Synthesis of Coupling Capacitance Based Hidden State Transitions for Sequential Logic Locking

Pratik Shrestha and Ioannis Savidis
Department of Electrical and Computer Engineering, Drexel University
Philadelphia, Pennslyvania 19104
ps937@drexel.edu, isavidis@coe.drexel.edu

2022 IEEE International Symposium on Circuits and Systems (ISCAS) | 978-1-6654-8485-5/22/$31.00 ©2022 IEEE | DOI: 10.1109/ISCAS48785.2022.9937990

***Abstract*—Oracle guided attacks, such as the SAT attack, and finite state machine (FSM) reconstruction-based structural attacks are two primary threats to sequential logic obfuscation of an integrated circuit (IC). Recent defense mechanisms apply hidden state transitions (HST) and logic cone modifications to a partitioned FSM to protect against both oracle-guided and structural attacks. HST triggering techniques are implemented on select state registers to induce controlled timing glitches in the FSM. However, the current implementations of HST are vulnerable to structural attack through the gate-level logic implementing the trigger. In this paper, a random walk-based security estimation metric is utilized to quantify the security of gate-level masking of the triggering topology. A novel coupling capacitance-based HST triggering topology is proposed, where the glitch is induced by manipulating the physical properties of the circuit rather than the gate-level logic. An average increase of 8.53x in the random walk-based security estimation score and an 887x increase in the geometric mean of the expected number paths to extract the key is observed for coupling capacitance based HSTs as compared to traditionally triggered HSTs. The schematic level equivalent of the proposed technique is implemented on a subset of ISCAS'89 benchmark circuits, resulting in an average overhead in area and power of 14.35% and 22.02% for all benchmark circuits and 2.23% and 1.25% for the four largest benchmark circuits, respectively, as compared to the original unobfuscated circuits.**

***Index Terms*—logic encryption, logic locking, hardware security, sequential obfuscation**

I. Introduction

As the semiconductor industry increasingly embraces a fabless fabrication model instead of in-house manufacturing of ICs, the security of the IC becomes a critical consideration. The outsourcing of IC fabrication to third-party foundries requires the revealing of intellectual property (IP) to a potentially untrusted entity. The threat of IP theft, counterfeiting, overproduction, and malicious changes necessitates the development of measures to secure the IC at different stages of the design and production flow.

Logic locking [1] encompasses a set of techniques that protect ICs from IP piracy, counterfeiting, and Trojan insertion. The obfuscation techniques protect IP through the insertion of key-controlled logic gates that mask the true functionality of the circuit, which renders a locked IC useless. The keys are owned by the IP owner(s) and are not shared with the untrusted foundry. The oracle-guided SAT attack [2] has been developed to effectively determine the keys of an IC locked with traditional key-based obfuscation. Techniques that obfuscate the finite state machine (FSM), including HARPOON [3], partition the FSM of a sequential IP block into an obfuscated and functional mode, which prevents oracle access to the obfuscated mode once the IP is activated and, therefore, secures the IP from SAT attacks. However, such techniques are vulnerable to structural attacks [4].

Hidden state transition (HST) based obfuscation [5] is a novel approach to sequential logic locking that enhances the masking of the FSM by applying an intentional timing glitch on a state register. The intentional timing glitch triggers a state transition not defined in the FSM of the circuit. Masking the glitching topology in the gate level netlist adds an additional layer of security to techniques implementing sequential obfuscation.

In this paper, a multiplexer-based circuit topology is proposed as a trigger of the hidden state transition.The modified circuit is utilized to assess the security of the obfuscation technique using random walk analysis. In addition, a synthesis flow that generates and integrates coupling capacitance-based hidden state transitions is proposed for the implementation of sequential logic obfuscation of a circuit. A closed-form impedance model is used to evaluate the efficacy of the technique on ISCAS'89 benchmark circuits. The proposed obfuscation technique introduces changes to the IC at the physical level (i.e. coupling capacitance) rather than the logical level such that the changes are not observable in the reverse-engineered gate-level netlist.

The paper is organized as follows. Background on HST based logic obfuscation and synthesis is provided in Section II. The assumed threat model and the random walk-based metric that quantifies the achieved security are discussed in Section III. The synthesis of coupling capacitance-based hidden state transitions is described in Section IV, and an analysis of the overhead to implement the proposed technique is provided in Section V. Some concluding remarks are provided in Section VI.

II. Background on Hidden State Transition based Sequential Logic Locking

A sequential circuit obfuscation technique is proposed where the FSM of an IC is partitioned into obfuscated and functional modes and an HST is utilized to transition between the partitions [5]–[7]. An implementation of a hidden state transition within an FSM is shown in Fig. 1, where instead of completing a normal state transition from state S2 to S1 when applying input X=1, a hidden state transition from state S2 to S3 is triggered. The transition effectively moves the circuit from the obfuscated mode to the functional mode.

*This work was supported in part by the Office of Naval Research under Award N00014-22-1-2071.

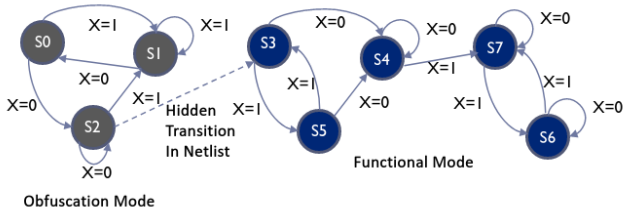


Fig. 1: Obfuscated FSM with a hidden state transition. The hidden state transition occurs between states S2 and S3 when an input of X=1 is applied.

A. Synthesis Algorithm for Hidden State Transitions

An algorithm is described in [5] that partitions a circuit into obfuscated and functional modes, modifies the partitioned FSM, and incorporates hidden state transitions that are triggered by applying a target key sequence. The steps to execute the algorithm are shown in Fig. 2.

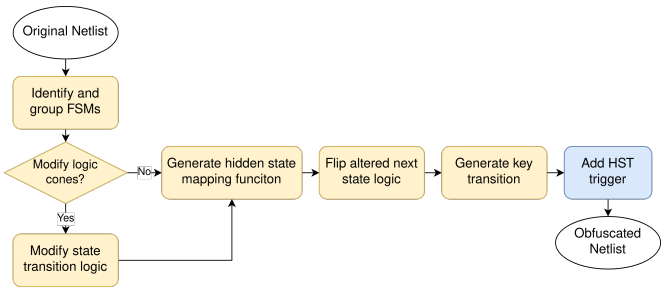


Fig. 2: Flow graph of the synthesis algorithm that implements hidden state transitions [5]. Steps highlighted in yellow are common to all HST synthesis flows. The step highlighted in blue is added for the implementation of the triggering mechanism.

B. Triggering Hidden State Transitions

Triggers are inserted in a circuit to permit hidden state transitions between partitions of an FSM. Consider N2, N1, and N0 as the encoding of the state registers of the FSM shown in Fig. 1. If an intentional timing violation is generated by forcing the data signal applied as an input to register N1 to miss the necessary arrival time, the value currently stored in N1 persists through the next clock cycle, which effectively leads to a transition from state S2 (0**1**0) to S3 (0**1**1) instead of to S1 (0**0**1) when an input of X=1 is applied. Implementing key gating-based hidden state transitions does not require changing the frequency of the circuit. Instead, the clock input of the target register is connected to clock gating logic triggered by the key K0 as shown in Fig. 3a.

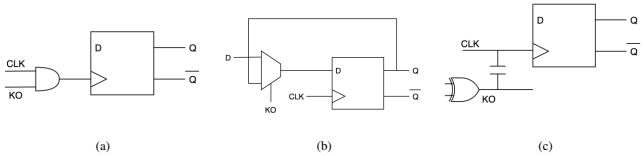


Fig. 3: Modified state register topologies that trigger hidden state transitions: (a) clock gating based trigger, (b) multiplexer based trigger, (c) coupling capacitance based trigger.

III. Security Overview

In Section III-A, the threat model considered for evaluation of the obfuscation technique is defined. In addition, a random walk based analysis is performed to quantitatively evaluate the security of the proposed technique in Section III-B.

A. Threat Model

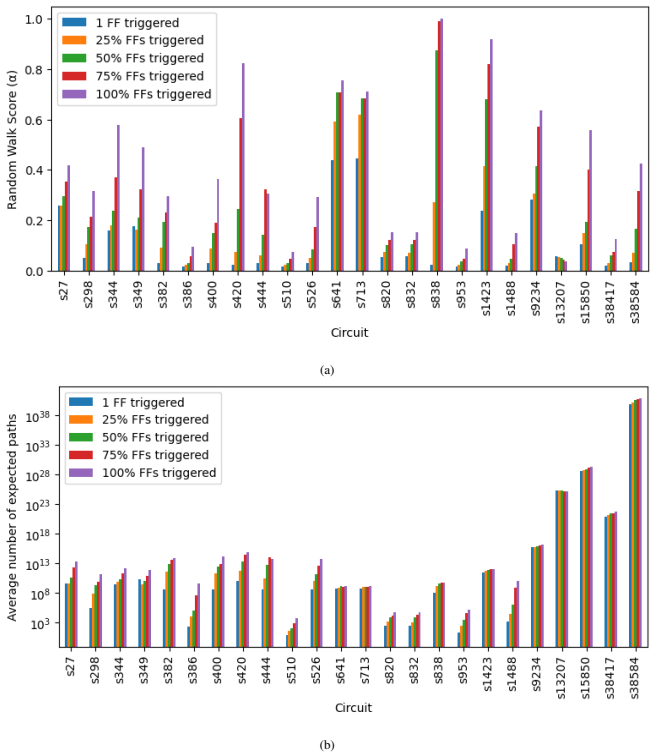
Based on the threat models described in [2] and [5], an adversary is assumed to have access to a reverse-engineered gate-level netlist and an activated functional IC (oracle). The objective of the adversary is to obtain the correct input key sequence from a locked IC. Attacks an adversary might employ include oracle guided attacks [2], FSM extraction [4], or random walk based activation sequence extraction [5].

B. Activation Sequence Extraction

Since an HST-triggered topology allows for multiple candidate transitions between obfuscated and functional mode, the circuit is no longer vulnerable to FSM extraction and Strongly Connected Component (SCC) based structural attacks. SAT attacks are also infeasible as access to an oracle IC only provides information regarding the state transitions of a circuit operating in the functional mode. Therefore, the adversary has to find a path from the starting state of the obfuscated mode to the starting state of the functional mode in s cycles. Given an FSM with n inputs and f state flip-flops, the expected number of paths $E[X] = \frac{[\alpha \times 2^{min(n,f)}]^s}{2}$ is proposed as a security measure in [5], where α is a weighted term between 0 and 1 obtained by performing a random walk analysis.

One of three scenarios is possible: I) the adversary is unaware of the implementation of the HST, II) the adversary is aware of the implementation of the HST but does not know which specific flip flop is glitched, and III) the adversary is aware of the implementation of the HST and also knows the specific glitched flip flop(s). In case I, the adversary disregards the critical HST and, therefore, never reaches the functional mode. For cases II and III, a random walk analysis is performed to characterize the security of the FSM.

The HST synthesis algorithm described in Section II-A is applied on ISCAS'89 benchmark circuits. The key-gating based HST triggering topology shown in Fig. 3a is replaced with the functionally equivalent multiplexer based topology shown in Fig. 3b. The random walk score α and the average number of expected paths to reach the functional mode are shown in Fig. 4 as a function of the proportion of glitched state registers. The random walk score α for circuits with all registers considered as potential glitching targets is 8.53x times higher on average than for circuits with one register considered for glitching. A corresponding exponential increase in the average number of expected paths for sequence extraction is observed. When considering the geometric mean, the average number of paths for circuits with all registers considered is 887x times higher than for circuits with one register considered. Therefore, assuming knowledge of the implementation of the HST, the least effort for the adversary to determine the key sequence is for case III, while case II requires the most effort as the adversary must assume all available flip-flops trigger HSTs when performing the random walk analysis. Since the efficient masking of the glitching topology prevents an adversary from targeting a subset of glitched registers, a capacitive coupling based trigger as shown in Fig. 3c results in registers that are indistinguishable from the normal state registers of a reverse-engineered gate level netlist.



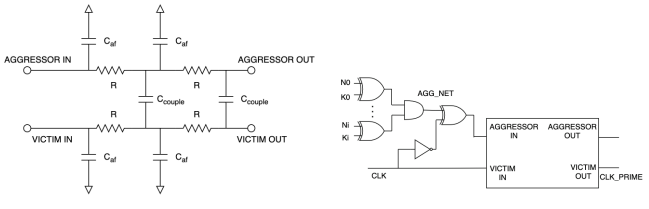
(a)

(b)

Fig. 4: Results from random walk analysis of the ISCAS'89 benchmark circuits with increasing proportion of glitch triggered flip-flops: (a) random walk score α and, (b) average number of expected paths (in log scale).

IV. Coupling Capacitance based Hidden State Transitions

Consider an obfuscated sequential IP block. The initial steps to synthesize an HST up to the insertion of the HST trigger are identical to the synthesis flow described in [5]. However, the topology to trigger glitches on the clock input based on capacitive coupling between the clock signal (CLK) of a state register and a keyed aggressor (K0), as shown in Fig. 3c, is utilized instead of the topology shown in Fig. 3a. The magnitude of the coupling capacitance and the subsequent delay that is produced is modified by changing the physical attributes of the interconnect including the coupling length, the spacing between the coupled interconnects, the transistor sizing of the driving gate(s) [8], and the propagating direction of the signals between the victim and aggressor. Extensive research has been performed on the modeling of coupling capacitance and the resulting delay [9], [10] as well as in the development of optimization algorithms [8], [11] that minimize the coupling capacitance.



(a) (b)

Fig. 5: Circuit implementation of a coupling capacitance based trigger of HST where a) depicts an interconnect *RC* model with C_{couple} and C_{af} calculated from closed form expressions proposed in [10], and b) depicts a circuit topology that utilizes the interconnect *RC* model that couples the aggressor net with the target clock net.

A. Modelling Interconnect Capacitance

Interconnect capacitance is composed of two components: 1) coupling capacitance, C_{couple}, between adjacent wires and 2) interconnect to ground capacitance, C_{af}, resulting from the parallel area and fringe flux to the underlying plane. Closed-form expressions of the capacitive components are utilized [10]. The resulting calculated capacitances are applied to an RC model of the interconnect, as shown in Fig. 5a, which provides an approximate estimate of the coupled crosstalk noise utilized to trigger the coupling capacitance based HST described in Section IV-B.

B. Synthesis of Coupling Capacitance based Hidden State Transitions

The ISCAS'89 benchmark circuit s27, with a set of state registers (N1, N2, N3), is considered for implementation of the HSTs. First, the synthesis algorithm described in Section II-A is executed on the s27 circuit to identify hidden state transitions and to add a hidden state register HS. A path from the obfuscated mode to the functional mode is determined starting from the encoded state (N1, N2, N3, HS) = (1, 0, 0, 1) in the obfuscated mode to the state (1, 0, 1, 1) in the functional mode by glitching state register N1, which differs from the expected ending state in the obfuscated mode of (1, 0, 1, 0). An aggressor logic net, AGG_NET, is introduced to the circuit that is set to logic 1 when the FSM is at the starting state of the HST (1, 0, 0, 1) and logic 0 when the FSM is in any other state. AGG_NET is XOR-ed with an inverted clock signal to obtain the aggressor signal AGG. The branch of the clock network from the clock source CLK to the state register S1 is coupled with the aggressor AGG. The victim line is referred to as CLK_PRIME. The circuit implementing the coupling between the aggressor and victim is shown in Fig. 5b. Elements with variable delays such as current starved buffers [12] are added to the data input of register N1 to reduce the positive slack to a minimum, which limits a given HST to a specific set of triggers (frequencies, glitched signals, etc). The induced glitch is sufficient to produce a timing violation that triggers an HST. The complete synthesis flow for the insertion of coupling capacitance based HSTs is shown in Fig. 6.

The obfuscated s27 netlist is synthesized in a TSMC 65 nm technology node using Synopsys DC Compiler and imported into Cadence Virtuoso. A coupling length of 100 µm and an interconnect spacing of 25 nm are selected. The schematic simulation of the circuit at a 1 GHz frequency is shown in Fig. 7a. When the FSM reaches state (1, 0, 0, 1), the aggressor induces crosstalk noise on the clock signal that results in

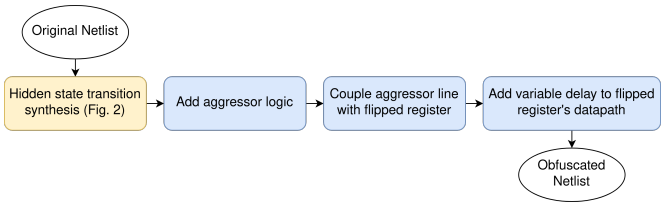


Fig. 6: Synthesis flow for the coupling capacitance based Hidden State Transitions. Steps highlighted in blue add coupling capacitance based triggers.

TABLE I: Area and power analysis of ISCAS'89 circuits without obfuscation, with key-gating based HST obfuscation, and with coupling capacitance based HST obfuscation.

Circuits	No. of inputs	No. of FFs	No. of gates	Original		Key gating based HST		Coupling capacitance based HST		Overhead: Original vs Key gating based HST		Overhead: Original vs Coup. based HST		Overhead: Key gating vs Coup. based HST	
				Area (nm^2)	Power (mW)	Area (nm^2)	Power (mW)	Area (nm^2)	Power (mW)	Area	Power	Area	Power	Area	Power
s27	4	3	10	3.10E+01	3.28E-02	5.22E+01	4.99E-02	5.62E+01	5.15E-02	68.60%	52.07%	81.40%	57.11%	7.59%	3.31%
s298	3	14	119	1.91E+02	1.94E-01	2.10E+02	2.10E-01	2.24E+02	2.13E-01	9.81%	8.20%	17.17%	9.85%	6.70%	1.52%
s344	9	15	160	2.13E+02	1.89E-01	2.62E+02	2.88E-01	2.80E+02	2.13E-01	22.60%	52.94%	31.20%	12.89%	7.02%	-26.19%
s349	9	15	161	2.13E+02	1.89E-01	2.56E+02	2.89E-01	2.74E+02	2.10E-01	19.90%	53.37%	28.16%	11.19%	6.89%	-27.50%
s382	3	21	158	2.81E+02	2.35E-01	3.05E+02	2.55E-01	3.21E+02	2.58E-01	8.58%	8.50%	14.21%	9.60%	5.19%	1.02%
s386	7	6	159	1.72E+02	8.92E-02	1.93E+02	9.05E-02	1.96E+02	9.12E-02	12.16%	1.45%	14.05%	2.26%	1.68%	0.80%
s400	3	21	162	2.79E+02	2.37E-01	3.02E+02	2.61E-01	3.19E+02	2.64E-01	8.25%	10.10%	14.05%	11.58%	5.36%	1.34%
s420	19	16	196	2.61E+02	1.63E-01	2.74E+02	1.74E-01	2.76E+02	1.79E-01	4.96%	6.43%	5.51%	9.37%	0.52%	2.76%
s444	3	21	181	2.83E+02	2.38E-01	3.03E+02	2.99E-01	3.14E+02	3.07E-01	6.86%	25.62%	10.93%	28.77%	3.80%	2.51%
s510	19	6	211	2.69E+02	1.18E-01	2.95E+02	2.58E-01	3.01E+02	2.61E-01	9.64%	118.64%	11.91%	120.76%	2.08%	0.97%
s526	3	21	193	2.88E+02	2.40E-01	3.06E+02	2.47E-01	3.25E+02	2.57E-01	5.99%	3.01%	12.86%	7.18%	6.48%	4.05%
s641	35	19	379	3.07E+02	2.15E-01	3.32E+02	2.25E-01	3.56E+02	2.29E-01	8.09%	4.66%	15.94%	6.56%	7.27%	1.82%
s713	35	19	393	3.05E+02	2.13E-01	3.27E+02	2.31E-01	3.43E+02	2.37E-01	7.08%	8.30%	12.26%	11.25%	4.85%	2.73%
s820	18	5	289	3.12E+02	8.79E-02	3.28E+02	1.00E-01	3.42E+02	9.44E-02	5.07%	13.85%	9.46%	7.38%	4.17%	-5.68%
s832	18	5	287	3.15E+02	8.75E-02	3.41E+02	1.38E-01	3.42E+02	1.42E-01	8.23%	57.87%	8.57%	62.67%	0.32%	3.04%
s838	35	32	390	5.30E+02	3.17E-01	5.32E+02	3.33E-01	5.48E+02	3.32E-01	0.34%	5.21%	3.26%	4.80%	2.91%	-0.39%
s953	16	29	395	5.89E+02	3.24E-01	6.02E+02	4.34E-01	6.08E+02	4.40E-01	2.14%	33.96%	3.30%	35.88%	1.14%	1.43%
s1423	17	74	657	1.28E+03	8.61E-01	1.32E+03	9.56E-01	1.37E+03	9.68E-01	3.15%	11.09%	6.83%	12.49%	3.57%	1.25%
s1488	8	6	653	6.16E+02	1.83E-01	6.52E+02	3.03E-01	6.62E+02	3.16E-01	5.91%	65.86%	7.49%	72.70%	1.49%	4.12%
s9234	36	211	5597	1.94E+03	1.49E+00	1.96E+03	1.50E+00	2.46E+03	1.92E+00	1.34%	1.03%	26.92%	29.11%	25.25%	27.79%
s13207	62	638	7951	6.71E+03	6.64E+00	6.69E+03	6.64E+00	6.86E+03	6.69E+00	-0.31%	0.10%	2.24%	0.87%	2.56%	0.77%
s15850	77	534	9772	6.96E+03	5.57E+00	7.19E+03	5.70E+00	7.24E+03	5.66E+00	3.32%	2.35%	4.02%	1.71%	0.68%	-0.63%
s38417	28	1636	22179	2.05E+04	1.63E+01	2.05E+04	1.63E+01	2.08E+04	1.66E+01	0.11%	0.01%	1.41%	1.41%	1.30%	1.40%
s38584	38	1426	19253	1.87E+04	1.62E+01	1.87E+04	1.62E+01	1.89E+04	1.63E+01	0.33%	0.48%	1.24%	0.99%	0.90%	0.51%
Average	-	-	-	-	-	-	-	-	-	**9.26%**	**22.71%**	**14.35%**	**22.02%**	**4.57%**	**0.12%**

the register missing the arrival time window and effectively transitioning from the obfuscated to functional mode. The effect on the clock input due to the aggressor is shown in Fig. 8. The delay in the transition time of the aggressor-coupled clock signal is approximately 40.55 ps longer than the clock signal with no coupling.

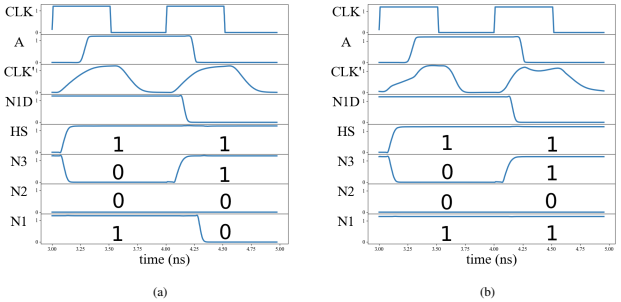


Fig. 7: Schematic simulation of s27 to characterize the clock CLK, AGG_NET A, coupled clock CLK', data input for glitched N1 register N1D, and state register outputs (HS, N3, N2, N1) for (a) no coupling with aggressor and (b) coupling with aggressor.

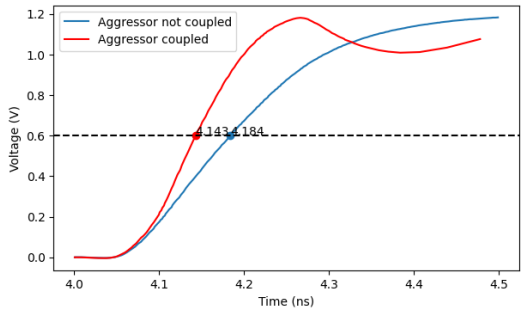


Fig. 8: Delay of an aggressor coupled clock signal and a clock signal not coupled with an aggressor.

V. Characterization of Circuit Overhead

The algorithm described in Section IV-A is applied to a set of ISCAS'89 benchmark circuits as listed in Table I. A target operating frequency of 1 GHz is selected and both the original and obfuscated logical designs are synthesized in a 65nm TSMC technology using Synopsys DC compiler. Key-based HST triggers are added to the obfuscated circuits. Separate coupling capacitance triggered circuits are also generated by importing the obfuscated circuits into Cadence Virtuoso and adding the coupling capacitance model shown in Fig. 5 with an interconnect coupling length of 100 µm and interconnect spacing of 25 nm.

The overheads in area and power due to the implementation of the obfuscation techniques are provided in Table I. Implementing coupling capacitance-based HST obfuscation results in an average overhead in area of 14.35% and in power of 22.02% as compared to the original unobfuscated circuits. The overhead in area and power is slightly greater than key gating based obfuscation, with average increases of 4.57% and 0.12% observed, respectively. Obfuscating larger circuits results in less overhead in area and power as compared to the obfuscation of smaller circuits. Locking the four largest circuits with coupling capacitance based obfuscation results in an average overhead of 2.23% in area and of 1.25% in power as compared to the unobfuscated versions of the circuits.

VI. Conclusion

In this paper, a random walk analysis is performed on ISCAS'89 sequential benchmark circuits to characterize the security of the obfuscated IC due to the logic level masking of the HST glitching topology. An 8.53x increase in the random walk score α and an increase of 887x in the geometric mean of the expected number paths for key extraction is observed as compared to non-hidden HST triggers (i.e. location of trigger is observable in the netlist). Synthesis of capacitive coupling-based HSTs is proposed to mask the glitching mechanism in the gate-level netlist and secure IP against oracle-guided and structural attacks. A closed-form capacitive crosstalk model is used to analyze the hidden state transitions through SPICE simulation. The developed synthesis algorithm is implemented on ISCAS'89 sequential benchmark circuits, resulting in secure netlists with an average overhead of 14.35% in area and 22.02% in power for all circuits and 2.23% in area and 1.25% in power for the four largest circuits.

REFERENCES

[1] J. Roy, F. Koushanfar, and I. Markov, "EPIC: Ending Piracy of Integrated Circuits," *Proceedings of the IEEE/ACM Design, Automation and Test in Europe Conference*, pp. 1069–1074, October 2008.

[2] P. Subramanyan, S. Ray, and S. Malik, "Evaluating the Security of Logic Encryption Algorithms," *Proceedings of the IEEE International Symposium on Hardware Oriented Security and Trust*, pp. 137–143, May 2015.

[3] S. Chakraborty and S. Bhunia, "HARPOON: An Obfuscation-based SoC Design Methodology for Hardware Protection," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, Vol. 28, No. 10, pp. 1493–1502, October 2009.

[4] T. Meade, Z. Zhao, S. Zhang, D. Pan, and Y. Jin, "Revisit Sequential Logic Obfuscation: Attacks and Defenses," *Proceedings of the IEEE International Conference on Circuits and Systems*, pp. 1367–1370, May 2017.

[5] K. Juretus and I. Savidis, "Synthesis of Hidden State Transitions for Sequential Logic Locking," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, Vol. 40, No. 1, pp. 11–23, January 2021.

[6] K. Juretus and I. Savidis, "Time Domain Sequential Locking for Increased Security," *Proceedings of the IEEE International Symposium on Circuits and Systems*, pp. 1–5, May 2018.

[7] K. Juretus and I. Savidis, "Enhanced Circuit Security Through Hidden State Transitions," *Proceedings of the Government Microcircuit Applications & Critical Technology Conference*, pp. 1–4, March 2018.

[8] A. Vittal, L. H. Chen, M. Marek-Sadowska, K.-P. Wang, and S. Yang, "Crosstalk in VLSI Interconnections," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, Vol. 18, No. 12, pp. 1817–1824, January 1999.

[9] A. Devgan, "Efficient Coupled Noise Estimation for On-chip Interconnects," *Proceedings of the IEEE International Conference on Computer Aided Design*, pp. 147–153, November 1997.

[10] S.-C. Wong, G.-Y. Lee, and D.-J. Ma, "Modeling of Interconnect Capacitance, Delay, and Crosstalk in VLSI," *IEEE Transactions on Semiconductor Manufacturing*, Vol. 13, No. 1, pp. 108–111, February 2000.

[11] I. H.-R. Jiang, S.-R. Pan, Y.-W. Chang, and J.-Y. Jou, "Reliable Crosstalk-driven Interconnect Optimization," *ACM Transactions on Design Automation of Electronic Systems*, Vol. 11, No. 1, pp. 88–103, January 2006.

[12] G.S Jovanović. and M. K. Stojčev, "Current Starved Delay Element with Symmetric Load," *International Journal of Electronics*, Vol. 93, No. 3, pp. 167–175, March 2006.