted in Fig. 1 – shows the classic cross-coupling inverters that form the bi-stable latch which holds the cell’s data. When the Wordline (WL) is at logic ‘0’, the access transistor (M5) disconnects the Bitline (BL) during read and write operations. Note that the common six-transistor configuration has been reduced in the scope of our analysis to a 5T structure for power-saving considerations.

The left-hand diagram in Fig. 2 is of a 3T MSET-based SRAM cell that follows a similar concept. MSETs S1 and

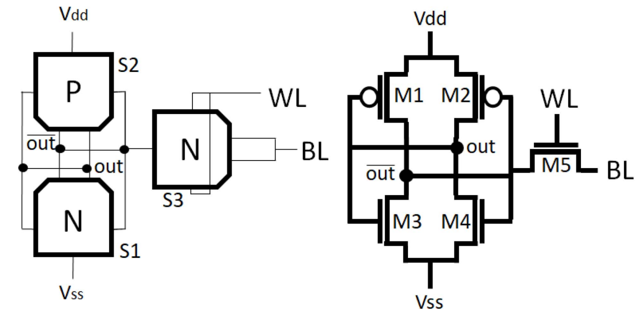

FIGURE 2. Left: SRAM cell schematics – MSET implementation. Right: SRAM cell schematics – FDSOI MOSFET implementation.

S2 constitute the cell's feed-forward latch, while data flow is controlled by access MSET S3. The MSETs are annotated 'N'-type or 'P'-type in accordance with the bulk doping. Details on the MSET-SRAM principles of operation and characteristics have been compiled in depth in [3].

The power consumption of the cell, or a register for that matter, can be monitored by inserting a small resistor within the supply chain, e.g., below the lower-end supply rail of the integrated circuit target device. Acquisition tools such as multi-channel oscilloscope normally accompany this type of attacks, and a computer is additionally used to conduct statistical analysis on the PAA traces. To measure the SRAM-cell power consumption, a small 1-Ohm resistor is inserted in series with the ground input [10], as seen in Fig. 3. The voltage difference across the resistor divided by the resistance yields the current, as illustrated in Fig. 3. From that point on, simple power analysis of the traces as measured on the resistor may serve to interpret the cell's power consumption and deduce information about its performed operations.

Figure 3 plots all four logic transitions of the abovementioned configuration for both the MSET and the FDSOI. The two devices were simulated in TCAD-Sentuaurs, employing mixed-mode simulations that enable analog components to be simulated in conjunction with finite-element models of the MSET and the FDSOI-MOSFET. As the dynamic range varies between the MSET and the MOSFET ($\pm 0.25V$ and $\pm 1V$ for the MSET and MOSFET, respectively), BL and WL in Fig. 3 are represented by logic values '0' and '1' for simplicity of notation. BL is assigned a square wave toggling between logic '1' and '0' with a 20ns duty cycle.

During assertion of WL, it can be readily observed that the FDSOI has an apparent advantage in terms of transition speed. The MSET has its inherent limitations stemming from the relative proximity of its five terminals. In the case of '1' to '0' logic transition (6.5ns-10.5ns), the MSET-SRAM's "OUT" node (see: Fig. 2) gradually acquires a negative value (−0.25V, or, '0' logic), whereas the right junction-gate of N-MSET S1 is at positive bias, therefore the right drain-right JG of S1 becomes steadily reversed biased, narrowing its pull-down current.

By contrast, from power-analysis attack perspective, the MSET-SRAM shows some remarkable advantages over the FDSOI. Fig. 3 (bottom part), shows the test-resistor currents in the MSET and FDSOI's SRAM configurations. Unlike the FDSOI, the I_R signals of the MSET configuration for each transition are virtually similar within a range of marginal

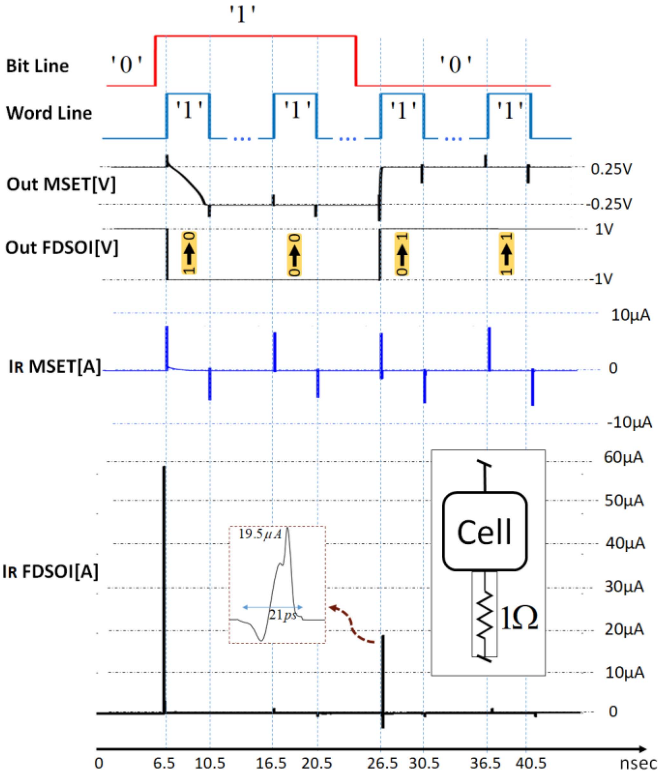

FIGURE 3. Bit-to-bit transition characteristics of an MSET and a MOSFET SRAM cell. Top to bottom: bit-line signal; word-line signal; MSET cell output; MOSFET cell output; test-resistor current in the MSET cell; test-resistor current in the MOSFET cell.

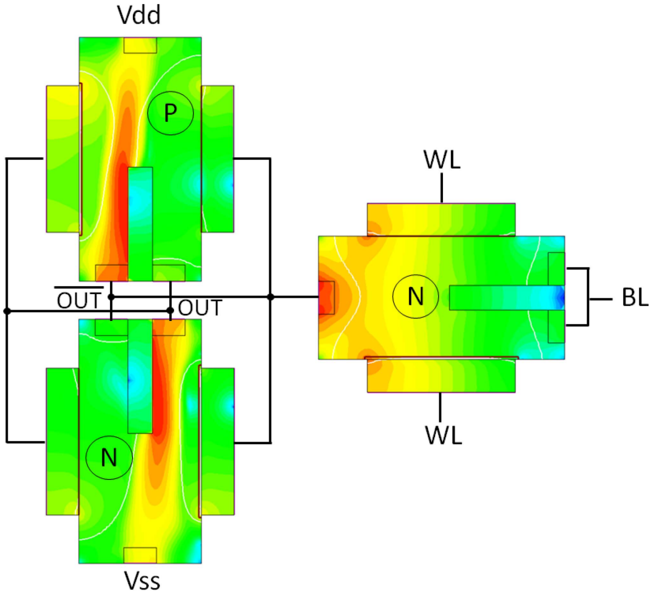

FIGURE 4. Transient-state capture from TCAD-Sentaurus at around 16.5ns (logic '0' to logic '0' switching activity), with qualitative display of current density within the MSET devices comprising the SRAM cell.

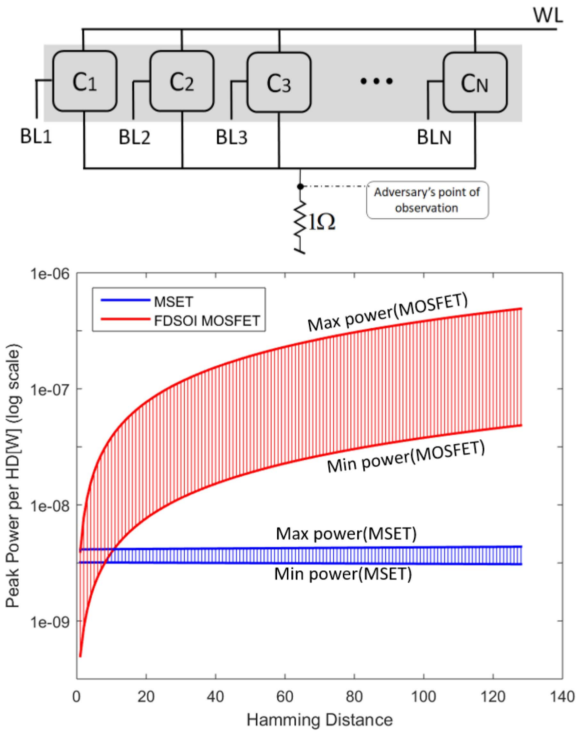

FIGURE 5. Top: N-bit register connected to a pull-down test resistor. The adversary's point of observation is annotated above the test resistor. Bottom: Power consumption limits vs Hamming distance.

TABLE 1. Key parameters–MSET and FDSOI SRAM.

Operation	MSET-SRAM	FDSOI_SRAM
$T_R(0\to0)$	10psec	24psec
$T_R(0\to1)$	10psec	21psec
$T_R(1\to0)$	9psec	30psec
$T_R(1\to1)$	10psec	23psec
$P_R(0\to0)$	24.98pW	0.94pW
$P_R(0\to1)$	24.09pW	378.4pW
$P_R(1\to0)$	34.08pW	38.3nW
$P_R(1\to1)$	32.09pW	0.93pW
$W_R(0\to0)$	$2.81\cdot10^{-23}J$	$3.79\cdot10^{-23}J$
$W_R(0\to1)$	$4.41\cdot10^{-23}J$	$1.11\cdot10^{-21}J$
$W_R(1\to0)$	$1.68\cdot10^{-22}J$	$3.98\cdot10^{-20}J$
$W_R(1\to1)$	$2.15\cdot10^{-23}J$	$2.91\cdot10^{-23}J$

error. The MSET cell can therefore impede the adversary's attempts to determine the data stored in the cell, as each transition between bit values contributes near identical power consumption.

An in-depth inspection into the "degenerated" switching activities ('0' to '0', '1' to '1') of the MSET-cell reveals to some extent the source of similarities between the test-resistor currents among its 4 logic transient modes. Fig. 4 captures the MSET-cell during the '0'-to-'0' transition, i.e., slightly after 16.5ns as seen in the I-V diagram of Fig. 3. The '0'-'0' WRITE cycle begins by applying logic '1' to the bit-line – BL (Note that due to its complementary logic structure, we define the cell OUT node as the output of the first feed-forward inverter. Therefore, '0' logic output requires logic '1' at the BL node).

The WL nodes of the access-MSET are then asserted and for a brief period, excess forward current from the access-MSET's junction gates find its way into the N-cell and P-cell MSETs at their non-cutoff sections. As the OUT node retains its '0' logic value, the right-hand side of the N-MSET is open for conduction. Moreover, as described above, a conduction path is also formed between the WL junctions of the access-MSET and the forward-biased right-hand JG of the cell's N-MSET. These parasitic currents, however limited, are sensed by the test resistor, such that the '0'-'1' and '1'-'0' currents are eventually balanced out by the uneventful switching states.

Table 1 summarizes the central test-resistor parameters: the duration of transition measured on the pull-down resistor (denoted T_R), resistor measured peak-power (denoted P_R) and transition energies (denoted W_R). The energy dissipated in the test resistor for a single cell configuration is calculated as:

$$W_R(b_1 \to b_2) = \int_{T_R(b_1\to b_2)} I_R^2 dt \qquad (1)$$

with $b_1 \to b_2$ indicating the transition between two distinct or similar logic levels, I_R is the transistor current and $T_R(b_1 \to b_2)$ is the duration of transition in which said current starts and ends its excursion.

When measuring power consumption in the FDSOI configuration in either supply rail, the highest peak in power should appear during charge of the cell's output capacitance, i.e., with the '0'-to-'1' transition. During discharge, however, the only current measureable is the short circuit path to the ground rail. This data-dependent power consumption distinguishes the side-channel information leakage in the FDSOI case.

Shown in Table 1, the energy consumption of the test resistor described by Eq. (1), in either technology, depends on the switching activity during WRITE operation into the cell. Unlike the MOSFET-cell, the energy consumption of different transitions in the MSET-cell are much closer to each other. In The FDSOI MOSFET, "no change" transitions 0-to-0, 1-to-1 consume energy 2 to 3 orders of magnitude less than the 0-to-1 and 1-to-0 transitions. Conversely, all four transitions in the MSET consume energy in the same order of magnitude, making it harder for the adversary to reveal the bit values being processed.

Taking this chain of reasoning one step further, these findings permit to elaborate our discussion from the cell onto the register level. An N-bit register comprising N cells is illustrated in Fig. 5. Let us assume that the memory register is connected to some cryptographic circuitry, storing an N-bit word. From the attacker's perspective, the register is an abstract mathematical object, or a black box, that should in principle exhibit specific characteristics for a set of different inputs. The dynamic power consumption of the register depends on the number of switching activities during WRITE operation, i.e., on the Hamming distance between the current word written in the register and the new word about to be written. By definition, The Hamming distance is the number of bit positions in which the two words differ. Put differently, let a binary word in an N-bit register be coded as $\sum_{j=0}^{N} b_j \cdot 2^j$, with the bit values $b_j = \{0, 1\}$, then the Hamming distance between two N-bit words with bit values b_j and d_j is simply:

$$HD = \sum_{j=1}^{N} |b_j - d_j| \tag{2}$$

For a given Hamming distance (HD) between two N-bit words, the minimum and maximum peak power that can be measured on the pull-down resistor of the register in Fig. 5 is:

$$(N - HD) \cdot \min(P_{0\to0}, P_{1\to1}) + HD \cdot \min(P_{0\to1}, P_{1\to0}) \tag{3}$$

$$(N - HD) \cdot \max(P_{0\to0}, P_{1\to1}) + HD \cdot \max(P_{0\to1}, P_{1\to0}) \tag{4}$$

with $P_{bit1\to bit2}$ being the peak power as measured on the resistor for the transition between bit1 and bit2.

Taking for example a 128-bit register, Fig. 5 shows the total peak power on the resistor for both devices, as a function of the Hamming distance between two successive words. The thick lines in the plot designate min and max limits in which the total peak power may reside. Most significantly, the peak-power limits in the MSET case remain near identical, irrespective of the Hamming distance, whereas those of the MOSFET increase with HD, thus reinforcing the observation that the adversary should encounter difficulties in determining a straightforward relationship between the MSET register's internal data and its externally observable power consumption [10].

Further on, suppose that the adversary selects the inputs that are fed into to the target register. If the adversary assumes that the power consumption at the point of observation in either technology depends on the switching activity during computation, the Hamming distance model can serve well to predict the leakage as measured on the test resistor in a correlation power attack. The adversary monitors the power consumption at the register's point of observation (see: Fig. 5) and obtains a leakage vector $\bar{L} = \{L_i\}_{i=1}^{N}$ that contains leakage traces corresponding to the inputs assigned by the adversary. Having the leakage traces obtained from the acquisition device, the adversary can apply statistics [25], [26], [27] to compare the predicted leakage traces corresponding to the input vectors. In theory, the adversary would anticipate the overall measured power consumption to rise as the Hamming distance between two successive input words increases. Therefore, to challenge the adversary's hypothesis, the target device leakage should be independent of the external inputs admitted.

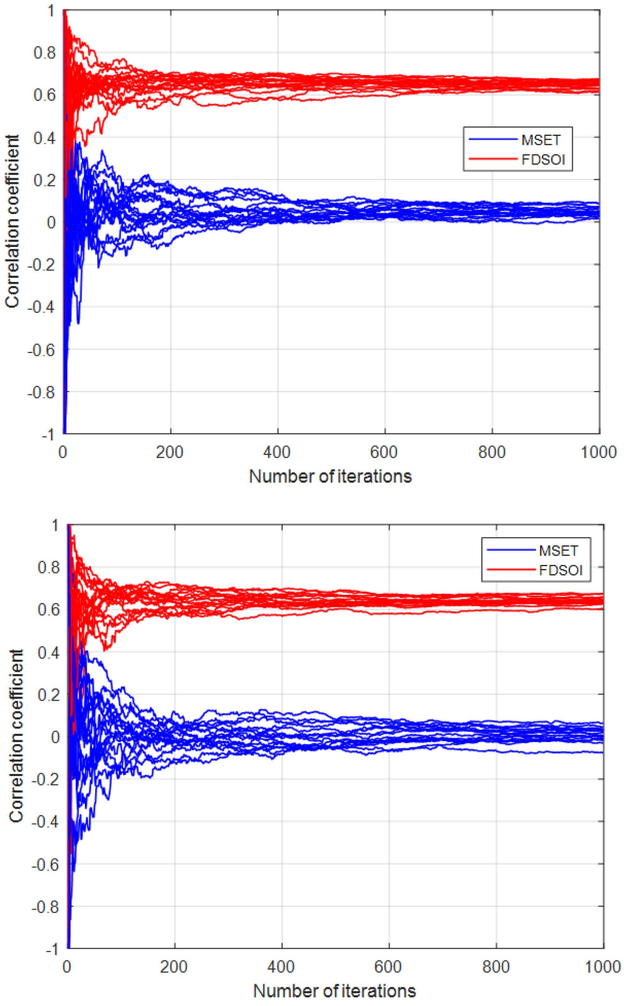

FIGURE 6. HD-to-peak power cross-correlation traces. Top: SNR = 25dB. Bottom: SNR = 15dB.

Suppose that the target device is a 16-bit register as illustrated in Fig. 5. To test his/her theory, the adversary performs the following inspection; an input vector $\{I_i\}_{i=1}^{N}$ comprising N 16-bit input words are fed into the register, such that each pair of successive words have different Hamming distance, HD. The peak power consumption at the point of observation is recorded as each successive word is being fed. The adversary uses the following classical statistics to correlate HD and the measured peak power at every input iteration:

$$\rho(n) = \frac{\sum_{i=1}^{n}\left(HD_i - \langle HD\rangle_1^n\right) \cdot \left(\hat{p}_i - \langle\hat{p}\rangle_1^n\right)}{\sqrt{\sum_{i=1}^{n}\left(HD_i - \langle HD\rangle_1^n\right)^2 \cdot \sum_{i=1}^{n}\left(\hat{p}_i - \langle\hat{p}\rangle_1^n\right)^2}} \tag{5}$$

where $\rho(n)$ is the correlation coefficient conforming to the first n-consecutive input words, $\langle HD\rangle_1^n$ is the mean value of HD associated with the n-words, $\hat{p}_i$ the peak power measured as the i-th word is fed, and $\langle\hat{p}\rangle_1^n$ the mean value of peak power measurement as summations are taken over the 'n' samples at each iteration step.

Fig. 6 shows multiple correlation power analysis traces as derived from Eq. (5), each of which iteratively computes the correlation coefficient over 1000 consecutive inputs. Out of

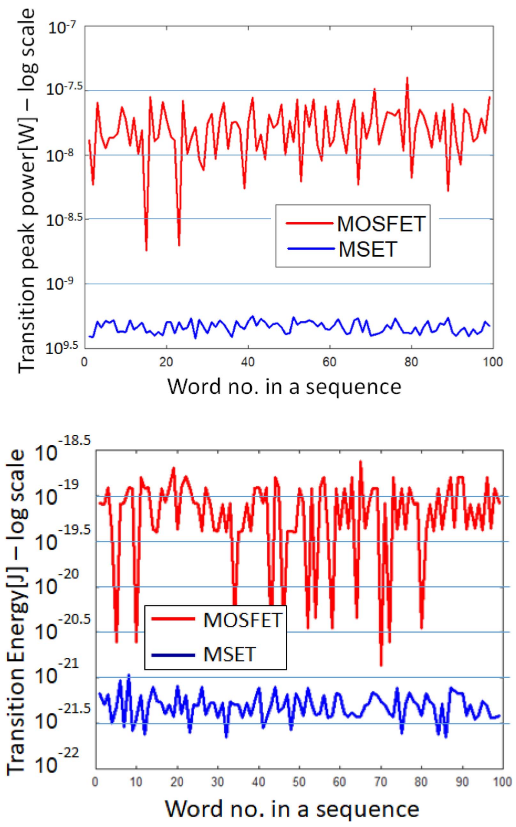

FIGURE 7. Successive binary words when a random sequence is applied. Top: Register pull-down resistor's peak power (log scale); Bottom: Register pull-down resistor's energy consumption (log-scale).

TABLE 2. Optimal correlation coefficient obtained vs. SNR.

OPTIMAL CORRELATION COEFFICIENT OBTAINED VS. SNR		
SNR[dB]	MSET	FDSOI
25	0.08	0.71
15	0.06	0.67

all the traces obtained in the test runs in Fig. 6, the adversary performs an exhaustive search to identify the trace having the highest $\rho(N = 1000)$, and then completes his "black-box" attack on the target device by revealing its input-output relationship. To render the analysis in Fig. 6 more realistic, additive random Gaussian noise is superimposed on the peak power values to create a disturbance that affects the attacker's efficiency. The top image in Fig. 6 corresponds to a high SNR of 25[dB], whereas the bottom image has SNR = 15[dB].

As expected, the optimal $\rho(N = 1000)$ commensurate with the SNR both for the MSET and the FDSOI. The correlation coefficient (ideally, close to 1) in each SNR case is tabulated in Table 2. As the power readings of the MSET-register at the point of observation are nearly balanced, the correlation traces are close to 0, thus eliminating the amount of information in the power leakages. To complete the picture, the adversary may choose to exploit the entire time-dependent power readings of the test resistor rather than their peak power, by averaging or integrating them to produce traces of energy. Fig. 7 plots the peak power and energy consumption profile of the test resistor for successive transitions between 8-bit words in a random sequence. The figure shows that apart from a small number of transitions, the peak power and energy consumption in the MSET's case study is roughly 2 orders of magnitude lower than the MOSFET's, rendering the signal readouts less detectable by decreasing their signal to noise ratio.

III. CONCLUSION

Previous studies on the MSET have demonstrated its low-power characteristics as well as the use of a reduced number of devices to form a variety of logic structures. These achievements are augmented in the current work by showing the inherent advantages of the MSET with regard to power analysis attacks. We consider a case study where fundamental integrated-circuits building blocks - in the example of SRAM cell and a memory register - are subject to non-invasive attacks by adversaries who wish to extract meaningful information from said circuits by probing its power. An elementary SRAM cell is examined first, wherein the cell is implemented in MSET technology and with fully-depleted SOI MOSFET in a 22nm technology node. Our analysis shows that the power measured at the point of observation of the adversary has near constant value in the MSET case, irrespective of the switching activities performed. We then elaborate on the implications of the latter findings by studying the behaviour of an N-bit memory register in the face of power analysis attacks. Our discussion shows that due to the near undistinguishable nature of the power signals at the point of attacker's observation, the foundations of power analysis attacks are virtually removed in the MSET case. Taking the Hamming distance as a metric to correlate the total power consumption of the register with the total number of switching activities, our study shows remarkably low correlation coefficient values over multiple generated power traces against the backdrop of additive noise.

REFERENCES

[1] A. Peled, O. Amrani, Y. Rosenwaks, and Y. Vaknin, "A paradigm for integrated circuits based on the MSET transistor," *IEEE Trans. Electron Devices*, vol. 65, no. 3, pp. 1192–1197, Mar. 2018, doi: 10.1109/TED.2017.2788563.

[2] G. Shalev, "The electrostatically formed nanowire: A novel platform for gas-sensing applications," *Sensors*, vol. 17, no. 3, p. 471, Mar. 2017, doi: 10.3390/s17030471.

[3] A. Henning, N. Swaminathan, A. Godkin, G. Shalev, I. Amit, and Y. Rosenwaks, "Tunable diameter electrostatically formed nanowire for high sensitivity gas sensing," *Nano Res.*, vol. 8, no. 7, pp. 2206–2215, 2015. [Online]. Available: https://doi.org/10.1007/s12274-015-0730-1

[4] A. Peled, X. Hu, O. Amrani, J. S. Friedman and Y. Rosenwaks, "An SRAM based on the MSET device," *IEEE Trans. Electron Devices*, vol. 66, no. 3, pp. 1262–1267, Mar. 2019, doi: 10.1109/TED.2019.2892319.

[5] G. Segev, I. Amit, A. Godkin, A. Henning, and Y. Rosenwaks, "Multiple state electrostatically formed nanowire transistors," *IEEE Electron Device Lett.*, vol. 36, no. 7, pp. 651–653, Jul. 2015, doi: 10.1109/LED.2015.2434793.

[6] M. Assif, G. Segev, and Y. Rosenwaks, "Dynamic and power performance of multiple state electrostatically formed nanowire transistors," *IEEE Trans. Electron Devices*, vol. 64, no. 2, pp. 571–578, Feb. 2017, doi: 10.1109/TED.2016.2635148.

[7] J. S. Friedman, A. Godkin, A. Henning, Y. Vaknin, Y. Rosenwaks, and A. V. Sahakian, "Threshold logic with electrostatically formed nanowires," *IEEE Trans. Electron Devices*, vol. 63, no. 3, pp. 1388–1391, Mar. 2016, doi: 10.1109/TED.2015.2512818.

[8] H. Ding, J. J. Liou, K. Green, and C. R. Cirba, "A new model for four-terminal junction field-effect transistors," *Solid-State Electron.*, vol.50, no.3, pp. 422–428, 2006, doi: 10.1016/j.sse.2006.01.001.

[9] J.-T. Park and J.-P. Colinge, "Multiple-gate SOI MOSFETs: Device design guidelines," *IEEE Trans. Electron Devices*, vol.49, no.12, pp. 2222–2229, Dec. 2002, doi: 10.1109/TED.2002.805634.

[10] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Proc. Adv. Cryptol.*, 1999, pp. 388–397. [Online]. Available: https://www.paulkocher.com/doc/DifferentialPowerAnalysis.pdf

[11] P. C. Kocher, "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems," in *Advances in Cryptography (CRYPTO)* (Lecture Notes in Computer Science), vol. 1109, N. Koblitz, Ed. Berlin, Germany: Springer, 1996. [Online]. Available: https://doi.org/10.1007/3-540-68697-5_9

[12] J. J. Quisquater and D. Samyde, "Electromagnetic analysis (EMA): Measures and counter-measures for smart cards," in *Smart Card Programming and Security. E-Smart* (Lecture Notes in Computer Science), vol. 2140, I. Attali and T. Jensen, Eds. Berlin, Germany: Springer, 2001. [Online]. Available: https://doi.org/10.1007/3-540-45418-7_17

[13] K. Gandolfi, C. Mourtel, and F. Olivier, "Electromagnetic analysis: Concrete results," in *Cryptographic Hardware and Embedded Systems (CHES)* (Lecture Notes in Computer Science), vol. 2162, C. K. Koc, D. Naccache, and C. Paar, Eds. Berlin, Germany: Springer, 2001. [Online]. Available: https://doi.org/10.1007/3-540-44709-1_21

[14] S. Mangard, E. Oswald, and T. Popp. (2008). *Power Analysis Attacks: Revealing the Secrets of Smart Cards*. [Online]. Available: https://www.springer.com/gp/book/9780387308579

[15] F. Schellenberg, D. R. E. Gnad, A. Moradi, and M. B. Tahoori, "An inside job: Remote power analysis attacks on FPGAs," in *Proc. Design Autom. Test Eur. Conf. Exhibition (DATE)*, 2018, pp. 1111–1116.

[16] T. Popp, S. Mangard, and E. Oswald, "Power analysis attacks and countermeasures," *IEEE Des. Test. Comput.*, vol 24, no. 6, pp. 535–543, Nov./Dec. 2007,

[17] D. Bellizia, S. Bongiovanni, P. Monsurro, G. Scotti, and A. Trifiletti, "Univariate power analysis attacks exploiting static dissipation of nanometer CMOS VLSI circuits for cryptographic applications," *IEEE Trans. Emerg. Topics Comput.*, vol 5, no. 3, pp. 329–339, Jul.–Sep. 2017,

[18] 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. IEEE 28th Eur. Solid-State Circuit Conf.*, Florence, Italy, Sep. 2002, pp. 403–406.

[19] K. Tiri and I. Verbauwhede, "A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation," in *Proc. IEEE Design Autom. Test Eur. Conf. Exhibition*, Paris, France, Feb. 2004, pp. 246–251, doi: 10.1109/DATE.2004.1268856.

[20] M. W. Allan and M. I. Elmasry, "Dynamic current mode logic (DyCML): A new low-power high-performance logic style," *IEEE J. Solid-State Circuits*, Vol.36, no.3, pp. 550–558, Mar. 2001, doi: 10.1109/4.910495.

[21] F. Mace, F. X. Standaert, I. Hassoune, J. D. Legat, and J. J. Quisquater, "A dynamic current mode logic to counteract power analysis attacks," in *Proc. DCIS*, Bordeaux, France, Nov. 2004, pp. 186–191.

[22] I. Hassoune, F. Mace, D. Flandre, and J. D. Legat, "Low-swing current mode logic (LSCML): A new logic style for secure and robust smart cards against power analysis attacks," *Microelectron. J.*, vol. 37, no. 9, pp. 997–1006, 2006. [Online]. Available: https://doi.org/10.1016/j.mejo.2006.01.020

[23] T. Popp and S. Mangard, "Masked dual-rail pre-charge logic: DPA-resistance without routing constraints," in *Cryptogrpahic Hardware and Embedded Systems (CHES)* (Lecture Notes in Computer Science), vol. 3659, J. R. Rao and B. Sunar, Eds. Berlin, Germany: Springer, 2005. [Online]. Available: https://doi.org/10.1007/11545262_13

[24] F. Mace, F. X. Standaert, and J. J. Quisquater, "Information theoretic evaluation of side-channel resistant logic styles," in *Cryptographic Hardware and Embedded Systems (CHES)* (Lecture Notes in Computer Science), vol. 4727, P. Paillier and I. Verbauwhede, Eds. Berlin, Germany: Springer, 2007. [Online]. Available: https://doi.org/10.1007/978-3-540-74735-2_29

[25] A. Sengupta, B. Mazumdar, M. Yasin, and O. Sinanoglu, "Logic locking with provable security against power analysis attacks," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 39, no. 4, pp. 766–778, Apr. 2020.

[26] J. S. Coron, P. Kocher, and D. Naccache, "Statistics and secret leakage," in *Financial Cryptography (FC)*, (Lecture Notes in Computer Science), vol. 1962, Y. Frankel, Ed. Berlin, Germany: Springer, 2001. [Online]. Available: http://doi.org/10.1007/3-540-45472-1_12

[27] E. Brier, C. Clavier, and F. Olivier, "Correlation power analysis with a leakage model," *Cryptographic Hardware and Embedded Systems (CHES)* (Lecture Notes in Computer Science), vol. 3156. Berlin, Germany: Springer, 2004. [Online]. Available: http://doi.org/10.1007/978-3-540-28632-5_2