Reliability Based Hardware Trojan Design Using Physics-Based Electromigration Models

Chase Cook, Sheriff Sadiqbatcha, Zeyu Sun, and Sheldon X.-D. Tan
Department of Electrical and Computer Engineering, University of California, Riverside, CA 92521, USA

***Abstract*—In recent years the concern over Hardware Trojans has come to the forefront of hardware security research as these types of attacks pose a real and dangerous threat to both commercial and mission-critical systems. One interesting threat model utilizes semiconductor physics, specifically aging effects such as Electromigration (EM). However, existing methods for EM-based Trojans based on empirical Black's models can easily lead to performance degradation and less accuracy in Trojan activation time prediction. In this paper, we study the EM-based Trojan attacks based on recently developed physics-based EM models. We propose novel EM attack techniques in which the EM-induced hydrostatic stress increase in a wire is caused by wire structure or layer changes without changing the current density of the wires. The proposed techniques consist of sink/reservoir insertion or sizing and layer switching techniques based on the early and late failure modes of EM wear-out effects. As a result, the proposed techniques can have minimal impact on circuit performance, which is in contrast with existing current-density-based EM attacks. The proposed techniques can serve as both a trigger or payload for the EM attack on power/ground networks and signal and clock networks.**

I. INTRODUCTION

The trend of ”fabless” semiconductor companies, that outsource fabrication to third party companies who provide foundry services, has globalized the industry [1]. This presents a problem, particularly for military and aerospace systems integrators who see it as a vulnerability to the integrity of their systems. By resorting to third party foundry services, a company loses control of the fabrication and therefore, cannot guarantee that the fabricated IC conforms to the original design specifications. It presents an opportunity for an attacker, at the foundry, to maliciously alter the original design or insert additional logic or modules into the IC at fabrication time. These alterations are referred to as “Hardware Trojans” and pose a significant security threat to critical applications.

A unique method of attack harnesses semiconductor aging effects, so-called reliability-based Trojans, to modify the operation of the circuit or accelerate device failure [2–4]. However, existing methods mainly exploit the front-end device reliability such as Negative Bias Temperature Instability and Hot Carrier Injection.

Reliability-based Trojans give an attacker a large advantage in terms of detectability. One of the primary methods of detecting hardware Trojans is to use functional testing in conjunction with side-channel analysis (the measurement of chip parameters such as temperature and power) [1, 5]. These methods attempt to trigger hardware Trojans to induce anomalies in the chip's functionality or the side-channels. However, reliability-based Trojans can be designed in such a way that activation is only achievable through chip aging. This means that there would be no functional test vectors that can activate these Trojans making them particularly difficult to detect without using destructive methods.

There are a few previous works that use back-end-of-line reliability (BEOL), for an attack [2, 3]. In these works, attacks are proposed for both electromigration (EM) and Time-Dependent-Dielectric-Breakdown, but they rely on current density based methods for EM analysis and Trojan design. However, simply changing the wire width to increase current density (thus reduce EM lifetime of the wire) does not work very well as those wires will affect the IR drops and RC delays, which degrades performance of the chips right away. Furthermore, for an EM-based attack, those methods still use traditional Black's equation [6], which ignore topology and copper via structural impacts [7], which are key to the proposed EM attacks in this work.

In this paper, we use a recently proposed physics-based EM model to leverage the impact of multi-segment wire topology and structure on EM wear-out for EM-based attacks. We first briefly present the basics of EM physics and the physics-based EM models, then review some of the challenges for designing a robust EM-based Trojan. Then we propose novel EM attack techniques based on stress condition increases from changes of the multi-segment wire structures without changing the current density of the wires. We propose the insertion or modification of atomic sinks and reservoirs in addition to metal layer switching to leverage multi-mode failure mechanics on the EM wear-out effect. Unlike previously proposed EM attacks, these methods, based on wire topology, avoid affecting the current density in target wires which gives them minimal impact on circuit performance. Furthermore, the proposed methods are applicable to power, clock, and signal nets.

II. ELECTROMIGRATION BASICS

Electromigration is a physical effect in metal wires that, effectively, causes a wire's structure to physically change. This change is due to the migration of metal atoms induced by momentum transfer from conducting electrons [6, 8]. The momentum transfer generates a hydrostatic stress within an embedded metal wire which, under normal circumstances, remains in an equilibrium state, with tensile stress in the cathode and compressive stress in the anode, preserving the metal atom lattice structure. However, if the momentum transfer from the conducting electrons is sufficient enough, stress can reach a critical level and cause atom diffusion and the subsequent formation of voids or hillocks within the wire as depicted in Fig. 1. This void formation then causes parametric failure, or critical failure, of the wire.

EM is typically modeled using two competing methods. The first, and most common for reliability sign-off, is Black's equation [6] which is a semi-physical empirical method relying on test data to fit parameters. This method can be difficult

This work is supported in part by NSF grant under No. CCF-1527324, and in part by UC-Mexus grant under CN 16-161.

978–1–5386–5153-7/18/$31.00 © 2018 IEEE

Authorized licensed use limited to: Univ of Calif Riverside. Downloaded on June 24,2026 at 22:34:18 UTC from IEEE Xplore. Restrictions apply.

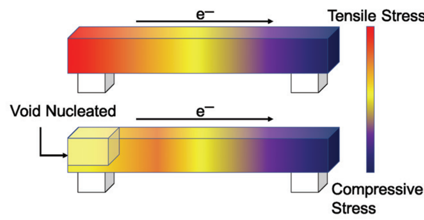


Fig. 1. EM failure process showing a metal wire being stressed by electron wind and subsequent void formation

to use for accurate Time to Failure (TTF) assessment due to its inability to handle wide ranges of current densities, multi-segment wire structures, and other stressing conditions that make fitting of parameters difficult. This method proves to be sufficient for EM sign-off as it gives a reliable conservative lower bound for EM TTF. However, the design of an EM Trojan requires more accurate TTF estimation without the restriction of requiring a conservative estimation. Furthermore, we are unable to leverage more complicated EM effects by using Black's model.

The other method is based on Korhonen's equation [8] which is a physics based method modeling the hydrostatic stress build-up in the metal wires and has shown good agreement with real EM testing [7]. The development of this equation has resulted in the creation of the so-called three phase model, as detailed in [9], which is the model used in this work. This model splits the failure processes into three phases: the Nucleation phase where stress accumulates in the wire, the Incubation phase where a void is formed but does not have an immediate effect on wire performance, and the Growth phase where the void has grown in size sufficient enough to cause parametric failure and will continue to grow until it saturates.

Most importantly, the three phased stress-based model used in this work allows us to consider many of the complex effects in the EM wear-out process. Primarily, it allows us to consider the effect that multi-segment wires and topology has on stress. Because of our ability to model these effects, we can leverage them to make effective and novel EM-based attacks not possible when using Black's method.

III. EM-BASED HARDWARE ATTACK MODELING

Reliability-based attacks are made possible due to the vulnerabilities in the design and manufacturing process of modern IC's as depicted in Fig. 2.

Once the design house sends the final physical design to the third party foundry, masks are created from the design which the lithography tools use to fabricate the chip. An attacker at a foundry could modify these masks, without the design house knowing, and compromise the chip.

The challenge for an attacker creating an EM-based Trojan is to design a wire with structure and configuration such that the wire fails at a desired time and accomplishes some malicious task without compromising the circuit performances and other design constraints prior to activation. In the following sections we outline some challenges to EM-based attack design, attack opportunities based on newly proposed physics-based EM models, and the newly proposed attacks.

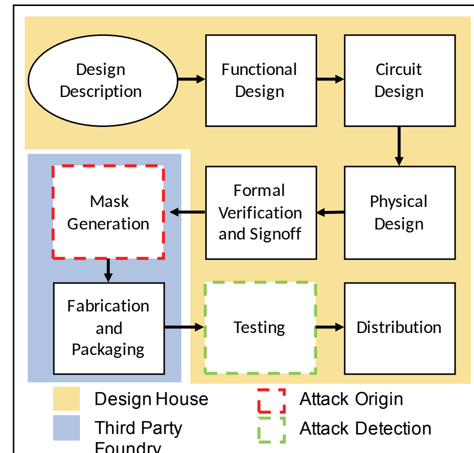


Fig. 2. IC design and manufacturing flow showing attack and detection opportunities

A. Challenges in EM-based attacks

In order for a wire to fail due to EM, it must be stressed by electronic currents. An attacker must increase the EM stress conditions so that the EM-induced lifetime of the wire will be reduced. Furthermore, an EM Trojan must have minimal impact on circuit performance to maintain its stealthiness and effectiveness. For these reasons the stress source in a wire must be considered, as well as the method an attack uses to induce failure.

The wire's stress source, wire current, is a major contributor to its EM vulnerability. Furthermore, it is known that there exists a stress relaxation effect in a wire that becomes unstressed [10]. If the stress source is not considered, a wire may never generate enough stress to result in void nucleation, or the TTF of the wire may be much larger than estimated. When designing an EM attack, there are three primary stress sources: power/ground networks (p/g), clock trees, and signal nets. P/G networks have strong unidirectional currents giving them a good stress profile. Clock trees, while periodic, have high enough frequency ensuring long term averaging currents providing a good stress source. Signal nets that are highly active are good stress sources but other nets, that have little activity, may not produce enough currents to induce EM failure.

Additionally, simple alterations to a wire, such as altering its widths to increase current density, can have unintended consequences on the wire's IR drop. In the case of p/g network wires, this can cause switching speed degradation to front end devices, thus affecting chip timing. This has two major consequences. Firstly, it can render the chip immediately inoperable. Secondly, it can cause enough change in performance that the EM Trojan is detectable through side-channel analysis. For this reason, novel techniques of inducing EM failure without degrading chip performance is required for effective EM attacks.

B. Electromigration topology effects

1) Multi-mode failure: EM induced atom migration results in parametric failure, e.g., causes resistance to change. However, depending on the wire topology, a wire may gradually experience resistance change once a void is nucleated (late

Authorized licensed use limited to: Univ of Calif Riverside. Downloaded on June 24,2026 at 22:34:18 UTC from IEEE Xplore. Restrictions apply.

failure), or the wire may immediately experience drastic resistance change causing an open circuit once a void has grown to a certain size (Early Failure) [11, 12].

Late failure typically occurs in a so-called via-below (or up-stream) structure when electron flow is from a lower layer of metalization to a higher level of metalization. In this case the void will form in the upper portion of the wire which will allow current flow for some time as shown in Fig. 3(a). Even after the void has saturated, current can still flow through the Ta barrier layer, albeit, with much higher resistance. This results in a gradual parametric failure. In contrast, early failure occurs in the via-above (or down-stream) structure, where electron flow is from a higher layer of metalization to a lower level of metalization as shown in Fig. 3(b). In this case, the void will form in the upper part of the wire at the via interface. This void quickly grows to the diameter of the via, blocking current flow. Current cannot continue to flow as the only remaining path is the wire capping layer which is typically a dielectric such as Si_3N_4 and does not shunt the current flow. This causes immediate resistance change and effectively an open circuit.

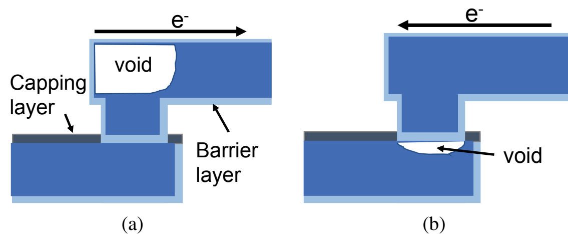


Fig. 3. Via-below (a) and Via-above (b) wire structures showing void formation locations.

2) Multi-segment wires: Electromigration sign-off typically considers only single wire segments individually, however, the stress in neighboring wires can effect each other. Because of this, the Korhonen model has been expanded to handle these multi-segment interconnect trees. Depending on the wire topology and current flow in neighboring segments, the stress can vary drastically in the wire under test.

To illustrate this point, we consider a simple two-segment wire as shown in Fig. 4. We compare the TTF results using equal unidirectional current against equal opposing currents.

Simulation results for these two structures show that the case with opposing currents has a TTF = 7.03 years and the case with a single unidirectional current has a TTF = 4.92 years which is quite a large difference.

Specific multi-segment configurations act as atomic reservoirs or sinks. These configurations have previously been observed to have effects on the TTF of a wire when either passive (having no current) or active (carrying current) [13]. The reservoir is situated at the cathode end of a target wire and when passive, can extend the TTF of a wire. Consequently, reduction or removal of this reservoir can reduce the TTF of a wire. The sink is attached to the anode of a wire. When the sink is passive, the stress is increased in the cathode end of the wire which decreases the TTF of the overall wire.

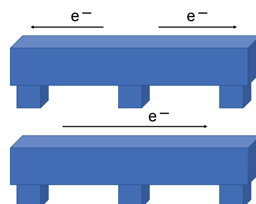


Fig. 4. A two segment wire structure with the same current density (below) and different current densities (above)

IV. EM ATTACK METHODS

With the proper modeling, simulation, and design challenges in mind, we can formulate specific attacks using the EM wear-out effect. Furthermore, we can create attacks that avoid the previously mentioned side-channel effects of the simple EM attack, wire width reduction, by using the wire structure impacts presented in III-B.

A. *EM as a Trojan payload*

As a payload, the EM-based attack results in performance or functionality degradation upon wire failure. This can be accomplished by modifying an existing wire to cause wire failure earlier than anticipated by the designers. An EM payload can be used to cause IR degradation in the p/g network, disrupt the functionality of the clock tree, or even disable highly active signal nets.

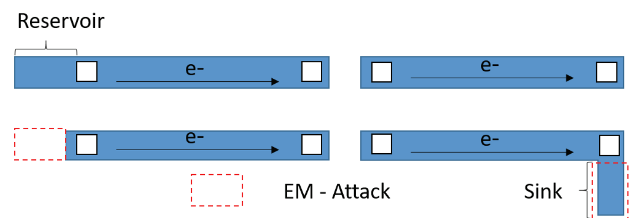


Fig. 5. The reservoir reduction and sink insertion attacks

1) Reservoir reduction p/g network attack: As discussed in III-B2, a passive reservoir structure in a multi-segment wire can help increase the TTF of a wire. In practice, passive reservoirs are a common occurrence in the p/g network. Thus, an effective and stealthy attack would be to reduce or remove the reservoirs from the p/g network of a chip. Because they are passive, their removal will not cause IR degradation.

To demonstrate the reservoir reduction attack, shown in Fig. 5, we design an immortal wire (meaning it will never fail due to EM) with a passive reservoir. The wire is $0.14um \times 50um$ with a reservoir size of $0.14um \times 15um$. After removing the reservoir, the initially immortal wire has a TTF of 5.704 years, rendering the wire quite vulnerable to EM aging.

2) Sink insertion attack: Many wires in a chip will not have passive reservoirs already attached to them, such is the case with the clock tree and signal nets. In these cases, a reservoir reduction cannot be attempted as reservoirs will likely be active and their removal will immediately cause chip failure at worst or performance degradation at best.

To target these wires, we can use a sink insertion attack, depicted in Fig. 5. As mentioned in III-B2, a passive sink added to a target wire will reduce its TTF. This type of attack is ideal for causing a target wire to fail when a passive reservoir is not present. Furthermore, like the previously mentioned reservoir reduction attack, this small addition will not have any large effect on the IR drop of the net.

Authorized licensed use limited to: Univ of Calif Riverside. Downloaded on June 24,2026 at 22:34:18 UTC from IEEE Xplore. Restrictions apply.

As a demonstration, we consider an immortal wire with periodic current density similar to that of a wire in a clock tree. We then insert a passive sink to the wire and observe the effects on TTF. It should be noted that for this simulation, we model the current density as the average current density due to the periodicity. It has been shown that for high frequency periodic signals, like we would find in a clock tree, the long term averaging effects mean that using the average current density is adequate [14]. The initial mortal wire is $0.05um \times 20um$ and the inserted passive sink is $3um \times 15um$. After inserting the sink, the initially mortal wire has a TTF of 0.7253 years, a drastic reduction in the TTF.

3) Layer demotion attack: In III-B1, it was shown that depending on the wire positioning, either up-stream or down-stream, a wire can experience the Early or Late failure effects. While this is something we can leverage in any EM attack, it can also be used as an attack by itself while also maintaining all the advantages of the topological attacks presented previously.

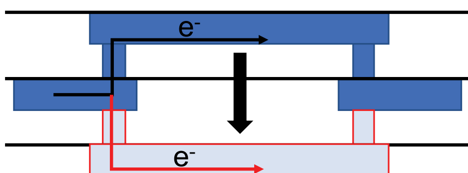


Fig. 6. The originally up-stream wire is moved to a lower level of metalization to put it in the down-stream configuration in the layer demotion attack

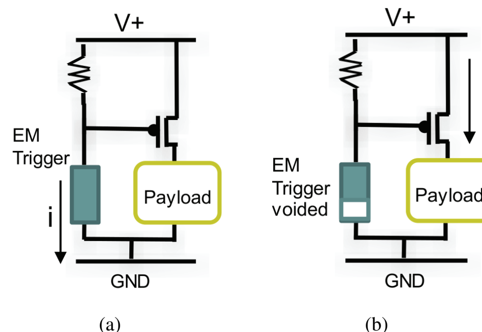
In this attack, a mortal wire that is normally positioned in the up-stream configuration, may have an acceptable TTF. However, if the wire were to be in the down-stream configuration, the Early failure mode would result in much more rapid failure. To achieve this, we can perform a layer demotion attack on an up-stream configured wire by moving the wire to a lower level of metalization than the wire its cathode is attached to. This will maintain the same electrical paths and IR drop of the circuit but will cause the wire to be in the down-stream configuration, and thus, experience Early failure.

To demonstrate this attack, we identify a mortal wire in the up-stream configuration with reasonably high TTF. In this case the wire has an initial TTF of 6.69 years. However, after reconfiguring the wire to a down-stream configuration, the TTF falls to 3.94 years.

B. EM as a Trojan trigger

In some cases, it may be desirable to activate a Trojan that does not render the chip inoperable. In this case, the challenge for an attacker is to embed a trigger for their payload in the chip that is difficult to activate or detect by the design house. EM-based Trojans offer a stealthy and lightweight option to triggering a Trojan payload due to their inherent stealthiness.

An EM-based trigger can utilize any of the modeling and attack techniques previously mentioned but are configured in such a way that their failure activates some other Trojan payload. In this case, it is best to use an early failure configured wire that, when activated, will quickly redirect current to the Trojan payload. We propose to use the EM-trigger to short the current past the Trojan payload. Upon failure of the Trojan wire, the current will be redirected to the payload, allowing it to perform some malicious task. An example of this configuration is shown in Fig. 7.



(a) (b)

Fig. 7. Example EM-based trigger for Trojan payloads showing circuit (a) prior to triggering and (b) with void present and payload activation.

V. Conclusion

In this paper we utilize recently proposed advanced EM modeling and simulation techniques to formulate novel reliability-based Trojan payloads. We propose two topology-based EM attacks that leverage the multi-segment stressing dynamics from atomic sinks and reservoirs. We also present a payload that exploits multi-mode failure mechanisms, early and late failure, by converting a wire from the up-stream configuration to the down-stream configuration. Furthermore, we propose an EM-based Trojan triggering mechanism for stealthy time-delayed activation of hardware Trojans. These proposed Trojans utilize the topology and structure of wires which gives them an advantage over previously proposed current density based EM-Trojans which can affect circuit performance.

References

[1] M. Tehranipoor and F. Koushanfar, "A survey of hardware trojan taxonomy and detection," *IEEE Design Test of Computers*, vol. 27, no. 1, pp. 10–25, 2010.
[2] Y. Shiyanovskii, F. G. Wolff, C. A. Papachristou, D. J. Weyer, and W. Clay, "Exploiting semiconductor properties for hardware trojans," *CoRR*, vol. abs/0906.3834, 2009.
[3] A. Sreedhar, S. Kundu, and I. Koren, "On reliability trojan injection and detection," *Journal on Low Power Electronics*, vol. 8, pp. 674–683, Dec. 2012.
[4] K. Vaidyanathan, B. Das, E. Sumbul, R. Liu, and L. Pileggi, "Building trusted ics using split fabrication," in *2014 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, pp. 1–6, May 2014.
[5] K. Xiao, D. Forte, Y. Jin, R. Karri, S. Bhundia, and M. Tehranipoor, "Hardware trojans: Lessons learned after one decade of research," *ACM Trans. on Design Automation of Electronics Systems*, pp. 6:1–6:23, May 2016.
[6] J. R. Black, "Electromigration-a brief survey and some recent results," *IEEE Transactions on Electron Devices*, vol. 16, no. 4, pp. 338–347, 1969.
[7] X. Huang, A. Kteyan, X. Tan, and V. Sukharev, "Physics-based electromigration models and full-chip assessment for power grid networks," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 35, pp. 1848–1861, Feb. 2016. DOI.
[8] M. A. Korhonen, P. Bo/rgesen, K. N. Tu, and C.-Y. Li, "Stress evolution due to electromigration in confined metal lines," *Journal of Applied Physics*, vol. 73, no. 8, pp. 3790–3799, 1993.
[9] S. X.-D. Tan, H. Amrouch, T. Kim, Z. Sun, C. Cook, and J. Henkel, "Recent advances in EM and BTI induced reliability modeling, analysis and optimization," *Integration, the VLSI Journal*, 2017. in press.
[10] X. Huang, V. Sukharev, and S. X.-D. Tan, "Dynamic electromigration modeling for transient stress evolution and recovery under time-dependent current and temperature stressing," *Integration, the VLSI Journal*, 2016.
[11] C.-K. Hu, D. Canaperi, S. T. Chen, L. M. Gignac, B. Herbst, S. Kaldor, M. Krishnan, E. Liniger, D. L. Rath, D. Restaino, R. Rosenberg, J. Rubino, S.-C. Seo, A. Simon, S. Smith, and W.-T. Tseng, "Effects of overlayers on electromigration reliability improvement for cu/low k interconnects," in *Reliability Physics Symposium Proceedings, 2004. 42nd Annual. 2004 IEEE International*, pp. 222–228, IEEE, 2004.
[12] L. Zhang, *Effects of Scaling and Grain Structure on Electromigration Reliability of Cu Interconnects*. PhD thesis, University of Texas at Austin, 2010.
[13] M. Lin and A. Oates, "An electromigration failure distribution model for short-length conductors incorporating passive sinks/reservoirs," *IEEE Transactions on Device and Materials Reliability*, vol. 13, pp. 322–326, March 2013.
[14] X. Huang, V. Sukharev, T. Kim, and S. X.-D. Tan, "Electromigration recovery modeling and analysis under time-depdendent current and temperature stressing," in *Proc. Asia South Pacific Design Automation Conf. (ASPDAC)*, pp. 244–249, 2016.

Authorized licensed use limited to: Univ of Calif Riverside. Downloaded on June 24,2026 at 22:34:18 UTC from IEEE Xplore. Restrictions apply.