Guaranteed Activation of Capacitive Trojan Triggers During Post Production Test via Supply Pulsing

Bora Bilgic
School of Electrical, Computer and Energy Engineering
Arizona State University
Tempe, USA
bbilgic@asu.edu

Sule Ozev
School of Electrical, Computer and Energy Engineering
Arizona State University
Tempe, USA
sule.ozev@asu.edu

***Abstract*—Involvement of many parties in the production of integrated circuits (ICs) makes the process more vulnerable to tampering. Consequently, IC security has become an important challenge to tackle. One of the threat models in hardware security domain is the insertion of unwanted and malicious hardware components, known as Hardware Trojans (HTs). A malicious attacker can insert a small modification into the functional circuit that can cause havoc in the field. To make the Trojan circuit stealthy, trigger circuits are typically used. The purpose of the trigger circuit is to hide the Trojan activity during post-production testing, and to randomize activation conditions, thereby making it very difficult to diagnose even after failures. Trigger mechanisms for Trojans typically delay and randomize the outcome based on a subset of internal digital signals. While there are many different ways of implementing the trigger mechanisms, charge based mechanisms have gained popularity due to their small size. In this paper, we propose a scheme to ensure that the trigger mechanisms are activated during production testing even if the conditions specified by the malicious attacker are not met. By disabling the mechanism that makes the Trojan stealthy, any of the parametric techniques can be used to detect Trojans at production time. The proposed technique relies on supply pulsing, where an increased potential difference between the gate and bulk of the active transistor in the output stage generates an alternate charge path for an otherwise unreachable capacitor and bypasses the input conditions to the trigger mechanism. SPICE simulations show that our method works well even for the smallest Trojan trigger mechanisms.**

***Index Terms*—analog, charge, domain, Trojan, capacitor, security, detection**

I. Introduction

Fabrication of semiconductor devices has been divided into a chain of services and processes supplied by many actors in order to minimize costs and meet stringent time-to-market constraints. This multi-player production structure has brought about new challenges and vulnerabilities for the semiconductor industry. In addition to defects and unintended process fluctuations, the IC vendors must now contend with the possibility of design modifications, malicious hardware and microcode insertions, and even intentional process modifications that result in various payloads, including information leakage and catastrophic or parametric failures [1].

Unlike a software Trojan, a HT cannot be removed after detection and can cause undesirable outcomes such as loss of life (in medical or automotive applications), failure of a critical mission (in military, governmental or space applications), or loss of reputation for the IC vendor, if tainted ICs are deployed. Therefore, reliability and security have become major figures of merit for modern ICs, especially in the zero-trust multi-player manufacturing environment.

The goal of the malicious attacker is to make the HT as stealthy as possible (e.g. by limiting size and impact) during testing. One way of achieving this stealthiness while not compromising on the effect of the payload is to provide a trigger mechanism that activates the HT in the field. Malicious attackers design HTs such that they are activated under specific rare conditions which makes them nearly impossible to detect using random or functional input patterns during post production testing. Attackers also try to make HTs as small as possible to keep changes to IC's dynamic profile (current consumption, heat dissipation etc.) to a minimum to evade detection during post production testing.

A typical HT structure is shown in Figure 1. The HT activation condition can be a certain combination of internal logic states, a specific input pattern, an internal counter value, or a particular value of a sensor that monitors environmental conditions [1]. To increase stealthiness, trigger mechanisms can be designed in a multi-stage scheme, where a series of such conditions have to be met to activate the Trojan.

Recent studies showed that analog design methods can create

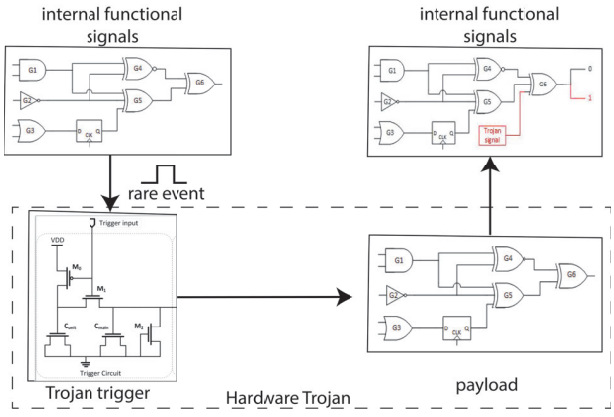

Fig. 1. Typical HT Structure

This work is supported by the National Science Foundation with Grant Number CCF-1617562.

smaller HT trigger mechanisms with a few circuit components which can evade detection techniques better than digital counterparts [2]–[4]. Capacitive analog HT triggers utilize switched capacitor design techniques to set the activation condition. They can be tied to any internal signal or a combination of them. Being small in size, they can be designed in a multi-stage manner to increase stealthiness.

The goal of this paper is to present a new and simple technique to activate such capacitive HT triggers during post production testing such that the HT (if it exists) can be detected with functional or parametric testing.

II. Prior Work

Generating and defending against HTs has been the focus of intense research over the past two decades. Most of the research activity has focused on digital implementation and detection techniques of gate-level HTs that can paralyze the IC or leak information to an unauthorized party. Many techniques have been developed to counter these threats and detect HTs either during post-production test or in the field. Side-channel analysis [5]–[8], reverse engineering techniques [9] [10], and devising dedicated test patterns [11]–[14] are successfully implemented for detection of HTs.

Recently, capacitive Trojans have also been developed as low-impact alternatives to digital HT [2]. Although capacitive Trojans pose an important threat to the reliability and security of the ICs, there are limited studies in the literature regarding the detection methods. In [15], an additional circuit guards a set of vulnerable signals and raises an interrupt when abnormal toggling events are detected on these signals. The limitations of this technique are the inability to guard all the signals and the area and power overhead it presents.

The method proposed in [4] utilizes information flow tracking (IFT) to model capacitor Trojans and detect charge domain leakage paths in a design based on these models. It recognizes the capacitors that are larger than a threshold as potential Trojans because charge sharing Trojans have large capacitances to trigger an event after a number of toggling events. This technique detects specific patterns of capacitive triggers and may fail to detect trigger structures such as the one presented in [3].

Reverse engineering techniques [9] that map a layout back to a schematic and match the functionality of the schematic to the intended design can be used to detect HTs. However, small capacitive HT triggers that use transistors that are *always off* may evade this kind of automated detection.

III. Background: Capacitive Trojan Triggers

To evade detection, HT designers have come up with various methods for delayed activation, which would leave the HT dormant until a series of pre-defined or random events are observed. Capacitor based HT trigger mechanisms have attracted attention due to their low area, power, and delay footprint characteristics [3].

A2 [2] is a typical implementation of a capacitive HT trigger mechanism. The circuit has the capability to trigger a payload with a short duration pulse train at its trigger input. Since it is built with a small number of components, it can be stealthily integrated into an IC.

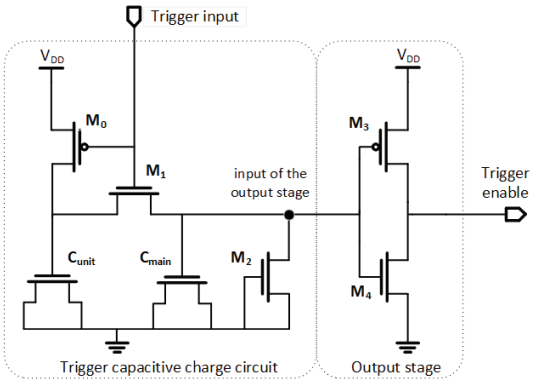

Fig. 2. Capacitive HT Trigger Circuit

The simple circuit of A2 capacitive HT trigger mechanism is depicted in Figure 2. In this embodiment of the implementation, the trigger input is connected to internal functional signals. When the trigger input is low, transistor M_0 is on and C_{unit} is charged to V_{DD}. If the trigger input goes to high due to a change in the functional signals, transistor M_1 turns on and C_{unit} begins to charge C_{main}, increasing the voltage on C_{main}. Eventually, C_{main} charges to a voltage level high enough to cause a transition at the output stage, which activates the HT and delivers the payload designed by the attacking party. Transistor M_2 is added to the circuit to provide a slow discharge path C_{main}. Without the presence of M_2, the trigger may get activated due to crosstalk and leakage. In Figure 2, an inverter is used as the output stage. Alternatively, a Schmitt Trigger can be used. To evade detection during post production testing, the trigger mechanisms can be connected to internal signals with low activity levels or user controllable signals.

The ratio between the two capacitors, C_{main} and C_{unit}, determines how many pulses will result in the activation. Assuming C_{unit} is kept at minimum, increasing C_{main} size would lead to lower probability of activation and thus better detection evasion during post-production test. However, it would lead to higher area and make the HT more visible during layout inspection. The main charge transfer unit can be replicated. Increasing the number of such stages also increases stealthiness during post production test at the expense of larger area. Similarly, the functional inputs can be gated with one another to reduce the probability of activation at the expense of larger area. Thus, there is always a trade-off between lowering activation probability during post-production test and keeping the trigger circuit small to evade visual layout inspection.

IV. Activation of Capacitive HT Triggers via Supply Voltage Pulsing

In the previous section, we discussed various methods of charging an otherwise unreachable capacitor through rarely activated digital signal combinations. While the attacker cannot guarantee that the HT trigger is not activated during production test, they can make this extremely unlikely by using multiple

stages and adjusting capacitances used in the trigger circuit. Many existing flavors of capacitive HT triggers share the same concept, namely a final digital output stage that changes its state when adequate charge is accumulated on its floating input.

Our goal is to ensure that the HT trigger is activated during production test so that its presence can be revealed through functional or parametric testing. In order to do so, we concentrate on the output stage of capacitive trigger mechanisms. We observe that the main charge path for the trigger capacitor is through the previous stages. However, there exists another charge path through the PMOS transistor of the output stage (inverter). The voltage difference between the source and the gate of this transistor can be temporarily altered by increasing the supply voltage to cause a significant increase in the tunneling current. Once the trigger capacitor is charged, the supply voltage can be normalized again. Since the trigger capacitor is a dynamic component (not connected to a discharge path), it will retain its charge for some duration to allow for testing. We propose to generate this voltage differential by pulsing the supply voltage temporarily above its nominal rate. Clearly, this would change the behavior of the circuits and make parametric testing very difficult. However, this temporary jolt will help charge the trigger capacitor, which will remain charged even after the supply level is brought down to normal levels since it is in isolation unless the necessary input combinations are met (at which point, the Trojan is triggered anyway so we do not focus on this unlikely event). We can utilize this time where the trigger signal remains active at the nominal supply level to conduct functional or parametric testing. The number of necessary triggers for a specific circuit can be determined by the number of test patterns, worst case Trojan activation duration (at smallest C_{main} value), and the test frequency for the given circuit and process.

The supply pulsing technique is non-destructive as long as the supply voltage is kept below the hard breakdown levels for the transistors. Furthermore, it should be noted that all the testing is conducted after the supply voltage is brought back to its functional value. Thus, normal test conditions and parameters can be used to detect any malfunction caused by the temporarily triggered HT. Finally, since HTs will be present in all manufactured circuits, it is only necessary to do this kind of testing on a randomly sampled subset of manufactured circuits to certify the design as HT-free.

A. Creating Temporary Alternate Charge Paths

One alternate charge path generated during the supply pulse is the tunneling current between the gate and the bulk/source of the PMOS device of the output stage. With technology scaling, the thickness of the gate oxide has decreased to levels where the tunneling current may be an issue, particularly if the stress on the oxide is high. For technology nodes beyond 0.18μm, the assumption of zero gate current becomes invalid because of quantum mechanical effects [16]. If sufficient potential different between the gate and the channel exists, electrons can tunnel from channel to gate which can result in a significant gate current [16]. Gate leakage currents are exponentially dependent on gate oxide potential [17]. For the case of an inverter, this

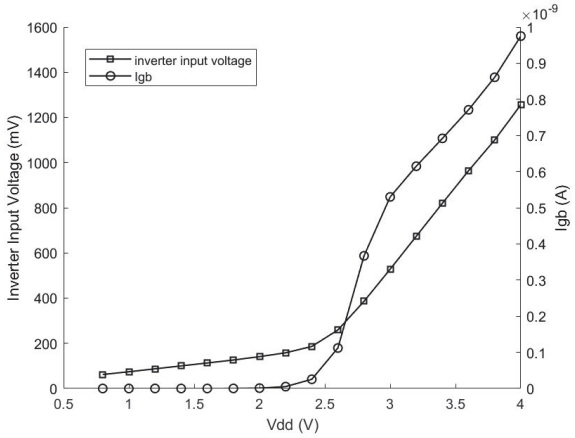

Fig. 3. V_{DD} vs. gate-to-bulk current and input voltage of the output stage

dependency is depicted in Figure 3. While this gate current may be present in all transistors experiencing the same increased voltage stress, the special structure of the trigger mechanism results in accumulation of charge on the capacitor, C_{main}, increasing the input voltage of the output stage.

At higher gate-source voltages, the gate-to-bulk leakage current (I_{gb}) dominates other gate leakage currents [18] and rises to significant levels. An example SPICE simulation using 65nm CMOS technology is shown in Figure 4. While negligible at nominal V_{DD} levels, the current increases exponentially with increasing V_{DD}, reaching to nA levels at high stress. Considering that capacitances are in the order fF, this current can charge the capacitance to the switching point in tens of microseconds.

A secondary charging mechanism is established due to charge sharing between the parasitic capacitances of the output stage and C_{main}. When M_1 is off, during the rising edge of V_{DD}, C_{main} charges through $C_{gs,M3}$, $C_{gd,M3}$ and $C_{gd,M4}$ parasitic capacitors. $I_{gb,M3}$ rises with increasing V_{DD} and speeds up charging of C_{main} (Figure 3).

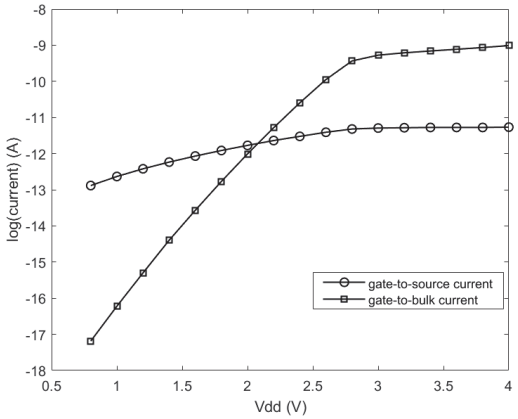

Fig. 4. Gate-to-bulk vs. gate-to-source current

After the supply voltage settles, the charging current, $I_{gb,M3}$, begins to fall due to rising gate voltage, $V_{G,M3}$, and it stabilizes at a stable level. The same process takes place for the Schmitt Trigger output stage. Note that when the supply level is increased, so does the switching point of the output stage. Hence, it is not possible to enable the HT trigger output just by increasing the supply level. The charge at the input of the output stage needs to be retained for some time after the supply level is brought back to its nominal value. This is possible due to the special architecture of the capacitive HT trigger wherein the node in question is nominally floating.

B. Retention of the Trigger Output After Restoration of the Supply Voltage to its Normal Level

Functional, structural, or parametric testing needs to be conducted at the nominal supply level. Hence, it is important for the trigger enable to be active for some time after the supply is brought back to the nominal level. At the nominal supply level, M_3 is in the triode region and M_4 is in the cut-off region. Input voltage of the output stage rises with increasing V_{DD} and M_4 goes into saturation. However, the output of the output stage remains high during the supply pulse. Thus, increased voltage at the input of the output stage does not necessarily enable the trigger output during this period. However, during the falling edge of the V_{DD} pulse, the input voltage of the output stage does not fall simultaneously with V_{DD} since the discharge paths for C_{main} are based on subthreshold leakage of M_2, which is designed to provide a certain amount of retention period.

At some point after the supply voltage returns to its nominal value, M_3 goes into saturation while the input voltage of the output stage remains high enough to trigger a temporary high-to-low transition at the output.

The input voltage of the output stage continues to fall due to leakage through M_2. Once the switching point of the output stage is reached, the output trigger will once again be disabled. Thus, after the supply voltage returns to its nominal level, the trigger is enabled for a duration of time, during which testing can be conducted.

Figure 5 shows an illustration of these sequence of events on a timing diagram. During supply pulsing, the main goal is to enable the charging of the capacitor C_{main} through the two aforementioned mechanisms. After supply pulsing, the switching point of the inverter falls back to the same nominal value. However, it takes some time for C_{main} to discharge through the subthreshold leakage of M_2. During this time, the input of the output stage remains above the switching point of the inverter and the trigger remains enabled. The charge on C_{main} eventually dissipates to a point where the trigger is disabled again. Testing duration is while the trigger is enabled.

Note that the behavior of the output stage due to supply pulsing is independent of the trigger input. It is also independent of how many cascaded stages may have been included the trigger circuit. Finally, the process is nearly identical for a Schmitt Trigger output stage with different switching points for H-L and L-H transition of the output stage. Thus, even for very stealthy triggers with many cascaded stages, this mechanism will inject charge into the output stage in the same manner, triggering them in an identical fashion regardless of these implementation choices by the attacker.

C. Pulse and Trigger Enable Duration

Some of the design decisions that affect the Trojan and trigger response by the attacker also influence how long a pulse duration is necessary to charge C_{main} and how long the retention duration will be. If C_{main} is chosen to be large, it will take longer (or a higher supply pulse amount) to charge it to the necessary levels to switch the output stage. This is a disadvantage for the purposes of activating the trigger. The retention duration also increases with increasing C_{main}, which will be advantageous for detection purposes. The pulse amplitude and duration as well as the retention duration (i.e. test duration) should be set to account for worst-case conditions. For instance, to set the pulse duration and magnitude, we should assume that the attacker uses a very large C_{main}, where the size is limited by the desire to evade visual layout inspection. To set the duration of testing after the trigger is activated, we should assume that the attacker has chosen a small C_{main} value (comparable to C_{unit}) and limit the test duration to the retention duration under this condition. If more testing is necessary, supply pulsing can be repeated.

V. Results and Analysis

In order to demonstrate how the supply pulsing technique works and present different design decisions, we implemented an A2 capacitive trigger with AND gate payload in 65nm CMOS technology. Note that the payload is not relevant to the discussion herein. Thus, the simplest payload is selected for demonstration purposes. The V_{DD} pulse level is limited well below the oxide breakdown voltage of the transistors to avoid any permanent harm to the circuit. To reiterate from earlier discussion, since HTs, if they exist, will be present in all manufactured devices, the security testing process can be conducted on a subset of manufactured devices. Hence, any long term reliability concern is also not relevant as these parts do not need to be shipped to the customers.

Capacitive HT trigger should be designed for a specific minimum operating frequency and work for all process, temperature, and voltage (PVT) variations. For the intended operation of the HT trigger, Table I shows the number of required input trigger pulses to enable the trigger output. Higher C_{main} values would require a higher number of trigger input pulses, making

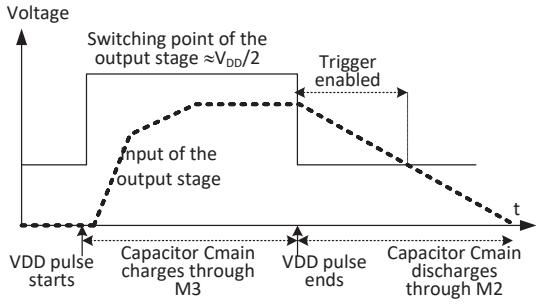

Fig. 5. Illustration of sequence of events during and after supply pulsing

TABLE I
C_{MAIN} SIZE VS. NUMBER OF REQUIRED TRIGGER PULSES TO TRANSITION THE OUTPUT

Number of C_{main} fingers	Number of trigger pulses required to transition the output
1	2
10	3
20	5
50	9
100	16

the activation of the trigger less likely during production test. Our goal is to decouple mechanism for trigger enable from the trigger input. As noted earlier, the number of cascaded stages is irrelevant for the activation as well as the trigger retention duration. Hence, in this section, we will analyze the effect of the size of C_{main} on Trojan activation and retention duration.

We designed two capacitor triggers with different C_{main} values. Design 1 utilizes a single finger transistor for C_{main}. Design 1 represents the best case scenario for trigger activation and worst case scenario for trigger retention. The discharge time of C_{main} is proportional to its capacitance according to the equation: $I = C\frac{\Delta V}{\Delta t}$. Since the discharge current is primarily determined by the subthreshold leakage of M_2, smaller C_{main} will result in shorter trigger retention.

Figure 6 shows the simulation results for supply pulsing, specifically the input and the output voltages of the output stage. In this simulation, V_{DD} is increased from 1.2V to 5V for 0.5μs. This cases the input voltage of the output stage ($V_{in,inverter}$) to rise to 2.06V. When V_{DD} is lowered back to 1.2V, $V_{in,inverter}$ remains high enough to trigger a transition at the trigger enable output due to the stored charge on C_{main}. The duration of the trigger enable is around 140ns. To put this into perspective, this duration corresponds to about 140 cycles for a 1GHz clock.

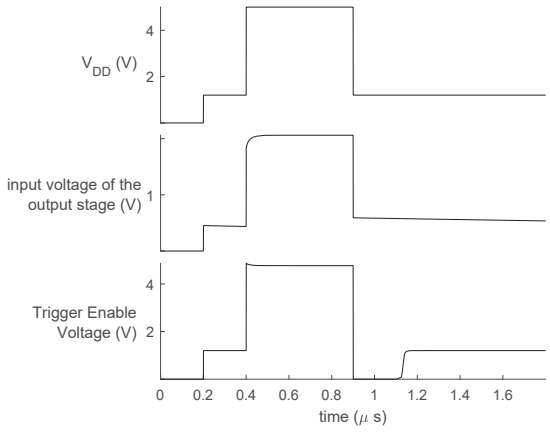

Fig. 6. HT trigger response to V_{DD} pulse (1 finger)

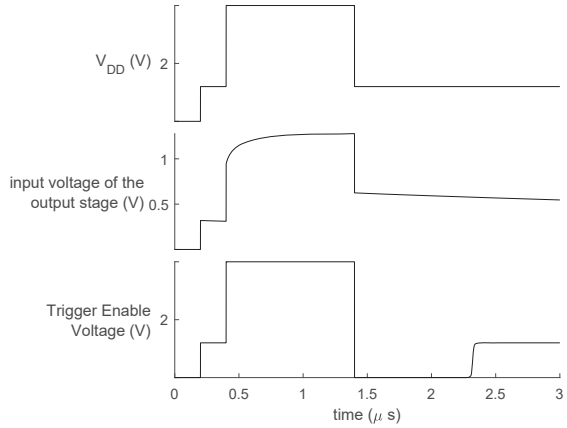

Fig. 7. HT trigger response to V_{DD} pulse (5 finger)

Design 2 has considerably larger C_{main} with a transistor size of 5 fingers. Figure 7 shows the response of this trigger to V_{DD} pulse. V_{DD} is increased from 1.2V to 4V for 1μs and the input voltage of the output stage ($V_{in,inverter}$) rises to 1.28V. In this case, the trigger retention duration is 860ns, which corresponds to 860 cycles of a 1GHz clock.

For bigger C_{main}, the level of V_{DD} pulse can be lowered because with bigger capacitance at the input $V_{in,inverter}$ decays more gradually during after V_{DD} is returned to its nominal level. The trigger enable retention time increases with increasing ΔV_{DD}. Table II shows simulated retention times for different ΔV_{DD} values.

Our activation method works for Schmitt Trigger output stage as well. Since low to high transition of Schmitt Trigger requires a higher input voltage than the inverter, higher ΔV_{DD} is needed to trigger a transition. Retention time is longer for Schmitt Trigger because low to high transition input level is lower than the inverter. Response of the trigger circuit with 5 finger C_{main} and Schmitt Trigger output stage is shown in Figure 8. Applied ΔV_{DD} is 4V and measured retention time is 4.5μs. If we switch the number of fingers of C_{main} to 1, the required ΔV_{DD} rises to 8V (still under gate oxide breakdown voltage) and retention time drops to 1.8μs.

To increase stealthiness of the Trojan, multi-input trigger

TABLE II
ΔV_{DD} VS. RETENTION TIME

1 finger C_{main}		5 finger C_{main}	
ΔV_{DD} (V)	Retention time	ΔV_{DD} (V)	Retention time
3.8	140ns	2.7	60ns
3.9	260ns	2.8	860ns
4	760ns	2.9	1.56μs
4.1	1.03μs	3	2.15μs
4.2	1.28μs	3.1	2.66μs
4.3	1.5μs	3.2	3.1μs

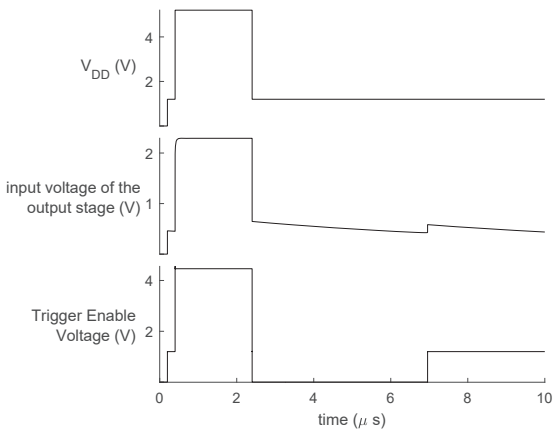

Fig. 8. HT trigger response to V_{DD} pulse (Schmitt Trigger, 5 finger C_{main})

mechanisms have been proposed in different researches. [2] mentions gated Trojan trigger mechanisms, an example of which is shown in Figure 9(a). Simulations for this OR-ed two input trigger mechanism also show similar results where the HT trigger enable is activated for a duration that is determined by the two inputs. Since our method activates the final stage, it is capable of triggering the Trojan enable output regardless of these implementation choices. As another example, in [3] a cascaded capacitor multi-stage trigger mechanism, shown in Figure 9(b) has been proposed. The last stage of the cascaded trigger circuit is similar to a single stage implementation. Thus, as noted earlier, our detection scheme works well for this architecture as well.

SPICE simulations show that our detection scheme works well within the acceptable supply voltage levels even against the smallest size capacitor Trojan trigger mechanisms. The proposed method does not require any complicated test equipment. The triggered output transitions have longer enough duration to be captured with reasonable clock frequencies.

VI. Conclusion

Attackers go to great lengths to shield the HT circuits from detection during production testing. In most cases, HTs utilize a trigger mechanism that makes them dormant until a series of events are observed. These events may not be triggered during production testing, making the detection of the HT extremely unlikely. In this paper, we propose a technique for guaranteed triggering of HTs that rely on capacitive trigger mechanisms. The proposed technique relies on supply pulsing, which generates two mechanisms to charge an otherwise unreachable capacitor, which triggers the enable output. We demonstrate, with SPICE simulations, that our supply voltage pulsing based activation scheme proves to activate capacitor Trojan triggers and their variants presented in [2] and [3]. The proposed technique works with different design decisions an attacker may make.

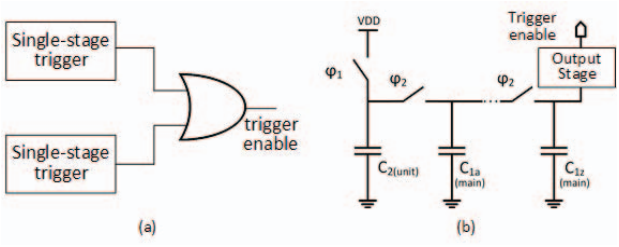

Fig. 9. Multi stage trigger mechanism combining multiple trigger units: (a) parallel replicated OR-ed trigger (b) series replicated charge unit based trigger

References

[1] M. Tehranipoor and F. Koushanfar, "A survey of hardware trojan taxonomy and detection," in *IEEE design & test of computers*, 2010, pp. 10–25.

[2] K. Yang, M. Hicks, Q. Dong, T. Austin, and D. Sylvester, "A2: Analog malicious hardware," in *IEEE symposium on security and privacy (SP)*, 2016, pp. 18–37.

[3] M. M. Bidmeshki, K. S. Subramani, and Y. Makris, "Revisiting capacitor-based trojan design," in *IEEE 37th International Conference on Computer Design (ICCD)*, 2019, pp. 309–312.

[4] X. Guo, H. Zhu, Y. Jin, and X. Zhang, "When capacitors attack: Formal method driven design and detection of charge-domain trojans," in *IEEE Design, Automation & Test in Europe Conference & Exhibition (DATE)*, 2019, pp. 1727–1732.

[5] D. Agrawal, S. Baktir, D. Karakoyunlu, P. Rohatgi, and B. Sunar, "Trojan detection using IC fingerprinting," in *IEEE Symposium on Security and Privacy (SP'07)*, 2007, pp. 296–310.

[6] F. S. I. Wilcox and J. Plusquellic, "GDS-II trojan detection using multiple supply pad vdd and gnd iddqs in asic functional units," in *IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, 2015, pp. 144–150.

[7] F. Karabacak, U. Y. Ogras, and S. Ozev, "Detection of malicious hardware components in mobile platforms," in *IEEE 17th International Symposium on Quality Electronic Design (ISQED)*, 2016, pp. 179–184.

[8] S. Narasimhan, X. Wang, D. Du, R. S. Chakraborty, and S. Bhunia, "TeSR: A robust temporal self-referencing approach for hardware trojan detection," in *IEEE International Symposium on Hardware-Oriented Security and Trust*, 2011, pp. 71–74.

[9] R. Torrance and D. James, "The state-of-the-art in IC reverse engineering," in *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 2009, pp. 363–381.

[10] F. Courbon, P. Loubet-Moundi, J. J. Fournier, and A. Tria, "A high efficiency hardware trojan detection technique based on fast SEM imaging," in *IEEE Design, Automation & Test in Europe Conference & Exhibition (DATE)*, 2015, pp. 788–793.

[11] X. Mingfu, H. Aiqun, and L. Guyue, "Detecting hardware trojan through heuristic partition and activity driven test pattern generation," in *ACM Communications Security Conference*, 2014, p. 3.

[12] H. Salmani, M. Tehranipoor, and J. Plusquellic, "A novel technique for improving hardware trojan detection and reducing trojan activation time," in *IEEE transactions on very large scale integration (VLSI) systems*, 2012, pp. 112–125.

[13] M. Banga and M. S. Hsiao, "A novel sustained vector technique for the detection of hardware trojans," in *IEEE 22nd International Conference on VLSI Design*, 2009, pp. 327–332.

[14] F. Karabacak, R. Welker, M. J. Casto, J. N. Kitchen, and S. Ozev, "RF circuit authentication for detection of process trojans," in *2018 IEEE 36th VLSI Test Symposium (VTS)*. IEEE, 2018, pp. 1–6.

[15] Y. Hou, H. He, K. Shamsi, Y. Jin, D. Wu, and H. Wu, "R2D2: Runtime reassurance and detection of A2 trojan," in *IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, 2018, pp. 195–200.

[16] C. M. Yannis Tsividis, *Operation and Modeling of the MOS Transistor*. New York: Oxford University Press, 2011.

[17] T. H. M. et.al., *BSIM (Berkeley Short-channel IGFET Model) Technical Manual*. Berkeley: University of California, Berkeley, 2009.

[18] H. J. M. T. E. Mitiko Miura-Mattausch, *The Physics and Modeling of MOSFETS Surface-Potential Model HiSIM*. Singapore: World Scientific, 2008.