TroScan: Enhancing On-Chip Delivery Resilience to Physical Attack through Frequency-Triggered Key Generation

Jianfeng Wang, Shuwen Deng†, Huazhong Yang, Vijaykrishnan Narayanan*, Xueqing Li†
BNRist, Electronic Engineering, Tsinghua University, China; *Pennsylvania State University, USA;
†Corresponding Email: xueqingli@tsinghua.edu.cn, shuwend@tsinghua.edu.cn

***Abstract*—Keys grant access to devices and are the core secrets in logic obfuscation. Typically, keys are stored in tamper-proof memory and are subsequently delivered to logic locking modules through scan chains. However, recent physical attacks have successfully extracted keys directly from registers, challenging the security of the prior scan obfuscation/blocking efforts. This paper mitigates the threat of direct value extraction by proposing TroScan, an architecture that leverages the internal frequency of register chains to activate trigger circuits. We propose three key generation methods for typical defense scenarios and gate-aware obfuscation optimization. To the authors' best knowledge, this work presents the first on-chip key delivery obfuscation architecture against Electro-Optical Frequency Mapping (EOFM) attacks. Evaluation shows ~100% key obfuscation effectiveness under two EOFM attack targets. For overheads, we demonstrate the worst-case fault coverage rate of 97.6%, average area/power overheads of 7.5%/11.8%, and an average key generation success rate of 98% across 80 process voltage temperature (PVT) conditions.**

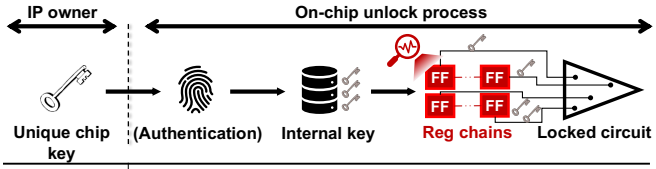
Keywords—Hardware security, logic obfuscation, scan chain, Trojan, physical attack, EOFM

I. INTRODUCTION

Logic obfuscation is commonly considered an effective measure against illegal counterfeiting and overproduction, presenting post-fabrication programmability for the globally integrated semiconductor industry [1]. The unlocked chip (referred to as the oracle) carries the secret key, prompting recent works to dedicate substantial efforts to prevent key leakage. Scan obfuscation and blocking are mainstream defense methods [2][3] as scan chains not only deliver keys but also serve as prerequisites for attackers to launch most Boolean satisfiability (SAT) attacks [4]. Both techniques provide circuit-level key protection from different perspectives, leading to the increased cost of attacks [5]-[7].

While secure scan architectures have effectively countered algorithmic attacks that rely on oracles [3], physical attacks pose a fundamental threat and have yet to gain widespread attention. In recent studies, the electro-optical frequency mapping (EOFM) attack can directly retrieve values from scan registers containing keys, and this has been validated at the hardware level [8]–[11]. Since keys in the register chain are typically either static or dynamic but based on static seeds [9], frequency-based attacks can identify and extract static values.

Existing defense designs become ineffective [8] because physical attacks target the inherent weak points of the fundamental structure of logic locking [12][13]. Even though scan obfuscation exploits dynamic keys with LFSR/PRNG, secret seeds are still static and vulnerable [3]. Fig. 1 illustrates the typical chip-unlocking process [12]. While most stages have received extensive research, the defense of the key delivery process is still lacking from the circuit level.



Design target	Uniqueness	Anti-tampering	Secure key delivery	Obfuscation
Research status	√	√	Physical attack (×)	√
Typical technique	PUF/TRNG	Tamper-proof memory	?	Logic locking

Fig. 1. Typical chip unlocking process and corresponding design target, research status, and techniques.

Therefore, for circuit designers, simply ignoring physical attacks or assuming them to be orthogonal to the hardware-level design is inappropriate.

This work proposes TroScan, the first circuit-level defense adopting the "frequency-key" delivery model that mitigates the threat of direct key extraction of physical attacks. Our key insight is to eliminate static keys in registers which are threatened by physical attacks, and use dynamic register values for key generation and delivery. To obtain the unique keys through dynamic values, TroScan harnesses the internal frequency of register chains and the Trojan triggers in the analog domain for key generation. Unlike LFSR-based approaches, TroScan can be applied to combinatorial logic locking without concerns about seed exposure. To the best of our knowledge, TroScan introduces the first frequency-triggered key generation method. In more detail, our contributions are summarized as follows:

- *TroScan architecture:* We propose the first on-chip key delivery obfuscation architecture based on a "frequency-key" delivery model that exhibits enhanced resilience against EOFM attacks.
- *Trojan-oriented key generation:* Within the TroScan architecture, we present the first design space exploration of analog circuits for frequency-triggered key generation. This exploration illustrates applicable key trigger methods tailored to three typical obfuscation scenarios.
- We conducted comprehensive evaluations. The novel "frequency-key" model exhibits ~100% key obfuscation characteristics against the EOFM attack. For overheads, TroScan shows a worst-case test coverage rate of 97.6%, average area and power overheads of 7.5% and 11.8%, and a key generation success rate of 98% under various PVT conditions.

The rest of this paper is organized as follows: Section II introduces the background. Sections III and IV present the architecture, design details, and security analysis. Section V evaluates TroScan and Section VI concludes this paper.

979-8-3503-4859-0/DATE24/© 2024 EDAA

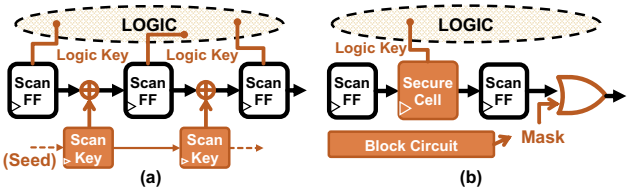


Fig. 2. Typical secure scan architectures. (a) Obfuscation. (b) Blocking.

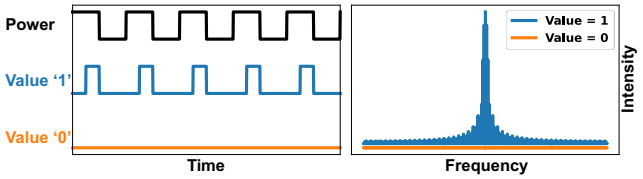


Fig. 3. Key detecting examples of EOFM. Values 0 and 1 can be distinguished through frequency analysis.

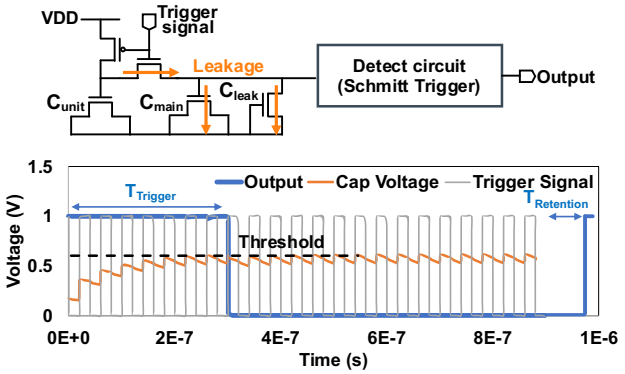


Fig. 4. Adopted trigger circuit A2 from [21] and trigger process. The output is switched to 0V at $T_{Trigger}$ when the capacitor voltage reaches the threshold voltage, and return to 1V after the trigger signal stops for $T_{Retention}$.

II. Background

This section introduces the secure scan architectures, EOFM physical attacks, and the analog trigger circuit.

A. Secure Scan Architectures

Typical secure scan architectures can be broadly categorized into two categories: scan obfuscation and blocking, as shown in Fig. 2. Scan obfuscation introduces extra static/dynamic scan keys to disrupt the input-output relationship of scan ports [14]–[16], and the scan itself is used for logic key delivery for logic locking, as shown in Fig. 2(a).

However, ScanSAT [7] and DynUnlock [17] broke prior defenses by attacking the static keys/seeds, leading to a research shift from scan obfuscation to blocking. The latter typically incorporates secure cells (SC) and block circuits (Fig. 2(b)) to mask the scan function. These designs effectively prevent key leakage through scan chains [3], [18]–[20]. For an in-depth overview of secure scan chains, please refer to [2][3].

In summary, unfortunately, since both scan architectures store static keys or seeds in registers, the recent physical attack threatens the security of the system.

B. Electro-Optical Frequency Mapping (EOFM)

Optical fault analysis techniques detect internal elements from the backside of chips. EOFM, in particular, is favored for physical attacks due to its high resolution, aligning well with modern technology nodes [11]. In EOFM, a scanning laser is used on the Device Under Test (DUT), and the reflected light is processed through a spectrum analyzer [9]. This isolates the reflected power at the switching transistor's frequency, effectively distinguishing it from the bulk material and other logic elements operating at different frequencies. Experimental validation of EOFM-based attacks has been done in [9]–[11]. Fig. 3 shows the frequency analysis example. Attackers reset the chip at a specific frequency to detect frequency variations of the target values.

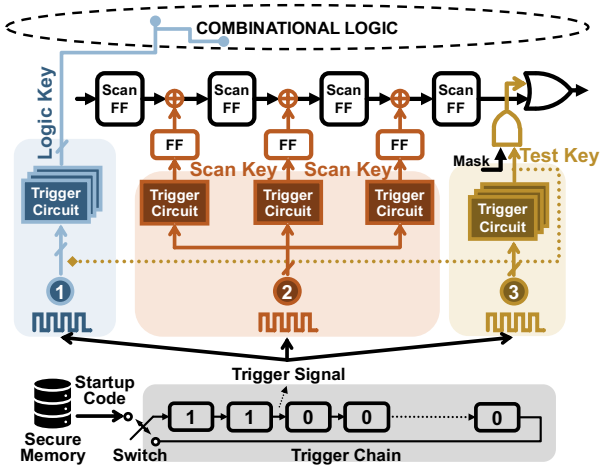


Fig. 5. The proposed TroScan architecture using the internal frequency of the trigger chain for three key generation scenarios.

C. Analog Trigger Circuit: A2 Trojan

Analog trojans are typically considered malicious hardware components that engage in covert attack processes. A2 was first introduced in [21], utilizing the trigger frequency of a trigger signal to accumulate charge and activate a malicious signal. When the trigger signal increases, the capacitor voltage rises by ΔV_C. When the trigger signal decreases, the capacitor voltage drops ΔV_L due to the presence of leakage current. If the capacitor voltage can gradually exceed the threshold of the detection circuit after $T_{Trigger}$, the output switches from 1 to 0. Otherwise, it remains untriggered. As depicted in Fig. 4, the trigger signal provides a specific input frequency. After $T_{Trigger}$, the output is switched to 0. Subsequently, when the trigger signal ends, after a time interval of $T_{Retention}$, the output signal returns to 1. In this work, we innovatively adopt Trojan triggering as a key generation method by exploring the extensive design space of frequency and circuit parameters.

III. Architecture and Methodology

The goal of this design is to generate the desired key through the frequency without relying on static register value. To achieve this objective, we introduce the TroScan architecture and subsequently present the key generation prototype for three typical obfuscation scenarios. In particular, note that this work targets key generation and delivery, we assume the designer has already determined key values.

A. TroScan Architecture

The TroScan architecture receives startup code from secure memory and generates the trigger signal by shifting bits within the trigger chain. The signal frequency is then fed into trigger circuits to generate the desired keys. As illustrated in Fig. 5, the primary distinction between the TroScan structure and traditional secure scan designs lies in the key delivery process. In TroScan, the memory dispatches a sequence of startup codes into the trigger chain. Subsequently, the trigger chain is disconnected from the memory using a switch, and the first and last bits are linked to create a circular shift register. This configuration enables the trigger chains to maintain internal frequencies through circular shifting, all without the need for additional storage capacity.

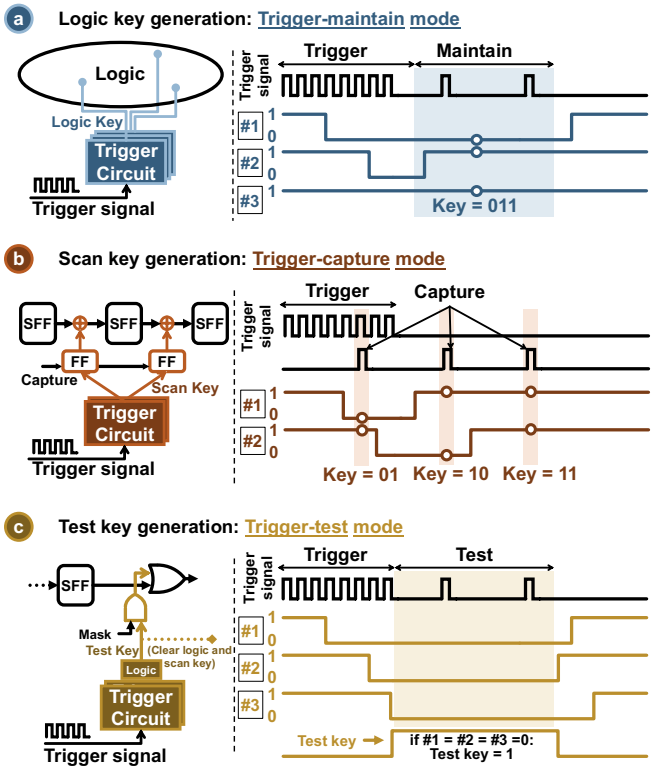


Fig. 6. The proposed three key generation methods for typical scenarios. (a) Logic locking. (b) Scan obfuscation. (c) Post-mask testing.

TroScan architecture is applicable in various key generation scenarios: (i) key for logic locking, (ii) key for scan chain obfuscation, and (iii) key for post-blocking testing. We will introduce the methodologies in the following sections.

B. Key Generation for Logic Locking

Combinational logic locking relies on keys to control circuit functions, and these keys are typically static and stable. However, the triggering process must guarantee both stable key generation and the prevention of static register values to counter physical attacks. Due to this contradiction, traditional dynamic keys cannot be used in this scenario [14]-[16].

To address this challenge, we introduce a "trigger-maintain" mode in Fig. 6(a). In this mode, the trigger chain initiates a trigger frequency, activating various trigger circuits. For example, in the given example, trigger circuit #1 activates the fastest, followed by #2, while #3 remains inactive. Note that #3 may either never be triggered or might not reach a specific trigger time, providing a space for design obfuscation. When all three trigger circuits reach the desired state (assume we need 011), they can be maintained using another frequency, typically lower. This serves the dual purpose of reducing energy consumption and thwarting potential hacking attempts targeting a single trigger frequency. We also present a verification result in Fig. 7. Circuit #1 triggers faster than #2 and retains slower than #2. Therefore, at 0.65us, #2 returns to 1 while #1 remains at 0. During the maintenance process, all three circuits maintain the value of 011. At 5us, the trigger signal stops, and #1 returns to 1 after the $T_{Retention\#1}$. Therefore, keys can be generated by selecting trigger frequencies and parameters.

C. Key Generation for Scan Obfuscation

Fig. 6(b) illustrates that the trigger circuits generate scan keys captured by flip-flops (FF). The trigger signal initiates the trigger process for a specified duration, during which #1 activates before #2. When the trigger process ends, #1 returns

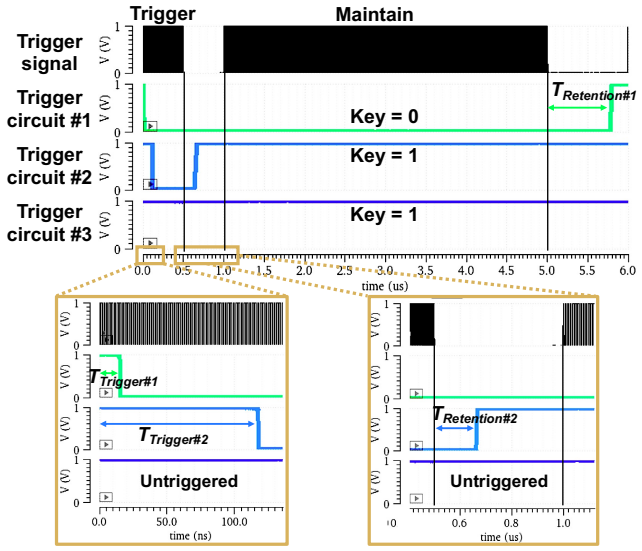


Fig. 7. Trigger process verification through SPICE simulation (key=011).

to its initial state earlier than #2 due to the lower $T_{Retention}$. By selecting three distinct capture signals, designers can sequentially obtain three different options of keys (01, 10, 11). This key space is larger than Fig. 6(a) and the primary reason is the use of registers for sampling, rather than relying on the Trojan's maintenance feature to preserve the key.

We employ FFs for capture, which might initially seem counterintuitive when considering physical attacks. However, it is crucial to note that scan chain obfuscations typically do not face the "attack one, attack all" problem. Scan structures primarily serve as aids for observation and testing purposes. Consequently, the key within the scan structure can be altered at any time without affecting the system's functionality. With this dynamic key switching, the attacker's ability to launch physical attacks on the key is diminished. Therefore, the key generation space is larger than the logic locking scenario while the requirement for registers becomes more relaxed.

D. Key Generation for Post-Blocking Testing

Recent advancements in secure scan techniques utilize a "mask" signal to block the scan chain output after the logic key is loaded. However, this approach can potentially impact in-field testing. In our design, we preserve the blocking feature while introducing a backdoor mechanism through the trigger circuit. As depicted in Fig. 6(c), when all three trigger circuits reach a specific predetermined value (for instance, 000 in this example), a test key signal is generated using an additional logic unit. This test key signal allows us to re-enable the scan output port. Simultaneously, to safeguard against leakage of both logic and scan keys, we utilize this test signal to clear all logic and scan keys within the circuit. The trigger signal in this configuration follows a pattern similar to what was described in Section III.B, involving the initial triggering and subsequent maintenance.

IV. Security Analysis and Optimization

This section analyzes the security of TroScan from the perspective of frequency analysis and algorithmic attacks.

Attack Model: Our analysis follows a model consistent with prior research [3][20]. We assume that an attacker can acquire an activated chip equipped with tamper-proof memory from the market, and that the scan structure is effectively blocked. Furthermore, we consider that the attacker has the capability to locate chip nodes and launch EOFM attacks at a reasonable

cost, aligning with scenarios discussed in [9][11].

Frequency Analysis: Here, we analyze the security of TroScan against the EOFM attack. In the key delivery model, each key register Reg_i stores static key/seed values $K_i \in \{0,1\}$. To launch EOFM attacks, the adversary firstly repeatedly resets the circuit at a specific frequency $f_{rst} = 1/T_{rst}$ and localizes Reg_i [9]. The behavior of all nodes in the circuit can be represented in the frequency domain as a linear combination of multiple frequencies, such as $f_1, f_2, \ldots, f_m$. The electric behavior for each node in the circuit can be expressed as:

$$C(t) = \sum_{n=1}^{N} A_n e^{i2\pi f_n t}, \quad t \in (0, T_{rst}) \qquad (1)$$

Here, $C(t)$ represents the node's behavior at time t, A_n is related to the amplitude for different frequencies f_n, and N is the number of orthogonal basis functions. We can use the filter to obtain the intensity A_{rst} of the reset frequency f_{rst}:

$$A_{rst} = \int_0^T C(t) \cdot e^{-i2\pi f_{rst} t} dt = \emptyset(K_i) \qquad (2)$$

A_{rst} serves to observe behavioral differences under different K_i values. In the case of static key/seed storage, the function ϕ exhibits significant variations when $K_i = 0$ and $K_i = 1$, leading to distinctions in A_{rst}. Consequently, A_{rst} can be detected from EOFM equipment and employed to infer K_i by observing these distinctions. In TroScan, both triggering key values 0 and 1 need to generate signals by registers at specific frequencies. Consequently, the values stored in registers no longer exert a substantial influence on A_{rst}, leading to a similar intensity of A_{rst} for both 0 and 1. This illustrates that inferring K_i from A_{rst} becomes more obfuscated, as $p(K_i = 0|A_{rst}) = p(K_i = 1|A_{rst})$. This obfuscation behavior is evaluated in Section V.C.

We further propose a gate-aware optimization method for enhanced obfuscation effect and provide corresponding security analysis. It is particularly noteworthy that logic gates directly connected to the key could potentially be vulnerable to EOFM identification. While some prior efforts [22] have presented physical-level defenses, TroScan introduces a novel optimization approach. We notice that in order to distinguish K_i from A_{rst}, A_{rst} exhibits distinct differences for $K_i = 0$ and $K_i = 1$. Therefore, (1) needs to satisfy the following condition: in each T_{rst} time period of each reset, $C(t)$ in (1) must manifest distinctions for $K_i = 0$ and $K_i = 1$.

Next, we implement obfuscation in the startup code and let $C(t)$ exhibit minimal differences during the T_{rst} time period, thereby invalidating the earlier condition. As depicted in Fig. 8(a), we add an extra obfuscation code before the key generation code, thereby extending the time required for key generation after power on. When the obfuscation time $T_{Obfuscation}$ surpasses the maximum detection period T_{max} of typical spectrum monitoring systems, the effectiveness of

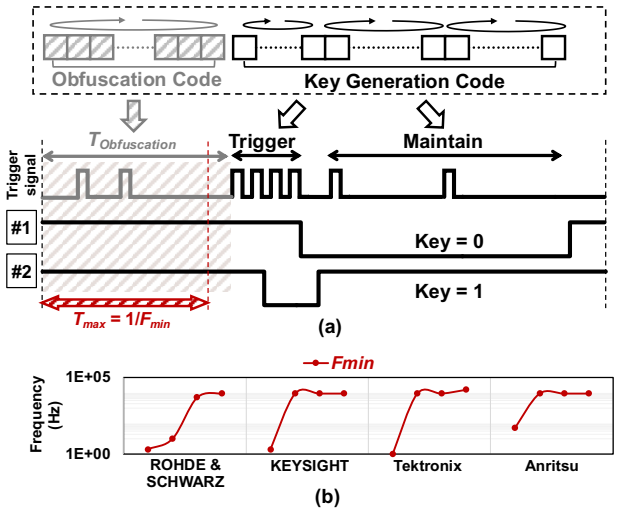


Fig. 8. The proposed obfuscation optimization scheme. (a) Obfuscation code implementation. (b) Minimum detect frequency F_{min} of 16 commercial spectrum analyzers. (Source: www.{rohde-schwarz, keysight, tek, anritsu}.com)

frequency detection diminishes. In Fig. 8(b), we conducted a survey of 16 different spectrum analyzers from four companies and determined the lowest limits for detection frequencies, denoted as F_{min}. The majority of F_{min} values were in the ~kHz range, with the lowest at 1Hz, indicating typical values for T_{max} in the millisecond range and a maximum in the second range. When $T_{max} = 1/\min(F_{min}) < T_{Obfuscation}$, frequency detection devices cannot distinguish K_i. Given that one-time key activation time can be negligible for normal execution, this approach mitigates the threats of detecting the value from logic gates as well as introduces minimum cost.

In summary, TroScan achieves two key objectives: (i) the elimination of static storage within register cells, and (ii) the obfuscation of static values connected to key gates, effectively implementing indistinguishable keys within the existing frequency detection boundary.

Algorithmic Attacks: In line with previous scan defense techniques [3][20], oracle-guided attacks, such as brute force attempts at trigger frequency or SAT-oriented attacks, are rendered ineffective due to the blocking of the scan structure of the oracle. Attacks that combine scan chain and physical attacks [11] are also thwarted, as attackers are unable to arbitrarily set all input ports from the scan. We also eliminate and optimize static values associated with secret information, thereby enhancing resistance against ScanSAT [7] and DynUnlock [17]. While it is true that attackers may attempt to compromise the system through sequential circuits, corresponding defenses can be found in [20][23].

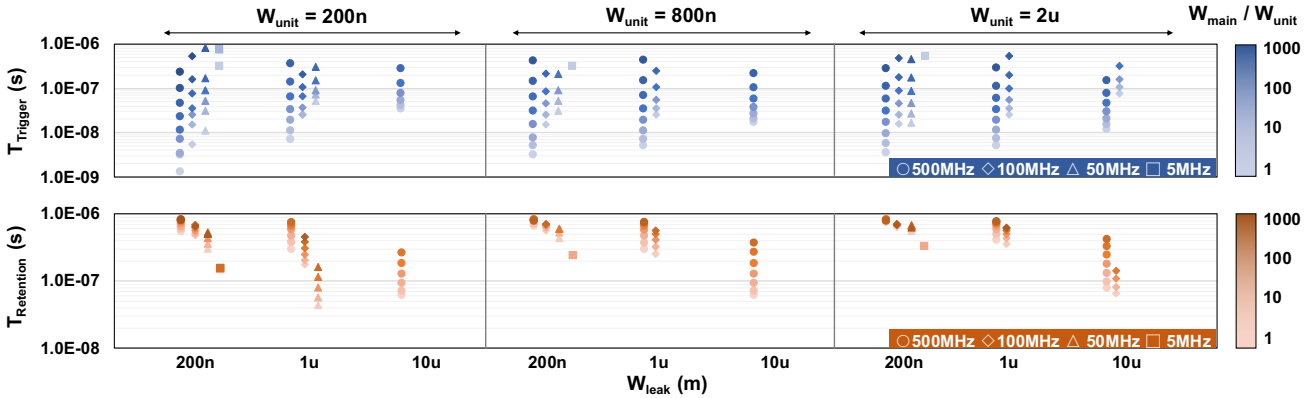


Fig. 9. A trigger and retention time evaluation of analog trigger circuits, providing multiple selection choices for key generation.

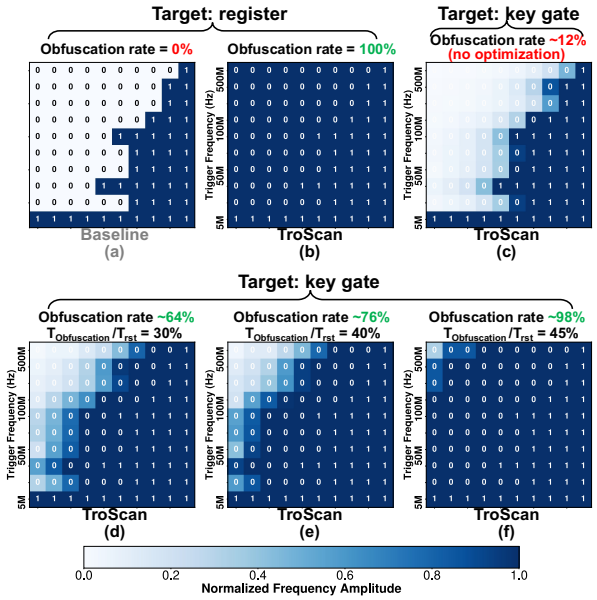


Fig. 10. The normalized frequency amplitude under different parameters during EOFM attacks. (a) Baseline without mitigating physical attack. (b-c) TroScan obfuscation effect on register and key gates (no optimization). (d-f) TroScan obfuscation effect on key gates under different $T_{Obfuscation}$ settings.

V. Evaluation

This section first explores the wide parameter space of the trigger circuit. We then evaluate and highlight the obfuscation effectiveness against EOFM attacks considering two different attack targets. To make the design more comprehensive and practical, we compare the hardware and testing overheads addressed in prior works, along with the reliability assessment.

A. Evaluation Setups

Our evaluation was conducted using nine of the most extensive benchmarks from ISCAS-89 [25] and ITC-99 [26]. We employed Cadence Virtuoso to assess the analog trigger circuits under the TSMC65 process. We used Synopsys DC Compiler for evaluating the digital components, DFT Compiler and TestMAX for the test-related evaluation.

B. Trigger Circuit Parameter Evaluation

In Section III, we provided a qualitative discussion of the key generation mechanisms. This section extends our analysis by offering a quantitative exploration of the parameter selection process for the trigger circuit.

We evaluate the trigger time $T_{Trigger}$ and retention time $T_{Retention}$ of the trigger circuit, taking into account various parameters such as trigger frequency and three transistors width W_{unit}, W_{main}, and W_{leak}, introduced in Fig. 4 [21]. The results are presented in Fig. 9, for each $W_{unit} \in$ {200nm, 800nm, 2um}, we choose three W_{leak} values, each with eight W_{main} values. Each circuit is triggered by four frequencies. There should be 8 data points per column, but some data points are missing in the figure, indicating untriggered conditions where the output remained consistently at 1. With knowledge of the trigger and retention times, specific circuit parameters can be selected to achieve the key generation.

C. Frequency Analysis Resistance

We conduct frequency analysis to demonstrate the obfuscation effect of TroScan. As illustrated in Fig. 10, we measure the normalized reset frequency amplitude of various target locations under different parameter settings. Correct key values are shown in each square. We define the obfuscation rate as the accuracy of inferred key values based on normalized amplitude (values below 0.5 are inferred as 0, and those above 0.5 are inferred as 1).

Suppose an attacker targets the key/trigger registers. We evaluate the defense without considering mitigation for EOFM attacks and TroScan. In Fig. 10(a), a noticeable distinction between the values 0 and 1 is visible under all trigger conditions. This allows attackers to infer the key based on the frequency amplitude. In Fig. 10(b), with TroScan, the generation of both 0 and 1 requires registers to periodically switch values for the specific trigger frequency. Consequently, distinguishing between 0 and 1 based on frequency amplitude becomes infeasible, as analyzed in Section IV.

We also consider attack scenarios where attackers can identify logic gates linked to a key [9]. As shown in Fig. 10(c), since logic gates typically rely on static keys to perform specific logical operations, they become vulnerable to EOFM attacks, resulting in an obfuscation rate of approximately 12%. In Fig. 10(d-f), we assess the optimization method introduced in Section IV for three cases. With a longer obfuscation time, the difficulty of distinguishing different key values gradually increases, leading to an obfuscation rate increase from 64% to 98%, while initialization time cost (milliseconds) is negligible.

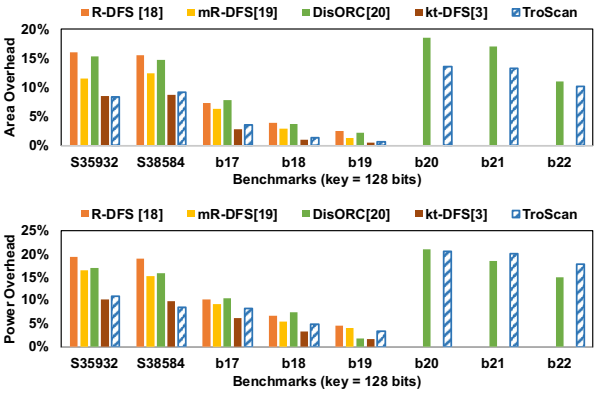


Fig. 11. Area and power overheads compared to the prior secure scan works.

TABLE I. Test Coverage Comparison

Benchmark Circuit [25][26]	Original	DisORC [20]	kt-DFS [3]	Proposed TroScan			
				w/o AMC [24]		w/ AMC [24]	
	Test	Test	Test	Test (Worst case)	Pattern	Test	Pattern
S35932	100%	100%	100%	**>98.71%**	**60**	**100%**	**66**
S38584	100%	100%	100%	**>98.94%**	**827**	**100%**	**820**
S38417	100%	No information		**>99.04%**	**1011**	**100%**	**1046**
b17	98.32%	99.91%	99.67%	**>97.60%**	**2334**	**99.53%**	**2487**
b18	99.20%	99.97%	99.73%	**>99.04%**	**6085**	**99.33%**	**6181**
b19	99.02%	99.82%	99.78%	**>98.83%**	**13814**	**99.07%**	**13810**
b20	99.99%	99.99%	No information	**>98.89%**	**1485**	**100%**	**1593**
b21	99.99%	100%		**>98.96%**	**1396**	**100%**	**1537**
b22	100%	100%		**>99.32%**	**1803**	**100%**	**1711**

D. Area and Power Overheads

We evaluate the hardware overhead of TroScan on different benchmarks and compare it to prior efforts [3], [18]-[20]. Fig. 11 shows that TroScan exhibits average area and power overheads of 7.5% and 11.8% compared to other works with 128-bit keys. The results are close to [3] and are significantly lower than [18]-[20]. This reduction can be attributed to the avoidance of secure cells, which have constituted a significant portion of the design cost in prior approaches. The main

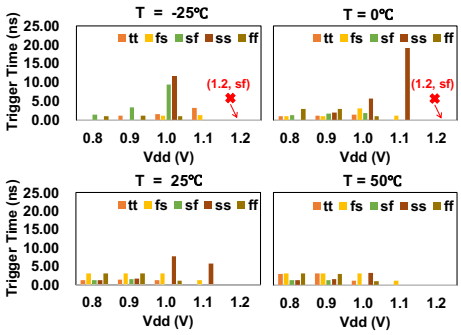


Fig. 12. Trigger time under different PVT conditions with 98% success rate.

overheads of TroScan are attributed to the power consumption arising from the frequency-triggering mechanism. However, there is no frequent bit flipping in the logic circuit, so it does not impose a substantial impact on power consumption.

E. Testing Overheads

In TroScan, the trigger circuits between the trigger chain and the circuit input restrict the flexibility of key ports during testing. We evaluate the test coverage for pre-activation tests, taking into account the impact of the trigger circuits. Table I presents the testing results for TroScan. When all key ports adhere to a specific pattern generated by the trigger chain, which is the worst-case condition, the coverage can still reach approximately 98%. To further enhance coverage, we adopted an additional multiplexer circuitry (AMC) approach [24]. This approach effectively alleviates the constraints by introducing additional MUX and test vectors, aiming for extensive fault coverage, and achieving close to 100% fault coverage.

F. PVT Conditions Analysis

This study conducted an assessment of key triggering under 80 different Process-Voltage-Temperature (PVT) conditions,. Remarkably, we achieved an impressive success rate of approximately 98% with merely two failed conditions, as illustrated in Fig. 12. This result shows the robustness of our method across diverse environmental conditions. Furthermore, it is important to note that this high success rate was attained without introducing significant timing variations, affirming the reliability of our proposed approach.

G. More Discussions and Future Works

At the architecture level, improving fault coverage when key ports are constrained could be further explored. For logic locking, we do not focus on evaluating SAT attack and logic locking-related indicators in this work due to the different design phases and attack models. Although this work focuses on key delivery, there is still room to investigate the compatibility of TroScan with various logic locking [1] and programmable logic camouflage [27] techniques.

VI. Conclusion

This work proposes TroScan, a novel architecture aiming at enhancing resilience against EOFM attacks. TroScan employs a "frequency-key" delivery mechanism, eliminating static storage in registers and making it challenging to directly access secret values. Within TroScan, we introduce three key generation strategies and gate-aware optimizations for typical obfuscation scenarios. To the best of our knowledge, this work presents the first obfuscation delivery architecture and the first key generation method using analog triggers, leading to secure on-chip key delivery against EOFM attacks.

The evaluation shows that TroScan achieves close to 100% key obfuscation effectiveness under two attack targets while ensuring fault coverage of at least 97.6%. The average overheads for area and power are 7.5% and 11.8%, respectively, on par with the state-of-the-art work. Through PVT simulations, we show a key generation success rate of approximately 98%. By addressing the limitations inherent in existing key delivery models, this work contributes to a novel defense mechanism capable of countering EOFM attacks.

VII. Acknowledgment

This work is supported in part by National Key R&D Program of China (#2019YFA0706100), NSFC (#U21B2030, #92264204), and NSF (#2008365).

References

[1] H. M. Kamali, K. Z. Azar, F. Farahmandi, and M. Tehranipoor, "Advances in Logic Locking: Past, Present, and Prospects". Cryptology ePrint Archive, 2022.
[2] K. Z. Azar, H. M. Kamali, H. Homayoun, and A. Sasan, "From Cryptography to Logic Locking: A Survey on the Architecture Evolution of Secure Scan Chains," IEEE Access, 2021.
[3] H. M. Kamali, "Secure and Robust Key-Trapped Design-for-Security Architecture for Protecting Obfuscated Logic". Cryptology ePrint 2022.
[4] P. Subramanyan, S. Ray, and S. Malik, "Evaluating the security of logic encryption algorithms," in 2015 IEEE HOST, Washington, US, May.
[5] M. E. Massad, S. Garg, and M. Tripunitara, "Reverse engineering camouflaged sequential circuits without scan access," in 2017 ICCAD.
[6] K. Shamsi, M. Li, D. Z. Pan, and Y. Jin, "KC2: Key-Condition Crunching for Fast Sequential Circuit Deobfuscation," in 2019 DATE.
[7] L. Alrahis et al., "ScanSAT: Unlocking Static and Dynamic Scan Obfuscation," IEEE TETC, vol. 9, no. 4, pp. 1867–1882, Oct. 2021.
[8] L. Lavdas, M. T. Rahman, and N. Asadizanjani, "Application of Optical Techniques to Hardware Assurance," in Emerging Topics in Hardware Security, M. Tehranipoor, Ed., Cham: 2021.
[9] M. T. Rahman, S. Tajik, M. S. Rahman, M. Tehranipoor, and N. Asadizanjani, "The Key is Left under the Mat: On the Inappropriate Security Assumption of Logic Locking Schemes," in 2020 IEEE HOST.
[10] T. Krachenfels, F. Ganji, A. Moradi, S. Tajik, and J.-P. Seifert, "Real-World Snapshots vs. Theory: Questioning the t-Probing Security Model," in 2021 IEEE SP, San Francisco, CA, USA.
[11] M. Zuzak, Y. Liu, I. McDaniel, and A. Srivastava, "A Combined Logical and Physical Attack on Logic Obfuscation," in Proceedings of the 41st IEEE/ACM ICCAD, San Diego California.
[12] S. Engels, M. Hoffmann, and C. Paar, "A critical view on the real-world security of logic locking," JCE., vol. 12, pp. 229–244, Sep. 2022.
[13] M. T. Rahman et al., "Defense-in-depth: A recipe for logic locking to prevail," Integration, vol. 72, pp. 39–57, May 2020.
[14] R. Karmakar, H. Kumar, and S. Chattopadhyay, "Efficient Key-Gate Placement and Dynamic Scan Obfuscation Towards Robust Logic Encryption," IEEE TETC, vol. 9, no. 4, pp. 2109–2124, Oct. 2021.
[15] R. Karmakar et al., "A scan obfuscation guided design-for-security approach for sequential circuits," IEEE TCAS II: Express Briefs, 2019.
[16] Dongrong Zhang, Miao He, Xiaoxiao Wang, and M. Tehranipoor, "Dynamically obfuscated scan for protecting IPs against scan-based attacks throughout the supply chain," in 2017 IEEE 35th VTS.
[17] N. Limaye and O. Sinanoglu, "DynUnlock: Unlocking Scan Chains Obfuscated using Dynamic Keys," in 2020 Design, Automation & Test in Europe Conference & Exhibition (DATE), IEEE, Mar. 2020.
[18] U. Guin,et. al, "Robust Design-for-Security Architecture for Enabling Trust in IC Manufacturing and Test," TVLSI 2018.
[19] N. Limaye, A. Sengupta, M. Nabeel, and O. Sinanoglu, "Is Robust Design-for-Security Robust Enough? Attack on Locked Circuits with Restricted Scan Chain Access," in 2019 IEEE/ACM ICCAD.
[20] N. Limaye, E. Kalligeros, N. Karousos, I. G. Karybali, and O. Sinanoglu, "Thwarting All Logic Locking Attacks: Dishonest Oracle With Truly Random Logic Locking," IEEE TCAD, Sep. 2021.
[21] K. Yang, M. Hicks, Q. Dong, T. Austin, and D. Sylvester, "A2: Analog Malicious Hardware," in 2016 IEEE SP, San Jose, IEEE, May 2016.
[22] M. T. Rahman, N. F. Dipu, D. Mehta, S. Tajik, M. Tehranipoor, and N. Asadizanjani, "CONCEALING-Gate: Optical Contactless Probing Resilient Design," ACM JETCAS., vol. 17, no. 3, pp. 1–25, Jul. 2021.
[23] N. Limaye and O. Sinanoglu, "RESCUE: Resilient, Scalable, High-corruption, Compact-Key-Set Locking Framework," TCAD, 2022.
[24] M. Yasin, S. Mohamed Saeed, J. (JV) Rajendran, and O. Sinanoglu, "Activation of Logic Encrypted Chips: Pre-Test or Post-Test?," in Proceedings of the 2016 DATE pp. 139–144.
[25] F. Brglez, D. Bryan and K. Kozminski, "Combinational profiles of sequential benchmark circuits," IEEE ISCAS, Portland, USA, 1989.
[26] F. Corno, et. al, "RT-level ITC'99 benchmarks and first ATPG results," in IEEE D&T of Computers, July-Sept. 2000
[27] J. Wang, et al, "A Module-Level Configuration Methodology for Programmable Camouflaged Logic," in TODAES, 2024.