Enhancing Side Channel Attack-Resistance of the STTL Combining Multi-V_t Transistors with Capacitance and Current Paths Counterbalancing

Vitor G. Lima[1], Rodrigo N. Wuerdig[1], Guilherme Paim[1], Leandro M. G Rocha[1],
Leomar da Rosa Jr.[2], Felipe Marques[2], Vinicius Camargo[2],
Eduardo A. C. da Costa[3], Rafael Soares[2], Sergio Bampi[1]

[1]Graduate Program in Microelectronics (PGMicro) - Federal University of Rio Grande do Sul (UFRGS), Porto Alegre - Brazil
[2]Graduate Program in Computing Science (PPGC) - Federal University of Pelotas (UFPel), Pelotas - Brazil
[3]Graduate Program in Electronic Engineering and Computing - Catholic University of Pelotas (UCPel), Pelotas - Brazil
e-mail: {vitor.lima, gppaim}@inf.ufrgs.br

Abstract— **Differential power analysis (DPA) exploits the difference between the instantaneous power of the circuit arches transitions to stole the state as information aiming to unveil the cryptographic key. Secure triple track logic (STTL) is a circuit-level countermeasure to DPA attacks based on dual-rail precharge logic (DPL). STTL is robust to attacks due to the delay in an insensitive feature that mitigates the logic glitches generated by the different path delays that lead to the logic gate inputs until they stabilize. The main STTL drawback, however, is the asymmetry of the transistor topology. Asymmetry causes unbalanced internal capacitances and different internal paths for the current flow, and DPA exploits it as a source of information leakage. Our work proposes three circuit topologies, combining multi-V_t transistors with a circuit counterbalancing strategy, aiming to improve the STTL DPA attack-resistance. Data encryption standard substitution-box circuit, designed in a TSMC 40 nm CMOS process, is our application case study to evaluate the DPA attack-resistance. Results gathered at the application-level show that our proposals outperform DPA attack-resistance of the prior work.**

Index Terms— **Hardware Security; Side Channel Attacks; Cryptography; Circuit Topology; Balanced Paths; Multi-V_t Transistors.**

I. INTRODUCTION

Cryptography is responsible for ensuring the confidentiality of data in an extensive range of applications of the cyber-physical systems on the internet-of-things (IoT) era [1]. The security of the modern cryptography circuits relies on secret keys since its algorithms are public and known. Attacks have been developed to retrieve the key from the algorithm to unveil the contents of an encrypted message. Cryptography can perform protection of all kinds of confidential information at the price of increase the entire system complexity. However, this is critical in real-life when in high-added-value IoT devices linked to the where maximum security can compensate the additional circuit overhead. As a motivation example: due to a weak proprietary cipher and the lack of mutual authentication in the challenge-response protocol a thorough analysis in the security immobilizer and Remote Keyless Entry systems reveals the viability to clone a Tesla Model S key fob with low-cost commercial off the shelf equipment. This security flaw can damage the client's and company's image [2].

Differential power analysis (DPA) and differential electromagnetic analysis (DEMA) are side-channel attacks (SCA) that exploit the correlation between the circuit instantaneous power dissipation and the data being processed [3]. DPA and DEMA exploit the run-time instantaneous power-dissipation asymmetry between the logic states caused by architectural, electrical, and physical choices at design-time. The correlation between the circuit logic states and the power-dissipation results in the possibility of exploits the power-data correlation. Designing secure cryptographic circuits requires countermeasures to prevent DPA action. Thus, many logic cell topologies have been developed aiming to reduce the power-data correlation, most of them based on the dual-rail precharge logic (DPL).

Secure triple track logic (STTL) [4] is a circuit-level countermeasure based on the DPL. Unlike DPL, STTL employs a third-track to validate the signal arrival. The signal arrival validation mitigates logic glitches generated before the stabilization of the inputs of combinational logic, hence improving the DPA-resistance. Despite its advantages, STTL-based circuits have three main drawbacks: (i) asymmetric transistor topology, (ii) latches in the non-validation outputs (iii) race condition between the outputs and the validation rail.

This work introduces three topologies based on the STTL aiming to optimize its drawbacks mentioned above. The first solution is a strategy that modifies some of the nominal-V_t transistors of the STTL to multi-V_t transistors (MT-STTL) improving delay and power dissipation. The second proposal is the balanced STTL (BSTTL) that adds redundant logic to reach full schematic symmetry increasing the DPA-resilience. The third contribution is to join both techniques to reach a multi-V_t balanced STTL (MT-BSTTL) that demonstrates from 30% up to 50% higher attack-resistance against DPA with almost the same circuit delay and energy-efficiency of its predecessor STTL.

The remaining of this paper is organized as follows: Section II. presents the technical background and related work in the realm of cryptosystems. Section III. exposes the three proposals MT-STTL, BSTTL, MT-BSTTL for circuit implementations. Analysis and circuit resistance comparisons of the proposed approaches against other secure topologies are shown in Section IV. Finally, Section V. draws the main conclusions of this work.

II. CRYPTOSYSTEMS BACKGROUND

The security of cryptography systems is critical to many applications, for which no expenses are spared to guarantee secrecy. Although safer algorithms have been developed to

Digital Object Identifier 10.29292/jics.v15i1.100

increase the mathematical complexity, the crypto devices are still vulnerable to side-channel attacks (SCA). SCA explores physical quantities in order to unveil the secret key, posing a severe threat to cryptographic devices like smart-cards [5], ATMs [6], IoT devices [7], and modern cars [8].

A. *Electrical-level Attacks*

Kocher [3] shows that circuits implemented with CMOS technology have different power dissipation traces while computing different source data. Regardless of the platform where the secure application is running, i.e., ASIC, FPGA, or a programmable microcontroller, it could be subjected to power analysis attacks [9] which explore electrical behavior arising from circuit characteristics. Design features like transistor topologies and sizing, capacitive and resistive effects, process variability, and so on, can provide distinguishable signatures for side-attacks.

DPA is the most popular type of power analysis attack since it does not require detailed knowledge about the hardware under attack. The goal of the DPA is to unveil the secret keys of cryptographic systems based on a large number of power traces measured from the power source current drawn. These traces are recorded while the circuit is encrypting or decrypting different data blocks. Further, it can unveil the secret key even if the recorded power traces are extremely noisy. Likewise, DEMA attacks follow a similar approach as DPA attacks; however is the electromagnetic emissions of the circuit generate the traces.

B. *Circuit-level Countermeasures*

There are several strategies to countermeasure DPA, some of these strategies are: transistor disposition [10], encoding scheme [11], buck-voltage regulators [12], switching capacitors [13], and passive elements [14]. Several strategies to minimize the information leaked on CMOS circuits rely on different logic styles to balance the combinational computations and electrical properties. These DPA- and DEMA-resistant logic styles aim to obtain a data-independent energy consumption. Solutions at the transistor level have been presented by [10, 15–17], mostly bringing an improvement in security with an overhead in area, power, and propagation delay.

B..1 Dual Rail Encoding: DR is an encoding scheme where a bit of information has two different voltage levels in a pair of wires, a conventional bit and its complementary value. Asynchronous circuits made out of quasi delay insensitive templates also rely on this kind of DR encoding. The DR improves the resilience to DPA because the output of the gate always switches regardless of the gate logic, or on true or false rails. The DR has another useful characteristic; DR-gates is similar to its complementary logic, e.g., NAND2 is equal to AND2. It reduces the leakage from gate discrepancies in the circuit and only requires to swap the output labels.

B..2 Dual Rail Precharge Logic Encoding: DPL has complementary rails of DR encoding improving it by using a two-steps protocol known as precharge and evaluation phases. The precharge performs at the beginning of each clock cycle and delivers all internal nodes to the same binary state. It guarantees the same initial energy condition eliminating logical hysteresis. The evaluation phase computes the logic information as DR encoding.

C. *Symmetric Cryptography Algorithms:*

Symmetric algorithms are the ones which have the same key to encrypt and decrypt the information. This type of algorithms reaches higher security when having low linearity between the raw text and encrypted information. Advanced encryption standard (AES) [18] and data encryption standard (DES) [19] are the most known symmetric algorithms. However, many other algorithms have been proposed as lightweight AES [20], lightweight DES [21], triple DES [22], 2-key triple DES [23], improved DES or international DES [24], Twofish [25], and Blowfish [26].

AES might have a different length for a key, varying from 128 to 256 bits. Regardless of key length, the maximum size for the message must be equal to the key. The key size interferes in the AES mathematics complexity and increases accordingly to the number of bits. AES operates through a combinational logic, known as substitution-box (SBox) and bit shifters. This process is repeated for 10, 12, or 14 rounds depending if the AES has respectively 128, 192, or 256 bits.

DES is a cryptography algorithm that computes its logic in 16 rounds. Each round is compound by eight combinational blocks (SBox), permutation, and expansion function. DES has 64 bits for input with eight of used for parity. These 56 bits are used for key and maximum messages allowed. Differently of AES that each SBox has the same logical expression, DES has a specific truth table for each SBox.

The symmetric algorithms exposed in this section were implemented, aiming to deliver some level of mathematical safety. However, both symmetric and asymmetric algorithms are known to be vulnerable to SCA even with high numerical robustness (i.e., higher bit-width encryption) [27].

D. *Security Metrics*

The robustness against DPA attacks is quantified using the normalized standard deviation (NSD) and normalized energy deviation (NED) metrics [15–17] given in Equations (1) and (2). The equations quantify the energy variation and, thus, the leaked information. Considering the NED and NSD equations, the *max(E)*, *min(E)*, σE, and $\overline{E}$ are the maximum, minimum, standard deviation, and average energy per cycle, respectively, considering all arches. NED and NSD values close to zero means that the circuit produces lower current variation between logic transitions, the expected behavior of a safe circuit that leaks minimal information. NED metric considers the maximum and minimum energy between all stimuli arches. Where higher the NED value, the higher the consumption differences, and more leakage information. When maximum and minimum energies are equal, it indicates that regardless of the input stimuli, the energy consumption will always be the same, which indicates no leaking information. The denominator *max(E)* is used for normalization. While NED considers both peaks of energy consumption, NSD is a metric that considers the standard deviation of energy for all stimuli arches, and the mean of energy is used to normalize the equation.

$$NED = \frac{max(E) - min(E)}{max(E)} \quad (1) \qquad NSD = \frac{\sigma E}{\overline{E}} \quad (2)$$

E. Related Work

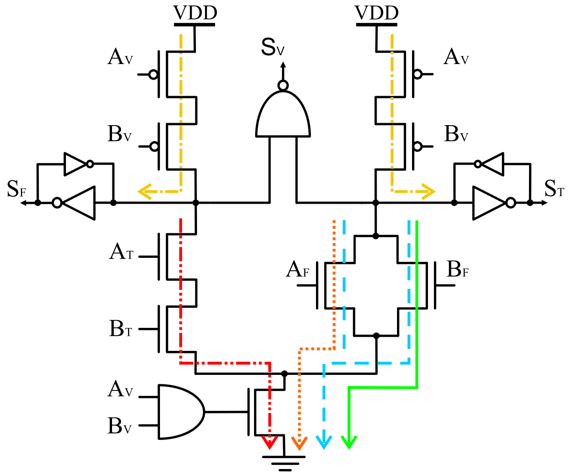
This section presents a review in the literature about countermeasures based on logic styles dedicated to mitigating DPA and DEMA attacks. The implementations and features of each logic style are highlighted and compared as follows.

Secure triple track logic (STTL) is a DPL-based logic with an extra validation rail [4]. The validation signal acts as a trigger, ensuring that gates compute the input signals only when all these signals are valid and stable. This eliminates the computation of input signals propagated at different times, which causes glitches dependent on its input value, an effect known as early propagation (EPE). This property reduces the information leakages compared to traditional DPL logics. Figure 1 shows a STTL-based implementation of a NAND2 gate.

STTL control for precharge and evaluation phases are respectively present by PMOS and NMOS network planes (see Fig. 1). Initially, the precharge is activated if the input $A_{\mathrm{V}} = 0$ and $B_{\mathrm{V}} = 0$, resetting the internal charges and S outputs. All inputs are valid with $A_{\mathrm{V}} = 1$ and $B_{\mathrm{V}} = 1$ when the evaluation phase starts, disconnecting the pull-up network. The evaluation phase modifies the output of the latches according to the inputs $A_{\mathrm{T/F}}$ and $B_{\mathrm{T/F}}$, discharging the latches through the pull-down network. The plane separation avoids the inherent electrical discrepancies, originated from static CMOS topologies. Although STTL-based circuits offer a robust strategy against DPA and DEMA attacks, the logic style has an irregular transistor topology. This undesired characteristic distributes the currents and capacitances unevenly within each logic gate, which still allows the information leakage. This phenomenon is aggravated when there are multiple gates on the same computation paths as these unbalances are accumulated.

STTL logic requires a pair of asymmetric back-to-back inverters on each data output due to its dynamic characteristics. The larger inverter (see Fig. 1) boosts the output while the smaller inverter, known as a keeper, provides a feedback path to restore the internal capacitance charge to avoid the signal degradation along time and flip to a wrong statement. The keeper must be sized small enough to allow the discharge of the node when the pull-down network is activated to drive the output to one.

Wave dynamic differential logic (WDDL) is a classic method that performs DPL using static CMOS gates [15]. Fig. 2 (a) depicts the NAND2 WDDL, which is composed of an AND2 and an OR2. NAND2 WDDL has the A_{T} and B_{T} inputs connected to AND2 to compute the false output S_{F} while the false inputs logic are connected to OR2 to compose the true output S_{T}. The precharge in this topology is serially propagated along the circuit when all inputs of the first gates receive 0 logic. The WDDL is widely used because of its standard cells-based implementation that drastically reduces the project effort to develop cryptographic systems resilient to DPA.



	AT BT	AF BF	Current	ST	SF	SV	Legend
Pre-charge	x x	x x	-·-·→	0	0	0	A - Input A
Evaluation	0 0	1 1	- - -→	1	0	1	B - Input B
	0 1	1 0	·······→	1	0	1	S - Output V - Validation
	1 0	0 1	——→	1	0	1	T - True Logic
	1 1	0 0	-··-→	0	1	1	F - False Logic

Fig. 1: Two-input NAND STTL topology.

Differential pass-transistors precharge logic (DPPL) is a dynamic logic that requires a full-custom design implementation [16]. DPPL is composed of pass-transistors, and its NAND2 transistor disposition is exposed in Fig. 2 (b). The NMOS transistors immediately connected to S_{T} and S_{F} are the logic core of the cell, while the other NFET transistors are used to minimize the EPE. DPPL uses the PFET transistors to perform the precharge, which is serially propagate along the circuit. This state is reached when all differential inputs of each cell are stimulated with 0 logic. The AND2 and OR2 DPPL have 28 transistors on their composition while XOR2 has 20 transistors.

The main drawback of DPPL is the differential inputs distribution. As seen in Fig. 2 (b), each differential input A_{T} and A_{F} are connected to 8 transistor gate terminals while each differential input B are connected to only 4. It matters because in CMOS technology, the Fan-out of a cell is directly related to fan-in of the following gates. The capacitance differences between the A and the B inputs result in variations in delay, power dissipation, and routing, resulting in sources of leak information for SCA attacks.

Precharge static logic (PCSL) is another DPL full-custom topology that balances the charging/discharging paths in order to mitigate the data-dependency [17]. Fig. 2 (c) depicts the PCSL arrangement in schematic level. As seen in the figure, the transistors represented with asterisk symbol, in PMOS and NMOS networks, are logically unnecessary. These four redundant transistors are used to match the internal capacitances between the differential paths. The REQ signal acts as the clock in dynamic logic and is used for precharge and evaluation phases. PCSL performs the precharge in parallel through all circuit when $REQ = 0$ and the evaluation is computed when $REQ = 1$.

However, even equalizing the capacitances, PCSL maintains a mismatching in the current flow to compute the different input stimuli. In the evaluation phase, the NMOS transistors in the S_{T} path has a similar behavior than the same path of STTL, shown in Fig. 1. Observing the first three lines of

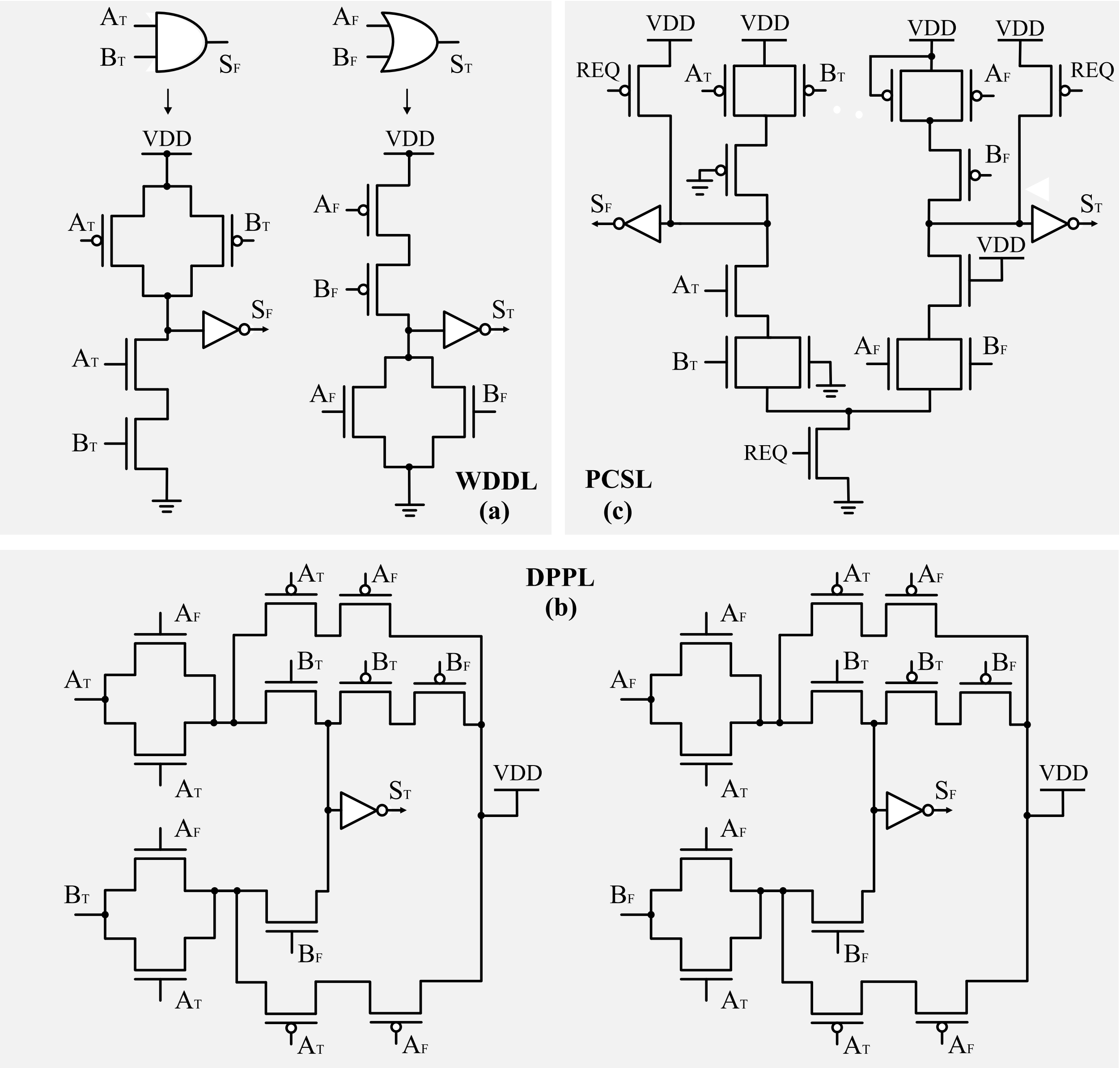


Fig. 2: Two-input NAND of (a) WDDL, (b) DPPL, and (c) PCSL topologies.

truth table and currents representation in Fig. 1, PCSL has the same current splitting for $A_{\mathrm{T}} = 0$ and $B_{\mathrm{T}} = 0$ while for all others arches it has not. As in STTL case, these asymmetries must be avoided in DPA-resistant topologies.

Security comparison between the topologies: Table I summarizes the topology implementations with regarding relevant characteristics and drawbacks to counteract DPA attacks. Topologies with glitching free are the ones that guarantee that purge signals do not propagate to further gates. Since the glitches do not occur in every cell and depend on the combinational logic inputs, these signals increase the data-power correlation.

Static-logic CMOS uses both FET planes to compose the binary logic, while the dynamic logic concentrates logic on a single logical plane. Each CMOS plane has its own electrical and physical specificities that are intrinsic from the behavioral and fabrication process. One can notice that even the dynamic logic utilizes both networks, such as STTL shown in Fig. 1. When the evaluation phase uses one plane, and the precharge utilizes the other, the topology has the ideal logical distribution. It is because DPA explores the power variation from different inputs in the same phase. Thus, the dynamic logic style is more robust than static-logic.

The physical and electrical discrepancies between the differential tracks of a gate are sources of potential vulnerabilities. Thus, the capacitances and current paths must be ideally equal. The columns *(C)* and *(E)* of Table I represent respectively the topologies that have symmetrical capacitances and current paths among the differential signals. Both features depend on the arrangement and size of the transistors. The information of Table I considers that the transistors of the topologies have the ideal sizing and exclusively consider the arrangement of the transistors.

While the columns *(C)* and *(E)* of Table I consider issues internally to gate, *(D)* exposes internal asymmetries that interfere on antecedent gates. It is consequence of the fan-in of a gate directly interferes in the fan-out of the previous gates. Thus, $A_{T/F}$ and $B_{T/F}$ must have ideally the same capacitance to reach higher power homogenization. It means that the number of transistors per literal and the sizing of the transistors have to be considered to guarantee the previous fan-out matching. Table I shows the logic styles that, if correctly sized, reaches the ideal fan-in balancing.

Table I shows important concepts for DPA-resiliency considering prior works and proposals. WDDL does not have any desirable characteristic, PCSL has two, while DDPL and STTL have the highest secure elements of previous works with three. Also, STTL is the single countermeasure that is resilient to purge glitches. The proposals increase resiliency. MT-STTL increases the STTL from three to four, BSTTL increases to five, while MT-BSTTL reaches all six desirable characteristics.

Table I.: DPA-resilience summary of related work.

Work	A	B	C	D	E	F
WDDL [15]	×	×	×	×	×	×
DPPL [16]	×	✓	✓	×	✓	×
PCSL [17]	×	×	✓	✓	×	×
STTL [4]	✓	✓	×	✓	×	×
Proposed MT-STTL	✓	✓	×	✓	×	✓
Proposed BSTTL	✓	✓	✓	✓	✓	×
Proposed MT-BSTTL	✓	✓	✓	✓	✓	✓

(A) Delay insensitive (Glitching free), **(B)** Dynamic logic, **(C)** Balanced intrinsic capacitances, **(D)** Balanced fan-in, **(E)** Balanced circuit current paths, **(F)** Multi-threshold.

III. IMPROVING STTL COMBINING MULTI-VT TRANSISTORS AND CAPACITANCE BALANCING

We propose three topologies that minimize the STTL drawbacks. Each proposal aims to improve the specific and essential aspects necessary to project cryptographic systems. The proposals take advantage of physical properties reachable by the semiconductor manufacturing process using multi-threshold transistors. Multi-V_t strategy aims to improve reliability, delay, and power dissipation, while higher safety to DPA is reached by balancing the transistors' disposition.

The proposals operate with the same triple track encoding than STTL described in Section II. It means that the proposals' improvement is not in the encoding scheme, but in the transistors' disposition that improves electrical characteristics in the current flow. Further details of the proposals are following described.

A. *Multi-threshold Secure Triple Track Logic*

MT-STTL has the same STTL transistor disposition with the threshold of some transistors strategically modified to minimize the STTL drawbacks. A challenge designer face when working with STTL-based circuits is to ensure that the validation signal is slower than the output signals. Fig. 3a shows the MT-STTL disposition. NAND2 has High-V_t to increase the delay of the validation signal concerning the differential pair. A higher delay in the validation rail decreases the effective propagation time of the cell. But, this extra delay turns a TT-based cell more resilient to process voltage temperature *PVT* variations and aging, resulting in devices with lower yield losses and increased life-time.

Another STTL issue is its latches. As discussed in Section II., the latches are essential to avoid signal degradation; however its substantially increase the delay and energy consumption. The drawback occurs as a consequence of the back-to-back keeper arrangement that opposites the logic switch. MT-STTL also aims to minimize the latches overhead.

On the one hand, the low-V_t transistors on the forward path of the MT-STTL makes them more sensitive to charge variations on the internal capacitance nodes. Then, as soon as the circuit enters into the evaluation phase, either C_{n1} or C_{n2} starts discharging, and the low-V_t inverter starts driving the output towards V_{DD} faster than nominal-V_t. On the other hand, the keeper uses high-V_t transistors to reduce the current flowing to nodes C_{n1} or C_{n2}. This current limitation mitigates the keeper influence on these capacitances nodes when the circuit enters into the evaluation phase. Thus, they can discharge faster when compared to a keeper using the standard- or low-V_t transistors while maintain its functionality to guarantee the non-degradation along time. The increase in PVT reliability is a consequence of delay increasing of the validation signal in relation to the differential pair S_T/S_F. STTL-based topologies must have the validation signal slower than the differential ones, otherwise, these topologies lose their timing insensitive behavior and might incur in logical errors. PVT and aging modify the threshold and delay of cell transistors. In case these variations benefit the validation delay and decrease the timing of the differential pair, S_V might be faster than S_T/S_F, resulting on cited problems. Our solution utilizes the high-V_t for S_V and multi-V_t for back-to-back inverters increases the delay between the critical signals, becoming less susceptible to PVT variations and aging effects.

B. *Balanced Secure Triple Track Logic*

BSTTL improves the STTL transistor disposition by balancing the internal capacitances and current paths. BSTTL has the same transistor disposition than the one exposed in Fig. 3b, switching the multi-V_t transistors by nominal ones. As seen in the figure, the strategy adds dummy transistors and redundant logic paths when compared to STTL (Fig. 1) or MT-STTL (Fig. 3a).

In the evaluation phase, the redundancy focuses on matching the pull-down network capacitances and current flows before each latch. Fig. 3b shows that BSTTL always has a wire node between the C_{n0} and C_{n1}/C_{n2} with the same capacitance. The capacitance equality is reached, in schematic level, if M_5 until M_{16} transistors are properly sized with the same widths, and length. Note, the current path from S_F output of the STTL and MT-STTL flow by the wire capacitances C_{n1}, C_{n3}, and C_{n0} while the S_T output flows only by C_{n2} and C_{n0}. In practice, it results in different capacitances flow depending on the inputs. Another issue is the splitting and the number of transistors that the current flows by, as shown by colored lines in Fig. 1. BSTTL solves these problems and guarantees that the current always flows by one path and three transistors.

The precharge phase is also benefited by the pull-down network symmetry of the BSTTL. STTL and MT-STTL wire

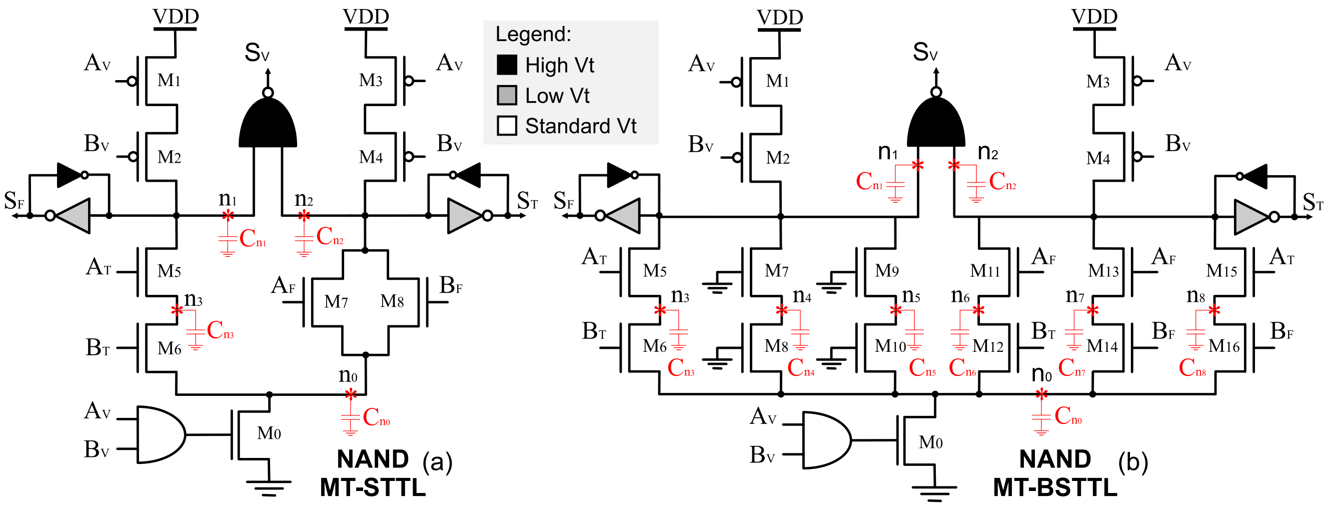


Fig. 3: NAND gates: (a) Multi-V_t STTL and (b) Multi-V_t BSTTL.

n_1 has one transistor in the Pull-down network while n_2 has two, making the flow from V_{DD} to S_T and S_F pass through different capacitances. The BSTTL n_1 and n_2 have higher capacitances, but they are the same in the schematic level.

While MT-STTL aims to improve global demands for CMOS devices, BSTTL is fully designed to guarantee high resilience to DPA-attacks regardless of circuit area, delay path, and power dissipation.

C. *Multi-threshold Balanced Secure Triple Track Logic*

MT-BSTTL merges both previous proposals combining multi-threshold and balancing transistors arrangement. Fig. 3b shows the transistor arrangement of NAND2 MT-BSTTL. Note, the AND2 and all transistors are the same as BSTTL. The latches and NAND2 explore multi-V_t of the TT-STTL in a way that maintains the BSTTL symmetry. MT-STTL has the multi-threshold to optimize reliability, delay, and power dissipation while BSTTL improves DPA-resiliency at the cost of operating frequency and energy consumption.

MT-BSTTL is the middle-term proposal between standard circuit requirements, achieved by MT-STTL, and high safety of BSTTL. The specificities of MT-BSTTL are the same as the other countermeasures discussed in this section.

IV. RESULTS AND DISCUSSIONS

In this section, the topologies proposed in this paper are compared with its predecessor, the STTL, and with other relevant secure topologies from the literature, which are WDDL, PCSL, and DPPL. In some projects, DPA-safety is not the only restriction. Thus, this section evaluates the security level to DPA, power, and performance. The results are exposed in two separated parts. The first compares the cells AND2/NAND2, OR2/NOR2, and XOR2/XNOR2. Later, these gates are used to compose a crypto-core module SBox-1 of the DES algorithm.

Every step of the symmetric algorithm is vulnerable. But, the SBox has a bitwise operation between the secret key and the message, becoming the most sensitive part of the device. Therefore, SBox is widely used as a figure of merit to quantify the security level of a cryptosystem [11, 28, 29].

This work implements the proposals and previous works to the same technology aiming to achieve a more accurate result. All case studies used in this work were performed using SPICE simulations with the Cadence Spectre^{TM} tool. Also, the technology node was TSMC 40 nm bulk-CMOS under a nominal supply voltage of 0.9 V. The transition slew was set to 20 ps at each pin, and all results are presented in a relative form to respect the non-disclosure agreement signed with TSMC.

The case studies for the logic gate and crypto core in this section are organized as follows. Firstly, a relevant discussion is introduced at the beginning of each section. Later, the implementation details are exposed followed by comparisons results considering the predecessor STTL and proposals. Finally, the discussion and results are extended for the other secure logic styles.

A. *Isolated Logic Gate Analysis*

This paper evaluates the security level of MT-STTL, BSTTL, and MT-BSTTL in a similar way than performed in [10], with the simulation environment being the main difference. In [10] was used 1.1 V for nominal voltage, and the inputs' slope was too steep to reflect a realistic scenario for 40 nm technology. This paper uses a more precise situation by using the simulation environment described next.

Implementation and testbench details: The simulation environment was strategically designed to allow a fair comparison among the different topologies. Fig. 4 shows the DUT setup for logic gates applied to the different topologies. The simulation environment is specified in the following aspects.

(i) The topology gates were sized to have the driving strength equals to a minimal inverter, called here as *X1* drive strength. In the exception of forwarding inverters of the STTL-based topologies that have driving strength of *X2*. It is necessary because the forward inverters must have more driver capability than the keepers to allow the logic flip. DPA-resistant topologies have many transistors in their logic. Therefore, for higher outputs load it is preferable to have differential buffers or inverters tree than scales such quantity of transistors.

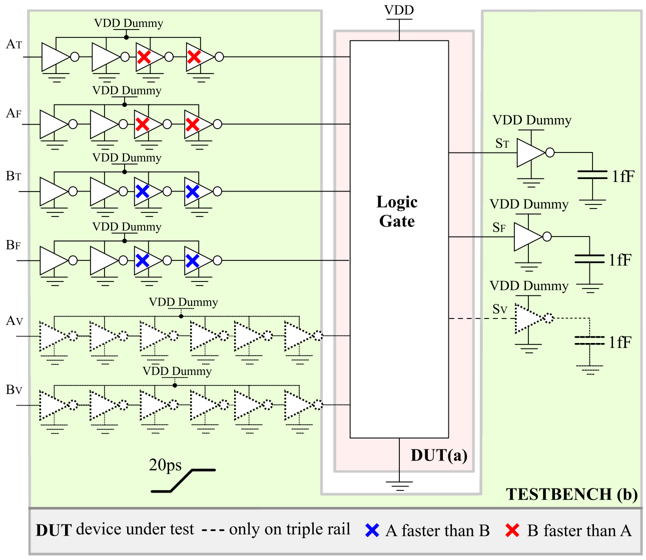


Fig. 4: Testbench environment for the logic gates (DUT) comparison.

(ii) The STTL-based proposals are glitch aware while the others DPL-based cells are not. In a real circuit the glitches do not occur in every cell and every cycle. Therefore, the simulations performed to evaluate the gate resilience to SCA consider the best case for these delay sensitive topologies, using the stimuli scenario exposed next on item iii). Glitches and EPE are sources of leakage exploitable by side-channel attacks since they are logical dependent and exploitable at power signatures.

(iii) The input characteristics change the electrical behavior of the cell. From a circuit perspective, these stimuli vary accordingly to the previous logic and, thus, all stimuli might be considered in the logic gate to achieve higher accuracy. So, this work considers 4 arches with A driving first than B and 4 more with B driving first than A. These delays have the same input slew of 20 ps being controlled by the number of inverters stacked, as shown by the blue and red X inverters in Fig. 4b. Triple-track (TT) logic requires that validation signal be slower than the complementary rails, wherefore TT delays are always generated with three buffers.

(iv) The delays discussed in (iii) might be simulated directly in the SPICE command.However, for the signals generated this way is ideal and disregard the capacitances, resistances, and specificity of the topology. Buffers were inserted on the DUT inputs to guarantee the non-idealities. Similarly, inverters were added in the outputs to represent a small Fan-out and not an ideal wire. Note, the buffers and the inverters have different power supply than the DUT. It is to guarantee the environment cited without the noise arising from the auxiliary gates.

Predecessor STTL comparisons: Table II shows the comparison between the predecessor STTL and the proposals regarding cell implementations. To better illustrate the results in the table, the cells where the STTL gate presents the advantage to the proposed ones are colored in red with negative values, while the cells are colored green with positive values when the proposed topology shows an advantage over the predecessor STTL. XOR2 comparisons are only assigned for XOR2 MT-STTL because the XOR2 STTL is identical to the BSTTL one and the MT-STTL is similar to the MT-BSTTL.

Table II.: Isolated cell analysis: STTL Relative Comparisons with regard to our three topology proposals for AND2, OR2, and XOR2 logic gates.

		Delay†	**Energy**$^{\alpha,\dagger}$	**NED**†	**NSD**†
AND	**MT-STTL**[1]	1.20×	1.18×	1.57×	1.70×
	BSTTL[2]	-1.18×	-1.25×	6.39×	8.39×
	MT-BSTTL[3]	1.05×	1.00×	4.74×	5.27×
OR	**MT-STTL**[1]	1.22×	1.18×	1.85×	1.95×
	BSTTL[2]	-1.21×	-1.25×	4.57×	5.09×
	MT-BSTTL[3]	1.02×	1.01×	5.21×	5.70×
XOR	**MT-STTL**[1]	1.19×	1.23×	-1.22×	-1.25×
STTL		1.00×	1.00×	1.00×	1.00×

$^{\alpha}$ Average of the energy consumed in all transition arcs. 🟢 + Better than STTL.

† Average results for precharge and evaluation phases. 🔴 – Worse than STTL.

[1] Improved STTL with multi-V_t optimization. [2] Proposed Balanced STTL.

[3] Proposed Balanced STTL with multi-V_t optimization.

The MT-STTL successfully reduces both delay and energy consumption of STTL in approximately 20% for all considered gates, as presented in Table II. MT-STTL has also shown to be very effective in improving STTL safety figures of merit for AND2 and OR2 gates while offering a loss for the XOR2 gate. MT-STTL improves STTL safety by 57% in NED and 70% for NSD of AND2, by 85% of NED and 95% for NSD of OR2 and reduces the safety by 22% for NED and 25% for NSD of XOR2. The losses on XOR2 and XNOR2 do not represent a severe problem for most of the symmetric algorithms. While XOR2 is widely used for arithmetic operations, the symmetric algorithms are composed of combinational logic and bitwise shifts. The DES SBox has less than 3% of XOR2 and XNOR2 instances after the logical synthesis. Considering AND2 and OR2 gates, the authors assign the security improvement to STTL asymmetric arrangement that is increased by the latches overhead. XOR2 does not present the same improvement as it is already a symmetric arrangement. The use of multi-V_t transistors lead to significant improvements in power and delay while also increase the security level.

The BSTTL inserts redundant logic to improve the DPA-resilience at the cost of delay, energy consumption, and circuit area. The simulation results, presented in Table II, confirms this relationship. BSTTL has gains varying from 4.57× up to 8.47× in the security figures of merit, at the cost around 20% in delay and 25% in energy consumption for AND2 and OR2 gates. These results indicate that the BSTTL topology has great potential in applications where the security is critical, and drawbacks in delay and power are tolerable.

The MT-BSTTL combines both multi-V_t and balancing strategies aiming for a reduction in the power and delay costs of the BSTTL. The results presented in Table II confirms that the improvement brought by the multi-V_t not only made the MT-BSTTL gates as fast and economical as the STTL ones while inheriting the BSTTL security. AND2 MT-BSTTL is 4.74× safer in NSD than STTL and 5.21× more secure in NED, while OR2 is 5.21× more resilient in NED and 5.7×

Table III.: Isolated cell analysis: MT-STTL relative comparison with regard to prior work for AND2, OR2, and XOR2 logic gates.

		Area	**Delay**†	**Energy**$^{\alpha,\dagger}$	**NED**†	**NSD**†
AND	**STTL**	1.00×	-1.20×	-1.18×	-1.57×	-1.70×
	WDDL	2.30×	1.96×	3.73×	-2.63×	-2.68×
	PCSL	1.01×	2.44×	2.57×	-3.46×	-3.40×
	DPPL	-2.28×	1.13×	1.16×	-4.66×	-8.50×
OR	**STTL**	1.00×	-1.22×	-1.18×	-1.85×	-1.95×
	WDDL	2.30×	1.93×	3.78×	-3.30×	-3.42×
	PCSL	1.01×	2.14×	2.76×	-4.72×	-6.88×
	DPPL	-2.28×	1.13×	1.18×	-5.86×	-10.82×
XOR	**STTL**	1.00×	-1.19×	-1.23×	1.22×	1.25×
	WDDL	1.29×	2.35×	2.96×	-1.02×	1.20×
	PCSL	1.01×	2.74×	2.74×	-3.80×	-6.08×
	DPPL	-1.28×	1.39×	1.82×	-3.67×	-4.63×
MT-STTL		1.00×	1.00×	1.00×	1.00×	1.00×

$^\alpha$ Average of the energy consumed in all transition arcs. 🟢 − Better than Baselines.

† Average results for precharge and evaluation phases. 🔴 + Worse than Baselines.

in NSD. At the gate level, the MT-BSTTL presented the best balance between security and performance metrics. However, the MT-STTL still has the edge on performance.

Related work comparisons: This paper also compares the proposals with other prior work topologies. Table III, Table IV, and Table V are respectively the comparison between MT-STTL, BSTTL, and MT-BSTTL w.r.t. others countermeasures. The tables consider circuit area, delay, energy, and security metrics. Note that STTL comparisons in Table II has the same information than the other three cited tables, being inserted to allow a perspective analyze with others DPA-resistant logic styles.

Considering the results of AND2 and OR2 showed in Table III, Table IV, and Table V, BSTTL has the highest area, delay, and energy consumption. BSTTL requires 3.24× more area and 5.58× more energy than WDDL being 2.84× slower than PCSL. These results come from the following explanation. AND2-WDDL and OR2-WDDL are composed of an AND2 and an OR2 available in the standard cell libraries. It makes AND2 and OR2 of WDDL be the smallest gates resulting in the lowest cricuit area and energy consumption. Usually, WDDL might have the shortest delay as well. But PCSL performs precharge logic through a transistor and an inverter. It makes PCSL require only a few picoseconds to perform the precharge, making PCSL the fastest topology.

While the proposals AND2 and OR2 are more significant, slower, and require more energy, they are much safer than the previous works. The proposals have security gains in every comparison overcoming from 57% up to 41.95×.

As mentioned earlier, XOR2-STTL and XOR2-BSTTL are equals because XOR2-STTL is already balanced, as well as the XOR2 of the MT-STTL is equal to MT-BSTTL XOR2-BSTTL also has the worst circuit area, delay, and energy consumption. XOR2-WDDL is composed of three AND2 and OR2, so, WDDL has the smallest delay and energy, where XOR2-BSTTL is 29% bigger and dissipates 3.63× more power to operate. XOR2-PCSL also needs only a transistor and an inverter to compute the precharge. It makes the PCSL be the fastest topology where BSTTL requires 3.36× more propagation time to finish the computation than PCSL.

The improvements in the NED and NSD metrics suggest that circuits designed using BSTTL and MT-BSTTL will be much more resilient to DPA attacks than STTL and than the other related works topologies studied in this paper. Regarding the power and delay metrics, the use of multi-V$_t$ reduced the gap to less secure topologies widening the applications where the highly reliable STTL and BSTTL might be used, however less secure topologies still hold the edge in this regard.

B. Application Case Study: DES SBox

This work utilizes the SBox 1 of the DES algorithm as a case study for proposals and prior works. But, our solutions optimize the transistor disposition to counteract the DPA threat. It means that these resilient cells would be used to implement any cryptographic system. Section II. C. briefly describes some of these algorithms.

It is also important to note that in the context of SBox, where the number of arches is enormous, the NSD metric is a more meaningful indicator as it uses the energy consumption in all possible arches and not only in the two arches with the maximum and minimum energy.

Implementation and testbench details: Similarly to gate analysis, the SBox implementation are separated into relevant topics presented next.

(i) The minimum size of the silicon die can be constrained by the higher number of I/O PADS (i.e., limited pad design) instead of the size of the core. Pad limited circuits impose an extra silicon area not occupied by any circuit due to the minimum width of the I/O PADS. Shift-registers – serial-in to parallel-out (SIPO) and parallel-in to serial-out (PISO) – are commonly employed to interface the circuit. Interface

Table IV.: Isolated cell analysis: BSTTL relative comparison with regard to prior work for AND2, OR2, and XOR2 logic gates.

		Area	**Delay**†	**Energy**$^{\alpha,\dagger}$	**NED**†	**NSD**†
AND	**STTL**	1.41×	1.18×	1.00×	-6.39×	-8.39×
	WDDL	3.24×	2.78×	4.42×	-10.73×	-13.25×
	PCSL	1.42×	3.45×	3.05×	-14.08×	-16.76×
	DPPL	-1.62×	1.60×	1.37×	-18.97×	-41.95×
OR	**STTL**	1.41×	1.21×	1.25×	-4.57×	-5.09×
	WDDL	3.24×	2.84×	5.58×	-8.14×	-8.95×
	PCSL	1.42×	3.14×	4.07×	-11.63×	-17.99×
	DPPL	-1.62×	1.66×	1.73×	-14.45×	-28.30×
XOR	**STTL**	1.00×	1.00×	1.00×	1.00×	1.00×
	WDDL	1.29×	2.81×	3.63×	-1.24×	-1.04×
	PCSL	1.01×	3.27×	3.36×	-4.64×	-7.60×
	DPPL	-1.28×	1.66×	2.23×	-4.49×	-5.79×
BSTTL		1.00×	1.00×	1.00×	1.00×	1.00×

$^\alpha$ Average of the energy consumed in all transition arcs. 🟢 − Better than the prior work.

† Average results for precharge and evaluation phases. 🔴 + Worse than the prior work.

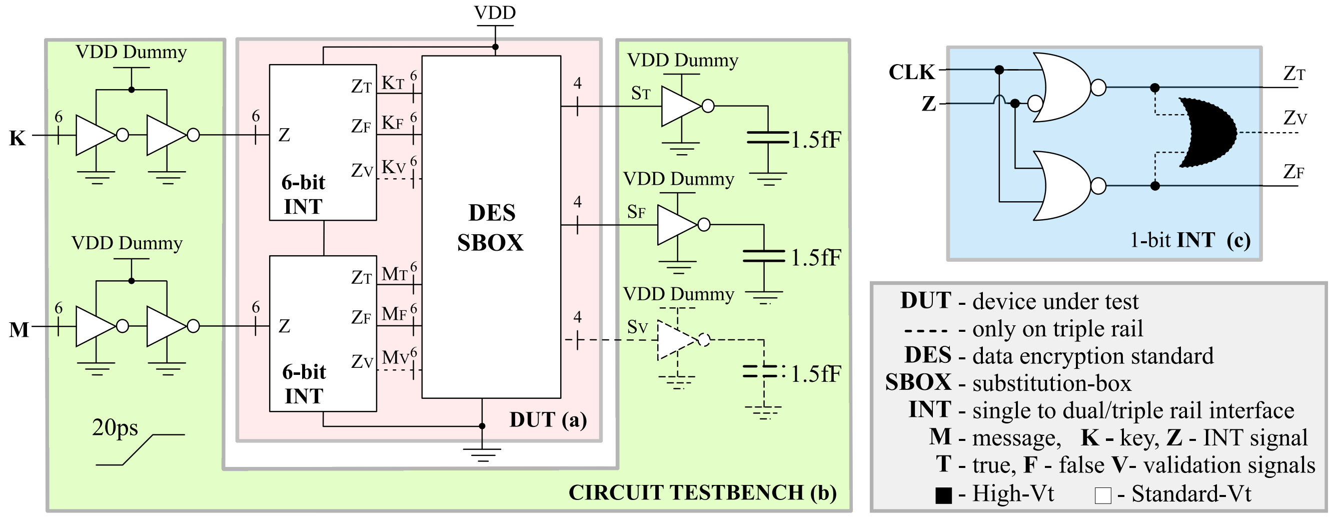

VDD
VDD Dummy
K
M
6
Z
ZT
ZF
ZV
KT
KF
KV
MT
MF
MV
6-bit INT
DES SBOX
4
ST
SF
SV
1.5fF
20ps
DUT (a)
CIRCUIT TESTBENCH (b)
CLK
1-bit INT (c)
DUT - device under test
---- - only on triple rail
DES - data encryption standard
SBOX - substitution-box
INT - single to dual/triple rail interface
M - message, K - key, Z - INT signal
T - true, F - false V- validation signals
■ - High-Vt □ - Standard-Vt

Fig. 5: Test environment for DES SBox-1.

Table V.: Isolated cell analysis: MT-BSTTL relative comparison with regard to prior work for AND2, OR2, and XOR2 logic gates.

		Area	Delay†	Energy$^{\alpha,\dagger}$	NED†	NSD†
AND	STTL	1.41×	-1.05×	1.00×	-4.74×	-5.27×
	WDDL	3.24×	2.25×	4.40×	-7.97×	-8.32×
	PCSL	1.42×	2.80×	3.04×	-10.45×	-10.52×
	DPPL	-1.62×	1.29×	1.37×	-14.08×	-26.33×
OR	STTL	1.41×	-1.02×	-1.01×	-5.21×	-5.70×
	WDDL	3.24×	2.32×	4.45×	-9.28×	-10.04×
	PCSL	1.42×	2.56×	3.25×	-13.26×	-20.17×
	DPPL	-1.62×	1.36×	1.38×	-16.48×	-31.72×
XOR	STTL	1.00×	-1.19×	-1.23×	1.22×	1.25×
	WDDL	1.29×	2.35×	2.96×	-1.02×	1.20×
	PCSL	1.01×	2.74×	2.74×	-3.80×	-6.08×
	DPPL	-1.28×	1.39×	1.82×	-3.67×	-4.63×
MT-BSTTL		1.00×	1.00×	1.00×	1.00×	1.00×

$^\alpha$ Average of the energy consumed in all transition arcs. 🟢 – Better than Baselines.

† Average results for precharge and evaluation phases. 🔴 + Worse than Baselines.

using strategy reduces the number of PADS and avoids pad-limited silicon area overhead, with a trade-off of an increase of clock cycles and circuit area (due to the extra flip-flops). Employing N-rails on inputs increases the number of I/Os or shift-registers interfaces by N times. Our work considers a single-rail input with an on-chip conversion to N-rails, aiming for efficient design, according to the number of tracks of the logic gate in the DUT.

Fig. 5c shows a 1-bit converter from single- to N-rails (up to N=3); both are composed of two NOR2 along with an inverter for complementary signals. Triple-Rail has an additional validation signal, and an OR2 composed by high-V_t transistors. Increase the threshold value results in a higher delay that increases the differences between the complementary and validation data, to guarantee the TT restriction. The precharge is reached when *CLK=0* which switches all outputs to *0*. In the evaluation phase, the outputs Z_T and Z_F receive the properly differential values from the Z signal. For TT-based topologies, Z_V switches to 1-logic when Z_T and Z_F assume their complementary statements.

(ii) Figure 5a represents the DUT-SBox utilized in this work. DES SBoxes has 4 bits for outputs, and 12 bits for inputs, where six are for key and six are for plaintext. These inputs are expanded by the module exposed in (i) and becomes the differential pairs of the SBox inputs. SBox implemented with TT encoding also has the validation stimulus generated by the expander and is represented by the dashed wires. The buffers and inverters of Fig. 5b are used to guarantee the non-idealities, similarly to specified at isolated logic gate simulation, described previously in this Section.

(iii) SBox netlist was generated using the Cadence Genus^{TM} logic synthesis tool by which the resulting netlist was used to perform electrical SPICE simulations.

On the security advances over the STTL: Table VI compares the delay, energy consumption and security between STTL and proposals. As indicated by the gate level results, the MT-STTL surpasses STTL in all aspects, being 8.6% faster, consuming 8.9% less energy and improving the NED and NSD in 36.4% and 31.6%, respectively. These results indicate that the multi-V_t solution allows the designer to obtain a circuit both more secure and with better performance without any penalty in the circuit area.

The results presented in Table VI also show that the BSTTL has the highest NSD through the proposals being 50.7% more resilient with NSD metric than STTL while NED also has a high value of 30.6%. However, the cost of 15.4% in delay and 20.9% in energy than the STTL is a vital drawback which may limit the applications of this topology. The MT-BSTTL, with the use of multi-V_t transistor, is the half-term proposal that improves the BSTTL delay and power overheads while improving MT-STTL safety. MT-BSTTL has a slightly higher delay of 2.3% and energy consumption while reaching high security of 30.9% for NED and 49.8% for NSD. In the SBox simulations, MT-BSTTL almost equalizes BSTTL NED, and NSD differently of showed in gate-level comparisons. The authors sign it to the nominal-V_t latches of BSTTL that opposes the logical switch aggravated by the multiple logic levels that compute in parallel in the SBox.

Table VI.: DES SBox case study: STTL relative comparison with regard to our three topology proposals.

	Delay†	Energy$^{\alpha,\dagger}$	NED†	NSD†
MT-STTL[1]	1.09×	1.09×	1.36×	1.32×
BSTTL[2]	-1.15×	-1.21×	1.31×	1.51×
MT-BSTTL[3]	-1.02×	-1.06×	1.31×	1.50×
STTL	1×	1×	1×	1×

$^{\alpha}$ Average of the energy consumed in all transition arcs. 🟢 + Better than STTL.

† Average results for precharge and evaluation phases. 🔴 − Worse than STTL.

[1]Improved STTL with multi-V_t optimization. [2]Proposed Balanced STTL.

[3]Proposed Balanced STTL with multi-V_t optimization.

In the SBox simulations, MT-BSTTL almost equalizes BSTTL NED, and NSD differently of showed in gate-level comparisons. The authors sign it to the nominal-V_t latches of BSTTL that opposes the logical switch aggravated by the multiple logic levels that compute in parallel in the SBox. MT-STTL also surpasses BSTTL and MT-BSTTL in NED while it has a very lower NSD. Possible causes are the MT-STTL fewer transistors to compose the gates, latches formed by multi-V_t transistors, and smaller internal resistances and capacitances.

On the security advances over the prior works: Related works are also implemented and compared to proposed topologies. The results are shown in Table VII, Table VIII, and Table IX. As expected, the glitch resilience, balanced arrangement, and multi-V_t strategies of proposals make them surpass the related work resiliency.

MT-STTL minimizes the latches' overhead of STTL, but the latches still are a necessary increasing delay and power dissipation. MT-STTL has higher energy consumption than the prior works in except for STTL. The energy losses vary from 12% to 4.4×. While delay loses varies from 1.99× until 4.59×. The increased delay is a consequence of the TT validation rail that must be slower than the complementary logic. It implies an additional delay per cell that accumulates along the circuit. This delay is essential to eliminate purge glitch propagation and improve security. The cost of delay and energy are justified by the high-security level reached. MT-STTL overcomes all other countermeasures by at least 46% and reaches more than 4× in both secure metrics.

Table VII.: DES SBox case study: MT-STTL relative comparison with regard to prior work.

	Area	Delay†	Energy$^{\alpha,\dagger}$	NED†	NSD†
STTL	1.00×	-1.09×	-1.10×	-1.57×	-1.46×
WDDL	2.24×	4.59×	4.40×	-3.43×	-3.46×
PCSL	1.05×	4.27×	2.67×	-4.25×	-4.59×
DPPL	-2.21×	1.99×	1.12×	-2.16×	-2.42×
MT-STTL	1×	1×	1×	1×	1×

$^{\alpha}$ Average of the energy consumed in all transition arcs. 🟢 − Better than prior work.

† Average results for precharge and evaluation phases. 🔴 + Worse than prior work.

Table VIII.: DES SBox case study: BSTTL relative comparison with regard to prior work.

	Area	Delay†	Energy$^{\alpha,\dagger}$	NED†	NSD†
STTL	1.39×	1.15×	1.21×	-1.44×	-2.03×
WDDL	3.11×	5.80×	5.83×	-3.14×	-4.81×
PCSL	1.46×	5.40×	3.55×	-3.90×	-6.37×
DPPL	-1.59×	2.51×	1.48×	-1.98×	-3.35×
BSTTL	1×	1×	1×	1×	1×

$^{\alpha}$ Average of the energy consumed in all transition arcs. 🟢 − Better than prior work.

† Average results for precharge and evaluation phases. 🔴 + Worse than prior work.

Table IX.: DES SBox case study: MT-BSTTL relative comparison with regard to prior work.

	Area	Delay†	Energy$^{\alpha,\dagger}$	NED†	NSD†
STTL	1.39×	1.02×	1.06×	-1.45×	-1.99×
WDDL	3.11×	5.14×	5.09×	-3.15×	-4.72×
PCSL	1.46×	4.78×	3.10×	-3.91×	-6.25×
DPPL	-1.59×	2.23×	1.29×	-1.99×	-3.29×
MT-BSTTL	1×	1×	1×	1×	1×

$^{\alpha}$ Average of the energy consumed in all transition arcs. 🟢 − Better than prior work.

† Average results for precharge and evaluation phases. 🔴 + Worse than prior work.

BSTTL balances the internal asymmetries of STTL but still has the predecessor latches and increased number of transistors. Therefore, BSTTL has a higher circuit area, delay, and energy consumption than MT-STTL, and the other considered works. BSTTL surpasses the DPPL circuit area by 59% while it is 3.1× bigger than WDDL. The increase in delay varies from 15% until 5.8×. BSTTL exceeds the safety of other countermeasures. The gains range rises from 44% until 3.9× in NED increasing even more for NSD, varying from 2.03× up to 6.37×.

MT-BSTTL combines MT-STTL and BSTTL strategies. MT-BSTTL has the same circuit area as BSTTL; however reduces the delay and energy of BSTTL. MT-BSTTL is slower and has a higher energy consumption of a ratio of 5.14× than WDDL. Like the other proposals, MT-BSTTL is very resilient to DPA attacks. When compared to prior works, MT-BSTTL has gains varying from 45% up to 6.25×. On the DES SBox, the MT-BSTTL is the proposal with high cost-benefit with regarding circuit area, critical delay path, energy consumption, and safety.

V. CONCLUSION

This work introduced three topologies to counteract differential power analysis (DPA) attacks. These logic styles are based on DPA-resistant secure triple track logic (STTL) and reduce the predecessor drawbacks. STTL has three issues: validation rail must be slower than its differential outputs; asymmetric transistor disposition; back-to-back latches in the differential outputs. These issues increase the delay, energy consumption, and leakage information. Simulations confirmed that the proposals overcome the predecessor STTL, in almost every case, with gains in delay and energy, and also security. When compared to other related works, we also obtained security improvements at the cost of the area, delay, and energy. We used the first substitution-box (SBox) of the DES circuit as a circuit case study. Although incurring in losses in delay, area, and energy consumption, the proposals presented overcome the safety of STTL and reach significant safety gains when compared to the other three countermeasures. Each proposal set forth in this work obtained better results in terms of security when compared to any other prior work considered, evidencing the effectiveness of our proposals to counteract DPA.

VI. ACKNOWLEDGEMENTS

The authors would like to thank CNPq, CAPES, and FAPERGS Brazilian agencies for financial support to our research, and NSCAD-UFRGS for EDA support. Additionally, the author L. M. G. Rocha would like to thank the IFRS for his temporary license to pursuing the Ph.D. with full-time dedication.

REFERENCES

[1] A. Humayed, J. Lin, F. Li, and B. Luo, "Cyber-Physical Systems Security—A Survey," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1802–1831, Dec 2017.

[2] Y. Zeng, Q. Yang, and J. Li., "Fast, Furious and Insecure: Passive Keyless Entry and Start in Modern Supercars," 2019. [Online]. Available: https://www.esat.kuleuven.be/cosic/passive-keyless-entry/

[3] 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, pp. 388–397.

[4] A. Razafindraibe, M. Robert, and P. Maurine, "Improvement of dual rail logic as a countermeasure against DPA," in *Proceedings of the IFIP International Conference on Very Large Scale Integration*, Oct 2007, pp. 270–275.

[5] R. Xu, L. Zhu, A. Wang, X. Du, K.-K. R. Choo, G. Zhang, and K. Gai, "Side-channel attack on a protected rfid card," *IEEE Access*, vol. 6, pp. 58 395–58 404, 2018.

[6] K. Mowery, S. Meiklejohn, and S. Savage, "Heat of the moment: Characterizing the efficacy of thermal camera-based attacks," in *Proceedings of the 5th USENIX conference on Offensive technologies*. USENIX Association, 2011, pp. 1–8.

[7] D. Gnad, J. Krautter, and M. Tahoori, "Leaky Noise: New Side-Channel Attack Vectors in Mixed-Signal IoT Devices," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, vol. 2019, no. 3, pp. 305–339, May 2019. [Online]. Available: https://tches.iacr.org/index.php/TCHES/article/view/8297

[8] Y. Kong and E. Saeedi, "Side-channel vulnerabilities of automobiles," *Transaction on IoT and Cloud Computing*, pp. 1–8, 2014.

[9] S. Mangard, E. Oswald, and T. Popp, *Power Analysis Attacks: Revealing the Secrets of Smart Cards (Advances in Information Security)*. Secaucus, NJ, USA: Springer-Verlag New York, Inc., 2007.

[10] V. G. Lima, G. Paim, L. M. Rocha, L. da Rosa, F. Marques, E. A. da Costa, V. Camargo, R. Soares, and S. Bampi, "Maximizing Side Channel Attack-Resistance and Energy-Efficiency of the STTL Combining Multi-V t Transistors with Current and Capacitance Balancing," in *2019 IEEE International Symposium on Circuits and Systems (ISCAS)*. IEEE, 2019, pp. 1–5.

[11] D. Bellizia, G. Scotti, and A. Trifiletti, "TEL Logic Style as a Countermeasure Against Side-Channel Attacks: Secure Cells Library in 65nm CMOS and Experimental Results," *IEEE Transactions on Circuits and Systems I: Regular Papers*, no. 99, pp. 1–11, 2018.

[12] M. Kar, A. Singh, S. Mathew, A. Rajan, V. De, and S. Mukhopadhyay, "8.1 Improved power-side-channel-attack resistance of an AES-128 core via a security-aware integrated buck voltage regulator," in *2017 IEEE International Solid-State Circuits Conference (ISSCC)*. IEEE, 2017, pp. 142–143.

[13] C. Tokunaga and D. Blaauw, "Securing encryption systems with a switched capacitor current equalizer," *IEEE Journal of Solid-State Circuits*, vol. 45, no. 1, pp. 23–31, 2009.

[14] M. Kar, A. Singh, S. Mathew, A. Rajan, V. De, and S. Mukhopadhyay, "Exploiting fully integrated inductive voltage regulators to improve side channel resistance of encryption engines," in *Proceedings of the 2016 International Symposium on Low Power Electronics and Design*. ACM, 2016, pp. 130–135.

[15] K. Tiri and I. Verbauwhede, "A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation," in *Proceeding of the Conference on Design, Automation and Test in Europe*, vol. 1. IEEE, 2004, pp. 246–251.

[16] X. Pang, J. Wang, C. Wang, and X. Wang, "A DPA resistant dual rail Préchargé logic cell," in *Proceedings of the IEEE 11th International Conference on ASIC (ASICON)*. IEEE, 2015, pp. 1–4.

[17] K.-S. Chong, K. Z. L. Ne, W.-G. Ho, N. Liu, A. H. Akbar, B.-H. Gwee, and J. S. Chang, "Counteracting differential power analysis: Hiding encrypted data from circuit cells," in *Proceeding of the IEEE International Conference on Electron Devices and Solid-State Circuits (EDSSC)*. IEEE, 2015, pp. 297–300.

[18] N.-F. Standard, "Announcing the advanced encryption standard (AES)," *Federal Information Processing Standards Publication*, vol. 197, no. 1-51, pp. 3–3, 2001.

[19] E. Biham and A. Shamir, *Differential cryptanalysis of the data encryption standard*. Springer Science & Business Media, 2012.

[20] R. A. E. B. L. Knudsen, "Serpent: A proposal for the advanced encryption standard," in *First Advanced Encryption Standard (AES) Conference, Ventura, CA*, 1998.

[21] A. Poschmann, G. Leander, K. Schramm, and C. Paar, "New lightweight crypto algorithms for RFID," in *2007 IEEE International Symposium on Circuits and Systems*. IEEE, 2007, pp. 1843–1846.

[22] A. R. Kumar, S. Mubeena, and V. S. Babu, "Implementation of Triple Data Encryption Standard Architecture," 2017.

[23] C. J. Mitchell, "On the security of 2-key triple DES," *IEEE Transactions on Information Theory*, vol. 62, no. 11, pp. 6260–6267, 2016.

[24] R. Zimmermann, A. Curiger, H. Bonnenberg, H. Kaeslin, N. Felber, and W. Fichtner, "A 177 Mb/s VLSI implementation of the international data encryption algorithm," *IEEE Journal of Solid-State Circuits*, vol. 29, no. 3, pp. 303–307, 1994.

[25] B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, and N. Ferguson, "Twofish: A 128-bit block cipher," *NIST AES Proposal*, vol. 15, no. 1, pp. 23–91, 1998.

[26] B. Schneier, "Description of a new variable-length key, 64-bit block cipher (Blowfish)," in *International Workshop on Fast Software Encryption*. Springer, 1993, pp. 191–204.

[27] J. Krämer, "Why cryptography should not rely on physical attack complexity," *it-Information Technology*, vol. 59, no. 1, pp. 53–56, 2017.

[28] S. Kaza, A. Tilak, and K. S. Rao, "Ultralow-Power and Secure S-Box Circuit Using FinFET Based ECRL Adiabatic Logic," *Journal of Science and Technology*, vol. 10, no. 3, 2018.

[29] J. Lim, W.-G. Ho, K.-S. Chong, and B.-H. Gwee, "DPA-resistant QDI dual-rail AES S-Box based on power-balanced weak-conditioned half-buffer," in *2017 IEEE International Symposium on Circuits and Systems (ISCAS)*. IEEE, 2017, pp. 1–4.