

RETRO: Mitigating Power Side-Channel Attacks with Reconfigurable RFET-based Ring Oscillators

Nima Kavand^{*†}, Tushar Niranjani[†], Armin Darjani^{*†}, Akash Kumar[†]

^{*}TU Dresden, Germany, [†]Ruhr University Bochum, Germany

Nima.Kavand@rub.de, Tushar.Niranjani@edu.ruhr-uni-bochum.de, Armin.Darjani@rub.de, Akash.Kumar@rub.de

Abstract—Power side-channel attacks are among the most effective physical attacks, threatening the security of circuits such as cryptographic circuits by exploiting information leakage from their physical implementation. Among various masking and hiding countermeasures that have been proposed, Ring Oscillator (RO)-based solutions are considered low-overhead circuitry additions that can be integrated into different circuits to hide the data dependency of power consumption by adding noise to their power signatures. The Three-Independent-Gate Reconfigurable Field-Effect Transistor (TIG-RFET) is an emerging technology that offers runtime reconfigurability between N-type and P-type operation, supports both low- V_T and high- V_T modes, and provides an internal wired-AND function, making it a strong candidate for efficient implementation of various hardware security methods. In this paper, we propose a novel reconfigurable RFET-based RO that provides controllable frequency through RFET-based inverters with reconfigurable delay. Using these ROs, we introduce a countermeasure called RETRO, which can generate noise by varying both the amplitude and frequency of power consumption. To evaluate the efficacy of RETRO, we applied it to the Piccolo S-box, a lightweight cryptographic circuit, and simulation results demonstrate that it effectively enhances resilience against Correlation Power Analysis (CPA). Furthermore, we show that reconfigurable frequency broadens the noise spectrum, making filtering considerably more difficult.

Index Terms—RFET, Hardware security, Side-channel attack, Correlation Power Analysis

I. INTRODUCTION

In recent decades, with the drastic growth in the use of connected portable digital devices such as IoT, ensuring data security has become crucial. For this reason, various standard cryptographic algorithms, such as AES and Piccolo [1], are widely used to protect sensitive data from unauthorized access or modification by encrypting the data using a secret key. Although the security of these algorithms is mathematically proven, their physical implementations may leak data through side channels such as power consumption, timing characteristics, and electromagnetic radiation. Kocher [2] first introduced Side-Channel Attacks (SCAs), which exploit the dependency between processed data and the physical behavior of a circuit to extract secret information, such as the encryption key of cryptographic circuits. Among various proposed SCAs, power attacks have attracted the most attention due to their effectiveness and practicality. Simple Power Analysis (SPA), Differential Power

Analysis (DPA), and Correlation Power Analysis (CPA) are the well-known classic power analysis methods.

Various algorithmic- and circuit-level countermeasures, such as masking and hiding, have been proposed to enhance the resilience of circuits against power SCAs by reducing the dependence between power consumption and sensitive data. Masking is an algorithmic method that introduces randomness by applying a random mask to the input, making power consumption depend on the mask, which is unknown to the attacker. Although masking is an effective countermeasure, it often significantly increases circuit size.

Hiding methods aim to reduce the Signal-to-Noise Ratio (SNR), thereby making attacks more difficult either by decreasing the exploitable signal through equalizing power consumption across different input combinations or by increasing noise through randomizing power traces. Several circuit-level power equalization techniques have been proposed to achieve almost constant and data-independent power consumption by employing dynamic differential logic styles such as Sense Amplifier-Based Logic (SABL) [3] and Wave Dynamic Differential Logic (WDDL) [4]. Although effective, in many cases, perfect power equalization is not possible. Besides, these approaches impose a large overhead on the circuit. For example, WDDL-based implementation can make a circuit 2–3 times larger. Because of these challenges, considerable research has shifted toward randomization methods. Power randomization can be realized through different approaches, such as randomly switching between different implementations of the same function [5], inserting random delays into the circuit [6], or employing Ring Oscillator (RO)-based noise generators [7]–[9].

Among these methods, RO-based randomization countermeasures offer several advantages:

- 1) *Low overhead*: they incur significantly lower area and power overhead than masking and most other hiding techniques, and they do not degrade circuit performance since they are placed alongside the circuit rather than on its critical path [7].
- 2) *Generality*: they serve as generic random noise generators that can be integrated into different circuits with minimal modifications. Moreover, unlike some other randomization methods [5], [6], they do not rely on reconfigurable hardware such as FPGAs and can also be efficiently implemented in ASICs.

Authors in [7] introduced a bank of digitally controlled ROs whose enable signals are governed by random bits from a

This work was financially supported by the Federal Ministry of Research, Technology and Space of Germany (BMFT) under project DI-ReDesign with project number 16ME0948, and by the Deutsche Forschungsgemeinschaft (DFG) within TRR 404 Active-3D with project number 528378584 and SecuReFET II with project number 439891087.

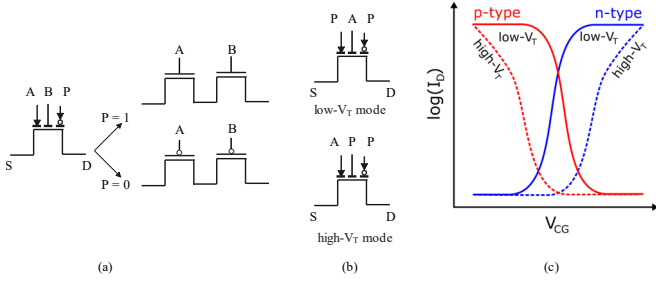


Fig. 1. TIG-RFET: (a) polarity controllability and wired-AND functionality, (b) threshold voltage reconfigurability, and (c) I-V characteristics.

random number generator, hence noise is generated by varying the number of enabled ROs in each operation. Subsequently, [8] adapted this approach for IoT applications and proposed a method to achieve a uniform distribution of the number of enabled ROs, enhancing variability. Since these works generate noise only by changing the power amplitude while the ROs operate at fixed frequencies, the resulting noise is narrowband and can be filtered out using band-pass filters or other post-processing techniques in the frequency domain [9]. In contrast, PRO [9] proposed an RO with variable length that generates noise by changing the power consumption frequency. However, this variability is achieved at the cost of additional inverters and multiplexers in each RO.

Reconfigurable Field-Effect Transistor (RFET) is an emerging technology with runtime reconfigurability between N-type and P-type modes. Among different RFET types, those with more than two independent gates, such as the Three-Independent-Gate RFET (TIG-RFET), offer internal wired-AND functionality as well as threshold voltage reconfigurability. These features position RFETs as a potent candidate for implementing hardware security solutions for IP [10] and data [11]–[14] protection.

In this paper, for the first time, we propose a reconfigurable RFET-based RO, called RETRO, as a countermeasure against power SCAs. To this end, we first design an RFET-based inverter with reconfigurable delay, and then develop an RO with variable frequency using these inverters, without the need for extra multiplexers. Moreover, we present a bank of ROs capable of generating noise through variations in both the amplitude and frequency of their power consumption. Finally, we evaluate our countermeasure by performing a CPA attack on a SPICE implementation of the Piccolo S-box.

II. BACKGROUND

A. RFET

RFETs are emerging transistors whose polarity can be set or reconfigured at run time to operate as either P-type or N-type devices by exploiting the nanoscale properties of Schottky junctions [15]. Various RFET implementations have been proposed, employing diverse materials, structures, and transport mechanisms [16]. Among them, TIG-RFET [17], [18] is one of the most common realizations (shown in Fig. 1). In TIG-RFET, the gate over the drain-side Schottky junction (DG) sets

the carrier polarity: a positive voltage enables N-type operation, while a negative voltage enables P-type operation. The other two gates control conduction mechanisms. The central gate (CG) modulates the channel’s thermal barrier to enable the low- V_T mode, whereas the gate over the source-side Schottky junction (SG) controls on/off switching for the high- V_T mode. Therefore, the TIG-RFET offers two forms of reconfigurability: polarity and threshold voltage. In addition, the availability of more than two independent gates provides an internal wired-AND functionality, which allows the integration of two transistors in series within a single TIG-RFET. Moreover, the superior control of carrier injection in RFETs results in extremely low off-currents, translating into low standby power consumption.

From a fabrication perspective, RFETs adopt widely used materials (e.g., silicon and germanium) from the semiconductor industry and follow CMOS-compatible processes, which facilitates the transition from laboratory-scale RFET prototypes to large-scale manufacturing platforms, such as 22-nm FDSOI technology [19], [20], enabling RFET-CMOS integration on a single chip [21].

The CMOS compatibility of RFETs, combined with their ability to implement compact and low-power circuits with reconfigurability and polymorphism features, makes them strong candidates for various hardware security applications [10].

B. RO-based Power SCA Countermeasures

The basic idea of RO-based countermeasures is to use a bank of controllable ROs, where the control signals can vary the amplitude or frequency of their power consumption. When this RO bank is placed near the sensitive circuit to be protected and its control signals are driven by random inputs, the power consumption profile changes each time the primary circuit operates, producing varying signatures that appear as noise in the overall power trace. The control inputs can be supplied by any random number generator, such as True Random Number Generator (TRNG) circuits.

Authors in [7] and [8] proposed a bank of identical ROs, where a random number of them are enabled each time, thereby varying the power amplitude to generate noise. Although this approach reduces the SNR, since all ROs share the same fixed frequency, the added noise remains narrowband in the frequency domain. Consequently, an attacker can suppress it using band-pass filtering during trace acquisition or post-processing in the frequency domain [9]. On the other hand, PRO [9] employs a single programmable RO whose length (i.e., the number of inverters in the oscillation path) can be adjusted to generate noise over a wider frequency band. Since only one RO is used, it is connected to an I/O pin with high load capacitance to amplify the noise. Although this countermeasure makes filtering more difficult, relying on a single RO may limit the variability of the power amplitude. In addition, frequency reconfigurability comes at the cost of extra inverters and multiplexers within the RO.

III. PROPOSED METHOD

As mentioned in Section II-B, the authors in [7] vary only the power amplitude by randomly changing the number of enabled

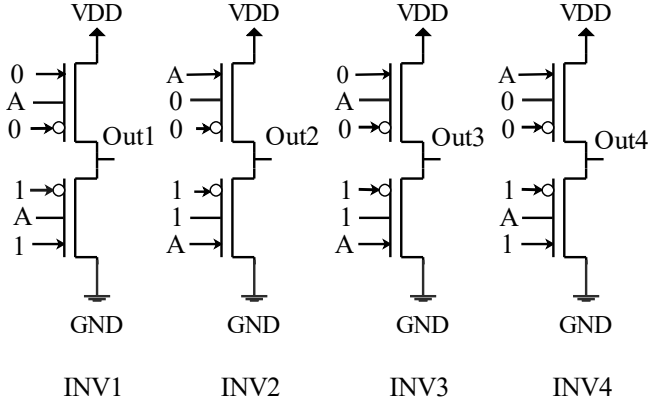


Fig. 2. Different possible RFET-based inverters based on the threshold voltages of their transistors.

ROs, resulting in narrowband noise. In contrast, PRO [9] generates noise through frequency variation by employing an RO with an adjustable length. In this section, we present RETRO, a countermeasure based on reconfigurable RFET-based ROs that generate noise by varying the frequency and amplitude of power consumption. To this end, we first introduce a novel RFET-based inverter with reconfigurable delay. We then design a reconfigurable RO composed of the proposed inverters and describe the overall structure of the countermeasure.

A. Reconfigurable RFET-based Inverter

As mentioned in Section II-A, TIG-RFET provides reconfigurability between low- V_T and high- V_T modes. Thus, as shown in Fig. 2, based on the threshold voltage of the P-type transistor in the Pull-Up Network (PUN) and the N-type transistor in the Pull-Down Network (PDN), four possible inverters can be created. In this work, we focused only on two configurations with symmetric PUN and PDN in which both transistors are low- V_T or high- V_T (INV1 and INV2 in Fig. 2). Due to the different I-V characteristics of TIG-RFET in high- V_T and low- V_T modes, shown in Fig. 1(c), the inverter composed of low- V_T transistors has higher switching speed and peak power consumption. Combining these two inverters, we created a reconfigurable inverter with fast and slow modes, which is controlled by a selector signal Sel . Internal wire-AND function of TIG-RFET allows us to integrate selection mechanisms without adding extra transistors in series. Fig. 3.(a,b) illustrates the schematic of the reconfigurable inverter. In this design, Sel controls the operating mode of the inverter: a value of '0' activates the low- V_T transistors (shown in green) for fast operation, while a value of '1' activates the high- V_T transistors (shown in red) for slow operation. In addition, we designed a special NAND gate, shown in Fig. 3.(c,d), that operates as an inverter with reconfigurable delay when $en = '1'$. This gate is used to switch the RO on or off, as explained in the following subsection.

B. RETRO Countermeasure

ROs are typically composed of an odd number of inverters, and their oscillation frequency f is determined by the number

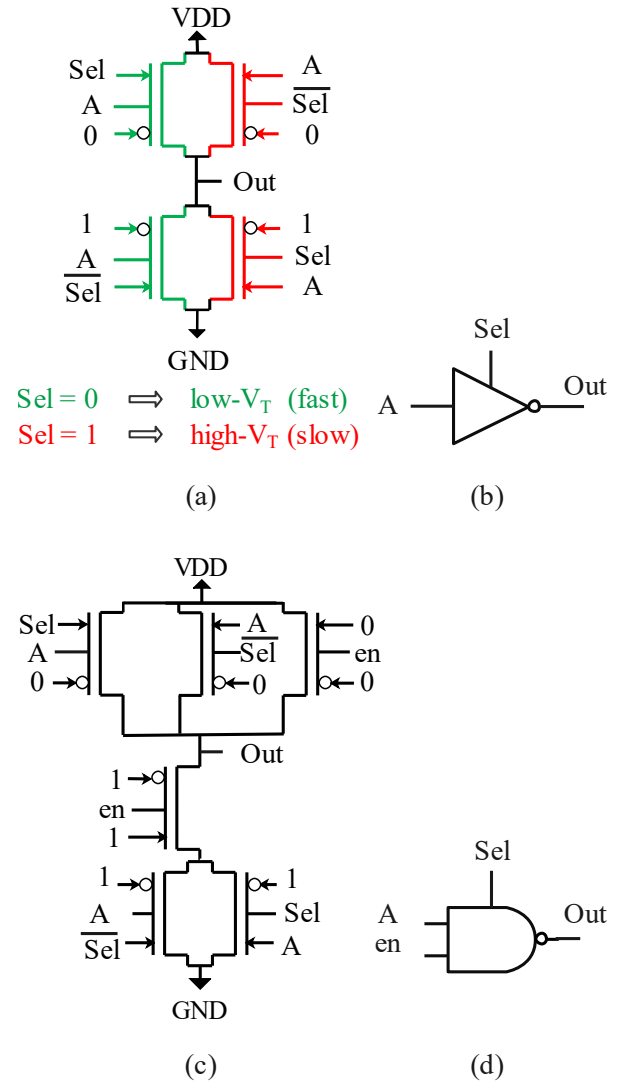


Fig. 3. Proposed RFET-based cells with reconfigurable delay: (a) transistor-level schematic and (b) logic symbol of a reconfigurable inverter, and (c) transistor-level schematic and (d) logic symbol of a reconfigurable NAND.

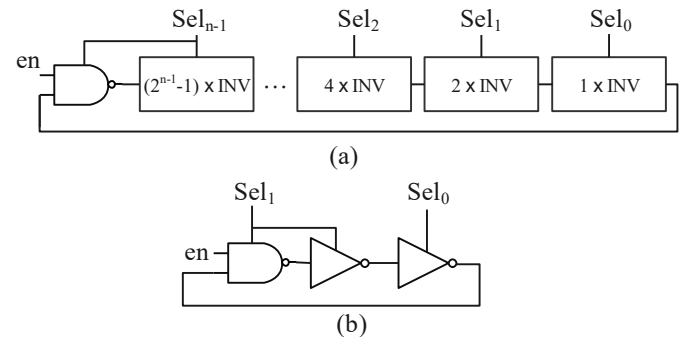


Fig. 4. Proposed RFET-based RO with reconfigurable frequency: (a) general structure of an RO with an n -bit frequency selector ($N = 2^n - 1$ stages), and (b) 3-stage RO with a 2-bit frequency selector.

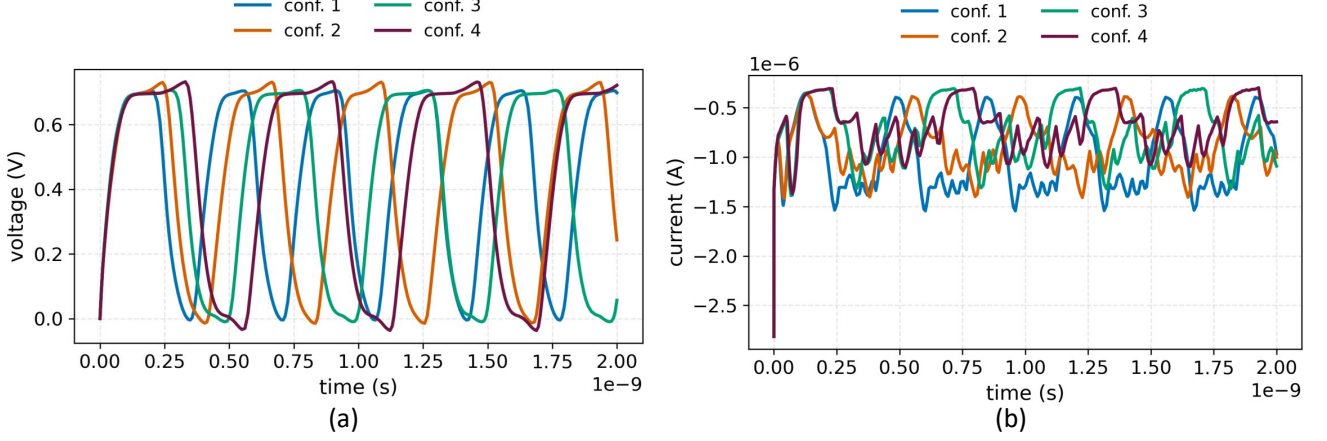


Fig. 5. (a) Output voltage and (b) current waveforms of a 3-stage reconfigurable RO under different configurations (i.e., different frequencies).

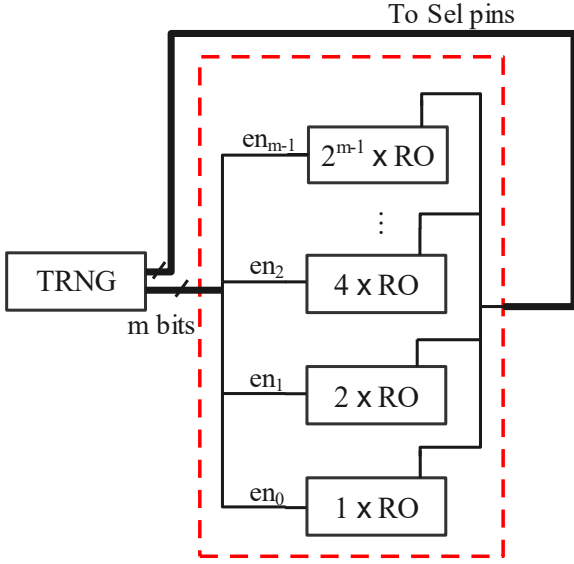


Fig. 6. The general structure of the RETRO countermeasure: a bank with an m -bit enabling signal ($M = 2^m - 1$ ROs), where each RO can have N stages. Depending on the design, each RO may either have an independent frequency selector signal or share selector signals with other ROs.

of inverters and their propagation delay. The frequency can be calculated using Formula 1:

$$f = \frac{1}{2 \cdot \sum_{i=1}^N t_{d_i}} \quad (1)$$

Where N is the total number of inverters, and t_{d_i} is the propagation delay of the inverter at stage i . PRO [9] modifies the RO frequency by bypassing a random number of inverters in the oscillation path using multiplexers, thereby changing N . In contrast, the proposed reconfigurable RFET-based inverter enables the construction of an RO with a tunable frequency by directly adjusting the delay (t_d) of each inverter.

The structure of a general N -stage reconfigurable RFET-based RO is depicted in Fig. 4.(a). The RO consists of n binary-weighted blocks ($N = 2^n - 1$), where the j -th block ($j \in [0, n-1]$) contains 2^j consecutive reconfigurable inverters,

except in the last block where an inverter is replaced by a NAND gate to activate or deactivate the RO. Fig. 4.(b) illustrates the structure of a 3-stage RO used in this work. The selector signals determine the operating mode (i.e., fast or slow) of all inverters within their corresponding blocks. With uniformly random selector bits, the binary-weighted grouping yields a uniform distribution of the number of inverters operating in the fast (or slow) mode, and consequently a uniform distribution over the possible oscillation frequencies. For example, the 3-stage RO uses a 2-bit selector that determines the RO frequency among four possible values, depending on whether 0, 1, 2, or all 3 inverters operate in fast mode. The output voltage and current waveforms of these four configurations are shown in Fig. 5. As seen in the figure, each configuration produces a distinct oscillation frequency and power trace; hence, the reconfigurable RO can serve as a noise generator to enhance SCA resilience.

To increase the noise amplitude, we considered a bank of M reconfigurable ROs with on/off control. If the enable pin of each RO is driven by an independent random signal, the number of enabled ROs follows a binomial distribution centered around $M/2$. This distribution, however, is not ideal, since greater variability is obtained with a uniform distribution [8]. To achieve this, we adopted the binary-weighted grouping method proposed in [8], which yields a uniform distribution of the number of enabled ROs. The general structure of RETRO bank is shown in Fig. 6. For a bank with $M = 2^m - 1$ ROs, an m -bit enabling signal is required.

To employ this design as an SCA countermeasure, it should be placed near the sensitive circuit, and its control signals should be driven by a TRNG. Any TRNG, such as an RFET-based TRNG [22], can be used for this purpose. Random variation of the n -bit frequency selector produces noise by altering the RO power frequency, while random variation of the m -bit enabling signals produces noise by modulating the power amplitude. As a result, the RO bank generates intense noise that cannot be easily filtered in the frequency domain.

In the general structure shown in Fig. 6, there are some parameters that should be defined by the designer regarding the

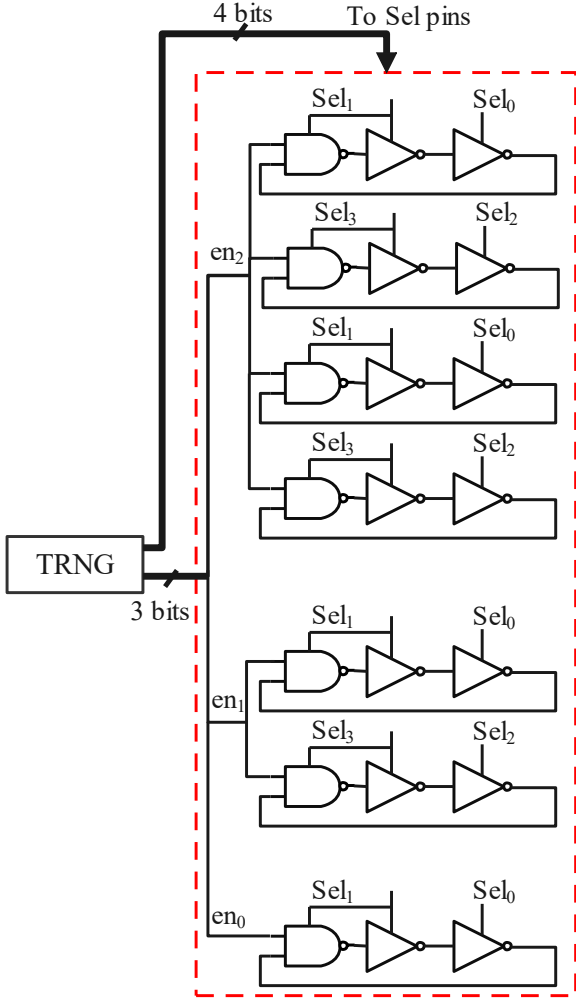


Fig. 7. Structure of the RETRO countermeasure used in the experiments of this paper.

design constraints, like acceptable overhead, type of circuits to be protected, and the target security level. These parameters include the number of ROs in the bank (M), the number of stages in each RO (N), and the maximum number of ROs whose frequencies can be independently controlled via distinct selector signals (K). For instance, if each RO has its own frequency selector signals, then $K = M$, whereas if all ROs share the same selector signals, then $K = 1$.

In this work, we target the protection of a 4-bit Piccolo S-box. Fig. 7 shows the RO bank designed for this purpose. Since the maximum possible Hamming distance of the circuit output is four, we use $m = 3$ enabling bits (i.e., $M = 7$) to generate seven (>4) distinct power levels [8]. To minimize hardware overhead, each RO is implemented with 3 stages. In addition, to keep the number of random control bits below eight, we set $K = 2$, meaning that two independent sets of frequency selector signals are used. ROs connected to different selector sets can operate at independently selected frequencies, whereas ROs sharing the same selector set operate at the same frequency. The selector sets are assigned to the ROs in a nearly balanced manner: four ROs share one selector set (Sel_0

and Sel_1), and three ROs share the other (Sel_2 and Sel_3). Consequently, the design requires $3 + 2 \times 2 = 7$ control bits ($m + K \times n$).

IV. EXPERIMENTAL RESULTS

In this section, we evaluate the efficacy of RETRO in enhancing the SCA resiliency of a circuit. To this aim, we implemented the Piccolo S-box, a lightweight cryptographic circuit for resource-constrained applications, and integrated RETRO into it. For circuit-level simulation, we first synthesized the HDL code of the S-box in Cadence Genus using basic logic cells (e.g., NAND, NOR, INV). Then, we translated the resulting gate-level netlist into a transistor-level SPICE netlist. In the protected circuit, RETRO is supplied by the same V_{DD} as the S-box, thereby introducing noise into the power traces. The entire circuit was implemented using RFET-based cells, and SPICE simulations were performed in Cadence Spectre with the 10 nm silicon nanowire (SiNW) TIG-RFET table-based model [18].

To assess circuit protection under a real attack, we performed a CPA attack using power traces obtained from the simulations. To consider the worst-case scenario, the traces were kept clean, without adding environmental or measurement noise. Fig. 8 illustrates the CPA results for the protected and unprotected circuits (with real key = 0), showing both the correlation over time and the peak correlation corresponding to each hypothetical key. Based on the results, unlike the unprotected circuit, the CPA attack cannot infer the correct key from the power traces of the RETRO-protected circuit, as the countermeasure effectively reduces the peak correlation of the real key, making it indistinguishable from other keys. Although the effect of noise can be mitigated by averaging over many traces, studies have shown that the required number of traces grows rapidly with increasing noise level [23].

In addition to the CPA attack, we also analyzed how frequency variation in ROs complicates noise filtering. For this purpose, we simulated a set of four 3-stage ROs, once when they all had the same frequency and once when each had a different frequency. Fig. 9 illustrates the power spectra of this RO set in the frequency domain. When all ROs run at the same frequency, discrete high-amplitude peaks appear. In contrast, when each RO operates at a different frequency, the energy is spread across a range of frequencies, which makes filtering considerably harder.

V. CONCLUSION

In this paper, we demonstrated how the threshold voltage reconfigurability of TIG-RFETs can be exploited to design inverter cells with reconfigurable delay. Using these inverters, we developed a novel RO with reconfigurable frequency, enabling a countermeasure that generates noise by varying both amplitude and frequency, without the costly overhead of changing RO length. Based on CPA attack results and frequency-domain analysis, the proposed countermeasure effectively produces wideband noise that enhances circuit resiliency against CPA and cannot be easily filtered due to its spectral spread.

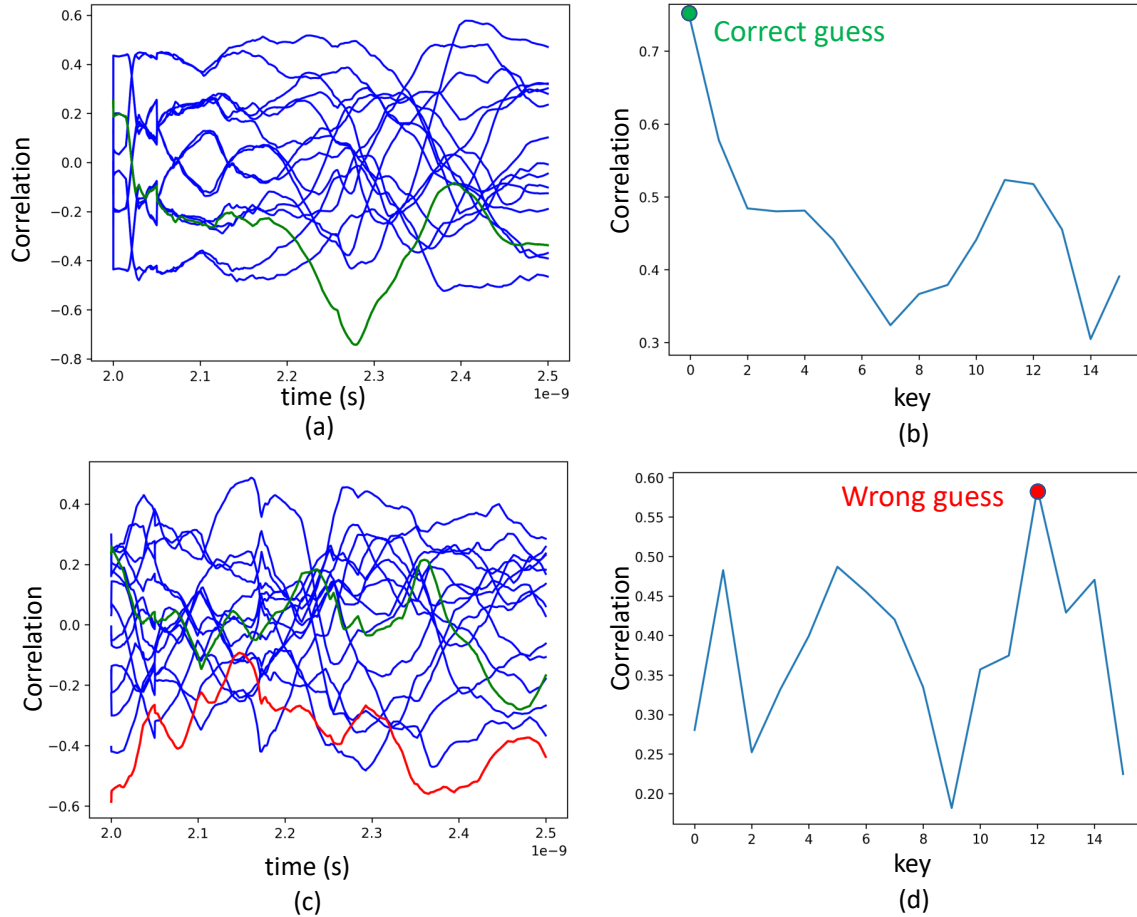


Fig. 8. CPA results on the Piccolo S-box: (a) correlation over time and (b) peak correlation for each key in the unprotected circuit, and (c) correlation over time and (d) peak correlation for each key in the RETRO-protected circuit. In (a) and (c), the green line indicates the correct key, the red line represents a wrongly guessed key, and the blue lines correspond to the remaining keys.

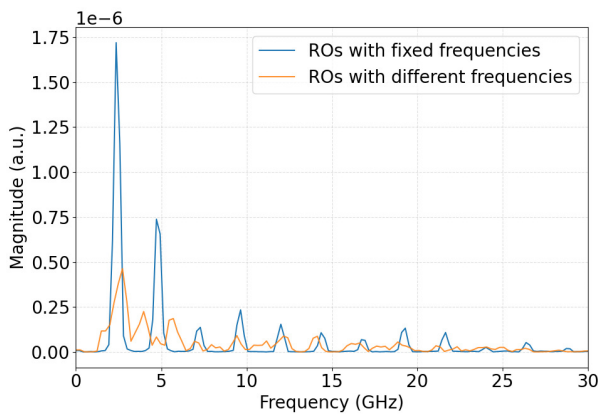


Fig. 9. Power spectra of four ROs with identical versus different frequencies.

REFERENCES

- [1] K. Shibutani, T. Isobe, H. Hiwatari, A. Mitsuda, T. Akishita, and T. Shirai, "Piccolo: an ultra-lightweight blockcipher," in *International workshop on cryptographic hardware and embedded systems*. Springer, 2011, pp. 342–357.
- [2] P. C. Kocher, "Timing attacks on implementations of diffie-hellman, rsa, dss, and other systems," in *Annual international cryptology conference*. Springer, 1996, pp. 104–113.
- [3] 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 *Proceedings of the 28th European solid-state circuits conference*. IEEE, 2002, pp. 403–406.
- [4] K. Tiri and I. Verbauwhede, "A logic level design methodology for a secure dpa resistant asic or fpga implementation," in *Proceedings Design, Automation and Test in Europe Conference and Exhibition*, vol. 1. IEEE, 2004, pp. 246–251.
- [5] B. Hettwer, J. Petersen, S. Gehrer, H. Neumann, and T. Güneysu, "Securing cryptographic circuits by exploiting implementation diversity and partial reconfiguration on fpgas," in *2019 Design, Automation & Test in Europe Conference & Exhibition (DATE)*. IEEE, 2019, pp. 260–263.
- [6] Y. Lu, M. P. O'Neill, and J. V. McCanny, "Fpga implementation and analysis of random delay insertion countermeasure against dpa," in *2008 International Conference on Field-Programmable Technology*. IEEE, 2008, pp. 201–208.
- [7] P.-C. Liu, H.-C. Chang, and C.-Y. Lee, "A low overhead dpa countermeasure circuit based on ring oscillators," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 57, no. 7, pp. 546–550, 2010.
- [8] S.-C. Chung, C.-Y. Yu, S.-S. Lee, H.-C. Chang, and C.-Y. Lee, "An improved dpa countermeasure based on uniform distribution random power generator for iot applications," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 64, no. 9, pp. 2522–2531, 2017.
- [9] Y. Yao, P. Kiaei, R. Singh, S. Tajik, and P. Schaumont, "Programmable ro (pro): A multipurpose countermeasure against side-channel and fault injection attack," in *Security of FPGA-Accelerated Cloud Computing Environments*. Springer, 2023, pp. 297–325.

- [10] S. Rai, S. Patnaik, A. Rupani, J. Knechtel, O. Sinanoglu, and A. Kumar, "Security promises and vulnerabilities in emerging reconfigurable nanotechnology-based circuits," *IEEE Transactions on Emerging Topics in Computing*, vol. 10, no. 2, pp. 763–778, 2020.
- [11] E. Giacomini and P.-E. Gaillardon, "Differential power analysis mitigation technique using three-independent-gate field effect transistors," in *2018 IFIP/IEEE International Conference on Very Large Scale Integration (VLSI-SoC)*. IEEE, 2018, pp. 107–112.
- [12] N. Kavand, A. Darjani, G. Galderisi, J. Trommer, T. Mikolajick, and A. Kumar, "Redcap: Reconfigurable rfet-based circuits against power side-channel attacks," in *2024 Design, Automation & Test in Europe Conference & Exhibition (DATE)*. IEEE, 2024, pp. 1–6.
- [13] M. M. Sharifi, R. Rajaei, P. Cadareanu, P.-E. Gaillardon, Y. Jin, M. T. Niemier, and X. S. Hu, "A novel tigtet-based dff design for improved resilience to power side-channel attacks," in *DATE*, 2020, pp. 1253–1258.
- [14] N. Kavand, A. Darjani, G. Chhabra, and A. Kumar, "Rfet-based dynamic differential logic cells against power side-channel attacks," in *2024 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*. IEEE, 2024, pp. 136–142.
- [15] T. Mikolajick, G. Galderisi, S. Rai, M. Simon, R. Böckle, M. Sistani, C. Cakirlar, N. Bhattacharjee, T. Mauersberger, A. Heinzig *et al.*, "Reconfigurable field effect transistors: A technology enablers perspective," *Solid-State Electronics*, vol. 194, p. 108381, 2022.
- [16] T. Mikolajick, G. Galderisi, M. Simon, S. Rai, A. Kumar, A. Heinzig, W. M. Weber, and J. Trommer, "20 years of reconfigurable field-effect transistors: From concepts to future applications," *Solid-State Electronics*, vol. 186, p. 108036, 2021.
- [17] J. Zhang, M. De Marchi, D. Sacchetto, P.-E. Gaillardon, Y. Leblebici, and G. De Micheli, "Polarity-controllable silicon nanowire transistors with dual threshold voltages," *IEEE Transactions on Electron Devices*, vol. 61, no. 11, pp. 3654–3660, 2014.
- [18] G. Gore, P. Cadareanu, E. Giacomini, and P.-E. Gaillardon, "A predictive process design kit for three-independent-gate field-effect transistors," in *2019 IFIP/IEEE 27th International Conference on Very Large Scale Integration (VLSI-SoC)*. IEEE, 2019, pp. 172–177.
- [19] V. Sessi, M. Simon, S. Slesazek, M. Drescher, H. Mulaosmanovic, K. Li, R. Binder, S. Waidmann, A. Zeun, A.-S. Pawlik *et al.*, "S2–2 back-bias reconfigurable field effect transistor: A flexible add-on functionality for 22 nm fdsoi," in *2021 Silicon Nanoelectronics Workshop (SNW)*. IEEE, 2021, pp. 1–2.
- [20] M. Simon, H. Mulaosmanovic, V. Sessi, M. Drescher, N. Bhattacharjee, S. Slesazek, M. Wiatr, T. Mikolajick, and J. Trommer, "Three-to-one analog signal modulation with a single back-bias-controlled reconfigurable transistor," *Nature communications*, vol. 13, no. 1, p. 7042, 2022.
- [21] N. Bhattacharjee, V. Havel, S. Kumari, N. Kavand, J. N. Quijada, A. Kumar, T. Mikolajick, and J. Trommer, "Dynamic reconfigurable security cells based on emerging devices integrable in fdsoi technology," in *2024 Design, Automation & Test in Europe Conference & Exhibition (DATE)*. IEEE, 2024, pp. 1–6.
- [22] S. Rai, N. Gupta, A. Bhattacharjee, A. Rupani, M. Raitza, J. Trommer, T. Mikolajick, and A. Kumar, "End-true: Emerging nanotechnology-based double-throughput true random number generator," in *IFIP/IEEE International Conference on Very Large Scale Integration-System on a Chip*. Springer, 2021, pp. 175–203.
- [23] L. Benini, A. Macii, E. Macii, E. Omerbegovic, F. Pro, and M. Poncino, "Energy-aware design techniques for differential power analysis protection," in *Proceedings of the 40th Annual Design Automation Conference*, 2003, pp. 36–41.