Reliability Based Hardware Trojan Design Using Physics-Based Electromigration Models

Chase Cook, Sheriff Sadiqbatcha, Zeyu Sun, 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 rely on empirical Black's models can easily lead to performance degradation and less accuracy in Trojan activation time prediction. In this article, 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 a trigger for the EM attack on power/ground networks and signal and clock networks. Furthermore, we also present two potential EM attack mitigation techniques, namely, the split fabrication and burn-in testing.

[☆] This work is supported in part by NSF grant under No. CCF-1527324, and in part by NSF grant under No. CCF-1816361.

Email addresses: ccook009@ucr.edu (Chase Cook), stan@ece.ucr.edu (Sheldon X.-D. Tan)

Reliability Based Hardware Trojan Design Using Physics-Based Electromigration Models

Chase Cook, Sheriff Sadiqbatcha, Zeyu Sun, Sheldon X.-D. Tan

Department of Electrical and Computer Engineering, University of California, Riverside, CA 92521 USA

1. 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 (Integrated Circuit) 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, 3, 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) [5, 1]. 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.

As technology continues to scale, the back-end-of-line (BEOL) reliability progressively becomes harder to maintain. Particularly the ITRS has predicted electromigration (EM) to be a primary limiting factor of future IC design [6, 7]. This makes the BEOL aging based attacks increasingly viable as the amount of modification required by an attacker will continually decrease as technology scales and IC's become increasingly vulnerable to this type of aging. There are a few previous works that use the 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 [8], which ignores topology and copper via structural impacts [9]; these 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 the target wires which gives them minimal impact on circuit performance. Furthermore, the proposed methods are applicable to power, clock, and signal nets.

2. Electromigration basics

Electromigration is a physical effect in metal wires that, effectively, causes a wire's structure to physically degrade. This change is due to the migration of metal ions induced by momentum transfer from conducting electrons [8, 10]. The momentum transfer generates a hydrostatic stress within an embedded metal wire which, under normal circumstances, remains in an equilibrium state,

[☆☆] This work is supported in part by NSF grant under No. CCF-1527324, and in part by NSF grant under No. CCF-1816361.

Email addresses: ccook009@ucr.edu (Chase Cook), stan@ece.ucr.edu (Sheldon X.-D. Tan)

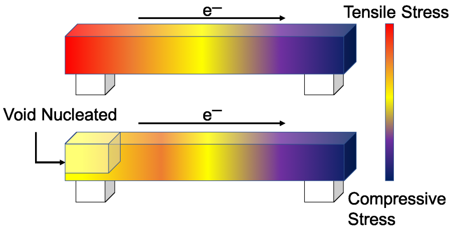


Figure 1: EM failure process showing a metal wire being stressed by electron wind and subsequent void formation

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 illustrated 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 [8], presented in 2.1, which is a semi-physical empirical method relying on test data to fit parameters. This method can be difficult 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 [10] 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 [9]. The development of this equation has resulted in the creation of the so-called three-phase model, as detailed in [11] and presented in 2.2, 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 until a void is formed, the Incubation phase where a void is formed and starts to grow 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 resistance change which may lead to 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.

2.1. Black's model

The traditionally employed method of predicting the time to failure is based on the approximate Black's equation [8].

$$MTTF = Aj^{-n}exp\{E_a/k_BT\} \tag{1}$$

Here, j is the current density, k_B is the Boltzmann's constant; T is the absolute temperature; E_a is the EM activation energy. The symbol A is a constant, which depends on a number of factors, including grain size, line structure and geometry, test conditions, current density, thermal history, etc. Current exponent n was found to be 2.

However, based experiments with real EM testing, it was found that Black's equation does not scale very well over a wide range of current densities. That is, the current exponent n, does not work for different ranges of current densities.

2.2. Three-phase model

Besides Black's equation, a more accurate three phase EM model has been developed recently [11]. In the new model, we have three phases including (1) the *nucleation phase* from $t = 0$ to t_{nuc}; (2) the *incubation phase* from t_{nuc} to t_i; and (3) the *growth phase* starting from t_i to t_{50}. The term t_{50} indicates the time-to-failure in statistical terms (50% of the samples fail). This model was later extended to consider more general multi-segment interconnect structures [12]. The following is a brief summary of this EM model.

In the **nucleation phase**, the void is formed at nucleation time (t_{nuc}) . Hydrostatic stress increases from the initial value to critical level. In order to model that, a more complete physics based modeling of transient hydrostatic stress evolution was proposed by Korhonen [10]. We illustrate the equation in the one dimensional case for the sake of presentation. Then stress $\sigma(x,t)$ is described by Korhonen's partial differential equation (PDE) with liner(Ta) blocked boundary conditions (BC):

$$\begin{aligned} PDE: &\frac{\partial \sigma}{\partial t} = \frac{\partial}{\partial x}\left[\kappa\left(\frac{\partial \sigma}{\partial x} + G\right)\right] \\ BC: &\frac{\partial \sigma}{\partial x}(0,t) = G,\ \frac{\partial \sigma}{\partial x}(L,t) = -G \end{aligned} \tag{2}$$

where, $\kappa = D_aB\Omega/kT$, B is the effective bulk elasticity modulus, Ω is the atomic lattice volume, $G = \frac{eZ\rho j}{\Omega}$ is the EM driving force, where e is the electron charge, eZ is the effective charge of the migrating atoms, ρ is the wire electrical resistivity. If the stress calculated by that model saturates before the critical level, the wire will never fail. Otherwise, the time in which stress reaches the critical level is t_{nuc}.

In the **incubation phase**, which is defined by the time period t_{nuc} to t_i, the void is nucleated, but its size is not significant. Hence the change in wire resistance will be very small and can be neglected. The incubation time($t_i - t_{nuc}$) can be estimated as:

$$t_i - t_{nuc} = \frac{\Delta L_{crit}}{v_d} \tag{3}$$

Here ΔL_{crit} is the length of critical void size and v_d is the void's growth rate. For a single segment wire, v_d is expressed as a function of atomic flux J, $v_d = \Omega J$ [13], where Ω is atomic volume. Atomic flux, $J = \frac{D_a f}{\Omega k T}$, is the number of atoms crossing a unit area per unit time. Thus, the atoms crossing per unit length can be expressed as JW, where f is electron wind force per atom: $f = eZ\rho j$.

For a multi-segment tree, all segments that share a terminal with the void can contribute to its growth. Electron wind at each segment can accelerate or slow down the void growth based on their direction. Hence, the total atom flux can be expressed as a combination of all the fluxes on the segments. For multi-segment wires, the effective atomic flux per unit length $v_d W_m$ is the void's growth rate on the main segment. This is expressed as:

$$v_d = \Omega J_m^* = \Omega \frac{1}{W_m} \sum_i J_i W_i = \frac{D_a e Z \rho}{k T W_m} \sum_i j_i W_i \tag{4}$$

Here j_i and W_i are the current density and width of the ith segment. W_m is the width of the main segment where the void is formed and J_m is the total flux contributing to the void. Here, we use $J_m^* = \frac{1}{W_m} \sum_i J_i W_i$ to compute the effective atomic flux J_m on the main segment. Note that if we only have one segment, then $v_d = \frac{D_a e Z \rho j}{kT}$ as shown in [14].

If the void volume saturates before it reaches the critical length, the wire will never fail. The **Incubation phase** ends when the void reaches L_{crit} at t_i. If the wire is a via-above wire, after the via is blocked by the void the current flow will also be blocked since the capping layer is fabricated with dielectrics such as Si3N4. This is referred to as early-failure and results in an immediate critical failure of the wire. However, if the wire is a via-below wire, the current flow can still pass but resistance of the wire will increase because current has to go through the liner which has much higher resistivity. This is referred to as late-failure. These concepts are explained in more detail further in the article.

Finally, in the **growth phase**, defined by time period from t_i to t_{50} the wire resistance starts increasing. Note that this phase is only possible in a via-below configuration and is unique to late-failure. After the via is blocked by the void, current is forced to flow through the liner. Since this liner is very thin, and its resistivity is much larger than copper, the current density and resistance on the liner will be very high. Resistance change can be expressed as [15]:

$$t - t_i = \frac{\Delta R(t)}{v_d [\frac{\rho_{Ta}}{h_{Ta}(2H+W)} - \frac{\rho_{Cu}}{HW}]} \tag{5}$$

where ρ_{Ta} and ρ_{Cu} are the resistances of the liner material (Ta for instance) and copper respectively, W is the line width of the segment where void is formed (main segment), H is the copper thickness, and h_{Ta} is the liner layer thickness.

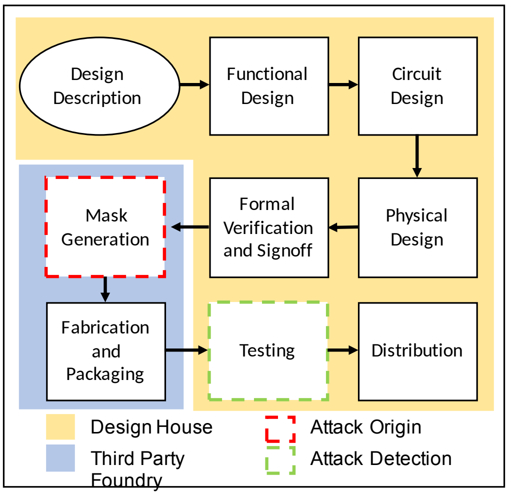


Figure 2: IC design and manufacturing flow showing attack and detection opportunities

Commercial tools do not utilize the Korhonen model or the three-phased model but instead still rely on the conservative Black's model. Using the three-phased Korhonen based method of modeling the EM-failure process is much more accurate, albeit time consuming. As such, commercial tools would be insufficient for the level of analysis we require to perform the attacks in this paper. However, several methods have been recently developed to solve this model quickly [16, 17] showing its viability as a simulation tool for these types of attacks. Both of the cited methods are very fast and accurate and only require analyzing the interconnect in question rather that performing the full chip EM sign-off that would be performed with a commercial tool. Further, this three-phase model allows us to make use of the complex EM failure process to engineer specific wire topologies that can be leveraged as a reliability based attack while the currently available commercial tools could not consider these effects.

3. 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. :w

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. Furthermore, with respect to the particular attacks presented in this article, an attacker must identify wires that are susceptible to these attacks. Primarily this requires an attacker to find wires with sufficient chip area around it or excess metal for modification and then find attack parameters that achieve the target life-time reduction. While automation tools could help in this regard, a determined attacker should not be too tightly constrained that they could not find candidate wires simply using visual inspection of the mask or layout in combination with commercially available physical design tools and published EM models such as the one we employ in this work.

In the following sections we outline some primary challenges to EM-based attack design, attack opportunities based on newly proposed physics-based EM models, and the newly proposed attacks.

3.1. Challenges in EM-based attacks

In order for a wire to fail due to EM, it must be stressed by electrical current. 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 [18]. 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 current providing a good stress source. Signal nets that are highly active are good stress sources but other nets, that have little activity, may not carry enough current to induce EM failure.

Additionally, simple alterations to a wire, such as altering its width 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.

3.2. Electromigration topology effects

3.2.1. 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 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) [14, 19].

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.

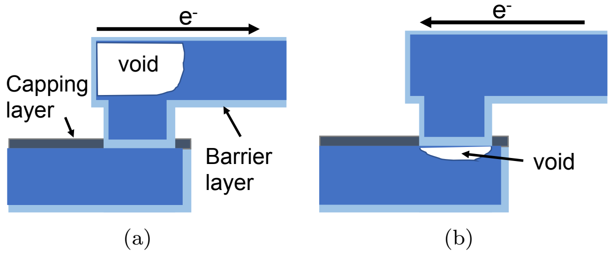


Figure 3: Via-below (a) and Via-above (b) wire structures showing void formation locations.

3.2.2. 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

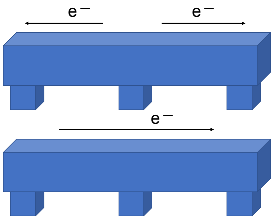


Figure 4: A two segment wire structure with the same current density (below) and different current densities (above)

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) [20]. 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.

4. EM attack methods

With the proper modeling, simulation, and design challenges in mind, we can formulate specific attacks using the EM wear-out effect. As mentioned previously, a naive method of attack relies on Black's equation where current density is the only parameter available to implement an attack. Practically, this means an attacker can simply decrease wire widths. While this can be an effective method, it has the drawbacks of affecting other circuit performance parameters, e.g., wire delay and IR drop. However, in this work we utilize the wire structure impacts on EM as presented in 3.2. In the following presented attacks IR drop and delay are not affected because, as we will present, we only need modify non-current carrying metal to create the attack.

In the following sections, to demonstrate our attacks, we generated EM resilient wire configurations. Then, we ran several simulations, using Finite Element Analysis and the three-phase model, on the target wire while sweeping attack parameters to find effective attack formulations.

4.1. 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.

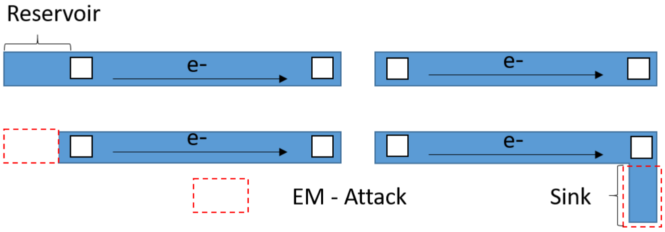


Figure 5: Illustrations of the reservoir reduction and sink insertion attacks

4.1.1. Reservoir reduction p/g network attack

As discussed in 3.2.2, 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. Often it is the case that large reservoirs are added for reliability reasons, primarily in the p/g network, or simply as a consequence of power grid synthesis that results in excess metal. 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.

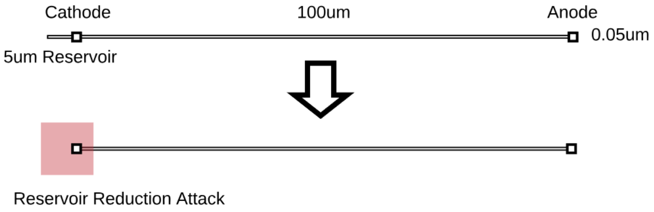


Figure 6: An example reservoir reduction attack

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 and show the attack in Fig. 6. The wire is $0.05\mu m \times 100\mu m$ with a reservoir size of $0.05\mu m \times 5\mu m$. After removing the reservoir, the initially immortal wire has a TTF of 5.197 years, rendering the wire quite vulnerable to EM aging.

4.1.2. Sink insertion attack

Many wires in a chip will not have passive reservoirs already attached to them, typically these will be 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 3.2.2, 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 since we are only adding passive metal to the wire.

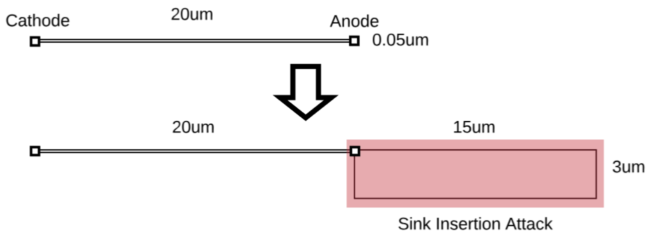


Figure 7: An example sink insertion attack

As a demonstration, we consider an immortal wire, shown in Fig.7, 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 [21]. The initially immortal wire is $0.05\mu m \times 20\mu m$ and the inserted passive sink is $3\mu m \times 15\mu m$. After inserting the sink, the initially immortal wire has a TTF of 0.7253 years, a drastic reduction in the TTF.

We note that in this particular example, the size of the reservoirs required can be quite large compared to the target wire. However, the area taken up by the reservoir is relatively small compared to the entire chip. Still, an attacker could be constrained by high density routing. In this case, care must be taken to find appropriate target wires to attack where room is available for a sink insertion. Additionally, sinks need not be rectangular but can take on all matter of shapes and sizes so long as the sink area is sufficient for the attack. Furthermore, it is not uncommon for large areas of a metal layer to be unoccupied requiring the insertion of passive dummy filler metal to maintain structural stability in the die during fabrication [22]. This provides an excellent opportunity for an attacker to attach the dummy metal to the anode of a wire, thereby creating a large passive reservoir without adding large amounts of metal.

4.1.3. Layer demotion attack

In 3.2.1, 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.

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.

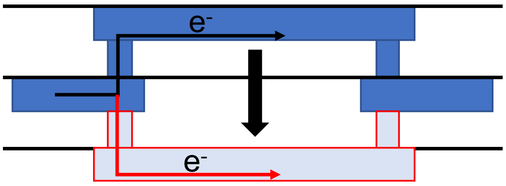


Figure 8: The originally up-stream wire is moved to a lower level of metalization to put it in the down-stream configuration in the layer demotion attack

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.

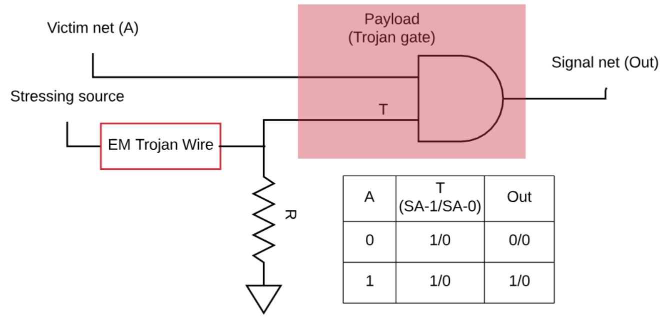
4.2. EM as a Trojan trigger

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 (or from) the Trojan payload. We propose to use the EM-trigger to control current flow such that during the aging process, the functional behavior of the circuit is unchanged. However, after activation, when the Trojan wire fails, the current flow will be redirected such that the Trojan payload becomes activated.

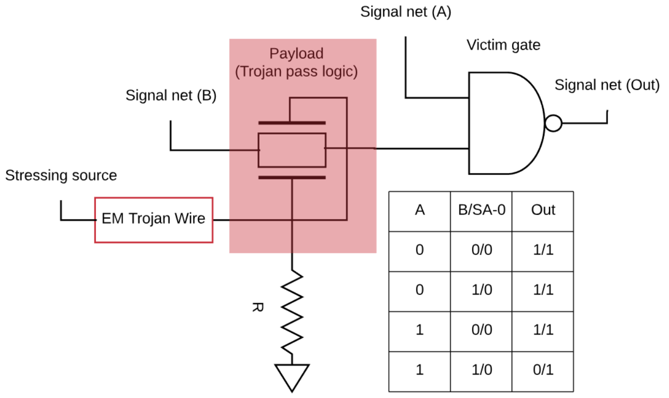
In Fig. 9 an example circuit is shown to demonstrate how an EM Trojan wire can be used to create a time-delayed trigger for a Trojan payload. In this case, the payload is an AND gate. Prior to activation, the victim net “A” will be input to the AND gate along with the Trojan net “T” which will be “stuck-at 1” (SA-1) while the Trojan wire still properly carries current. Because of this, the output “Out” will simply retain the value of “A”. However, once the Trojan wire fails, “T” will become “stuck-at 0” (SA-0) and consequently, “Out” will also be SA-0 regardless of stimulus at “A”.

In another example, shown in Fig. 10, an EM-based trigger wire is used in conjunction with pass logic transis-



A	T (SA-1/SA-0)	Out
0	1/0	0/0
1	1/0	1/0

Figure 9: Example circuit of an EM Trojan wire being used as a trigger for a Trojan gate payload



A	B/SA-0	Out
0	0/0	1/1
0	1/0	1/1
1	0/0	1/1
1	1/0	0/1

Figure 10: Example circuit of an EM Trojan wire being used as a trigger to deactivate a pass logic Payload

tors to attack a victim gate. In this case, the pass logic transistors allow for normal functional operation of the circuit, so long as voltage is sufficient at either input to the transistors. Prior to activation, the victim NAND gate will operate normally with inputs “A” and “B”. However, after the EM Trojan wire fails, the pass logic transistors will no longer allow the “B” net to pass and will create a SA-0 fault at the “B” input of the victim net. At this point, the victim gate’s output “Out” will always retain a high logic level.

The only drawback of using the EM-based Trojan wire as a trigger is that it likely requires the introduction of more circuitry to ensure the wire is stressed. That is, the wire needs a sufficient stressing source which requires the introduction of circuitry to create current flow which will have some effect on chip power consumption. This is because the current generated on signal nets may not be sufficient to stress an EM-Trojan wire. In the above examples we utilized a resistor connecting to a reference which will complete a circuit and allow constant current flow through the EM Trojan wire while ensuring we avoid shorting the circuit all together. However, this resistor could potentially be any circuit or structure that ensures the Trojan wire is stressed. Furthermore, making use of the structural attacks presented earlier can help mitigate the added power consumption as current draw may not have to be as significant compared to a purely current density based EM Trojan design. Lastly, other methods could be utilized to stress the wire that would not result in significant additional power consumption, e.g., the current from the charging and discharging of gate capacitance generated by a periodic signal such as a clock net could be sufficient to stress the Trojan wire.

5. Mitigation techniques for EM-based Trojans

EM-based Trojans pose a real threat due to the difficulty in detecting them through conventional testing methodologies. However, there are measures that chip designers can take to mitigate the possibility of an EM-based attack and to also enhance traditional testing methodologies to increase their chance of detecting these types of attacks.

5.1. Split-fabrication

As discussed previously,the primary concern over hardware Trojan attacks stems from the decentralization of the design and fabrication of ICs, due to increasing costs associated with manufacturing these devices, thus making them vulnerable to attack by third party fabs. The primary reason for the rising costs of manufacturing has to do with the highly advanced technology nodes, specifically the front end devices of the IC. However, the process for manufacturing the back-end-of-line interconnects is relatively unchanged from previous technology nodes. Split-fabrication has been proposed in several works [23, 4, 24] to take advantage of this fact and effectively makes the IC design process immune to EM-based attacks.

Split-fabrication separates the front-end and back-end-of-line manufacturing which provides several advantages with respect to the integrity of the fabrication process. The idea is to allow the third party fabs, which have invested in the advanced fabs with the tools and processes to manufacture at advanced technology nodes, continue to manufacture the front-end devices while the design house or other trusted manufacturer can finish the IC’s back-end with a relatively less expensive fab.

This methodology provides a few advantages. Firstly, the design house no longer needs to provide detailed design files that reveal the actual architecture of their designs. This makes the insertion of hardware Trojans that target the chip logic extremely difficult while also protecting the design house’s IP. Secondly, this methodology allows the design house to visually inspect the front-end of the chip before the back-end is manufactured, thus allowing the detection of any Trojan logic gates. lastly, with respect to EM-based attacks, this methodology would be particularly effective. EM-based attacks target the back-end-of-line interconnects, however, if the design house is using a split-fabrication process, then any untrusted fab could not insert this type of attack.

While not yet adopted by industry, real ICs have been manufactured using split-fabrication by researchers [4] showing its feasibility.

5.2. Burn-in testing

EM-based attacks are particularly difficult to detect due to their passive behavior prior to activation due to aging. While test vectors and side-channel analysis will fail to detect these types of attacks on their own, they could be used for detecting an EM-based Trojan if the Trojan was forced to activate during test time.

Burn-in testing is already a common methodology for ensuring an IC or PCB is free of defects or excessive process variation. These tests subject a chip to high stress conditions, outside of the normal use conditions, designed to cause failure in chips that do not meet reliability specifications. After testing, the chips that pass are considered reliable and can be introduced into the market where the expectation is that they will be used in the normal use condition which is far less extreme than the high stressing conditions they have been subjected to in the burn-in testing. Additionally, this type of testing is often employed by fabs to judge the EM resilience of a particular fabrication process by subjecting wires with varying dimensions and current densities to high stress until they fail. These results are then extrapolated to real world use cases to determine design rules for EM sign-off.

By subjecting a chip to burn-in testing, an EM Trojan, which is designed to fail early already, can be subjected to high stress conditions which will accelerate their aging. Coupling this with traditional logic based testing and side channel analysis, EM-Trojans which are forced to fail early during this process can be detected. Not all EM-Trojans will be detected in this manner however.

This technique will only affect Trojans with aggressive failure targets. However, this effectively reduces the design margin for the attacker by limiting the aging range that can be selected for the EM-attack. In other words, an attacker cannot create a Trojan that will fail very early without risking its activation during a burn-in test. This may be enough to limit an attacker to such an extent that an EM-based Trojan may never even be activated, even if inserted and not detected.

The burn-in technique is illustrated in Fig. 11. We simulate the EM-induced TTF for a wire under high stressing conditions of 390K with a voltage scaled to +5% and assume a burn-in duration of one week. Trojan wires with failure times below the 7 day burn-in duration under these conditions would likely have been activated at test time and detected.

6. Conclusion

In this article, we utilized recently proposed advanced EM modeling and simulation techniques to formulate novel reliability-based Trojan payloads. We proposed two topology-based EM attacks that leverage the multi-segment stressing dynamics from atomic sinks and reservoirs. We also presented 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 proposed an EM-based Trojan triggering mechanism for stealthy time-delayed activation of hardware Trojans. These 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. Finally, we discussed two potential EM attack mitigation techniques including split fabrication and burn-in testing.

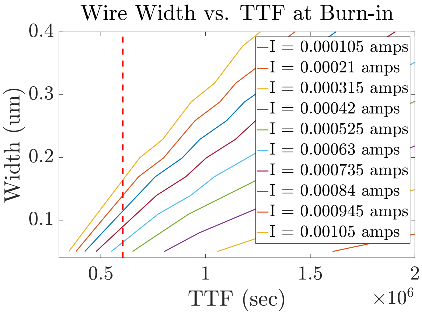


Figure 11: Burn-in testing reduces the range of failure times available to an attacker by inducing failure in aggressive TTF targets.

[1] M. Tehranipoor, F. Koushanfar, A survey of hardware trojan taxonomy and detection, IEEE Design Test of Computers 27 (1) (2010) 10–25.

[2] Y. Shiyanovskii, F. G. Wolff, C. A. Papachristou, D. J. Weyer, W. Clay, Exploiting semiconductor properties for hardware trojans, CoRR abs/0906.3834. `arXiv:0906.3834`.
URL `http://arxiv.org/abs/0906.3834`

[3] A. Sreedhar, S. Kundu, I. Koren, On reliability trojan injection and detection, Journal on Low Power Electronics 8 (5) (2012) 674–683.

[4] K. Vaidyanathan, B. Das, E. Sumbul, R. Liu, L. Pileggi, Building trusted ICs using split fabrication, in: 2014 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), 2014, pp. 1–6.

[5] K. Xiao, D. Forte, Y. Jin, R. Karri, S. Bhundia, M. Tehranipoor, Hardware trojans: Lessons learned after one decade of research, ACM Trans. on Design Automation of Electronics Systems (1) (2016) 6:1–6:23.

[6] International technology roadmap for semiconductors (ITRS) interconnect, 2015 edition, `http://public.itrs.net` (2015).

[7] J. Lienig, M. Thiele, Fundamentals of Electromigration-Aware Integrated Circuit Design, Springer, 2018.

[8] J. R. Black, Electromigration-a brief survey and some recent results, IEEE Transactions on Electron Devices 16 (4) (1969) 338–347.

[9] X. Huang, A. Kteyan, S. X.-D. Tan, V. Sukharev, Physics-based electromigration models and full-chip assessment for power grid networks, IEEE Trans. on Computer-Aided Design of Integrated Circuits and Systems 35 (11) (2016) 1848–1861.

[10] M. A. Korhonen, P. Bo/rgesen, K. N. Tu, C.-Y. Li, Stress evolution due to electromigration in confined metal lines, Journal of Applied Physics 73 (8) (1993) 3790–3799.

[11] S. X.-D. Tan, H. Amrouch, T. Kim, Z. Sun, C. Cook, J. Henkel, Recent advances in em and bti induced reliability modeling,

analysis and optimization, Integration, the VLSI Journal 60 (2018) 132–152.

[12] Z. Sun, S. Sadiqbatcha, H. Zhao, S. X.-D. Tan, Accelerating electromigration aging for fast failure detection for nanometer ICs, in: Proc. Asia South Pacific Design Automation Conf. (ASPDAC), IEEE, 2018, pp. 623–630.

[13] Z. Suo, Reliability of Interconnect Structures, Vol. 8 of Comprehensive Structural Integrity, Elsevier, Amsterdam, 2003.

[14] 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, 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, IEEE, 2004, pp. 222–228.

[15] X. Huang, T. Yu, V. Sukharev, S. X.-D. Tan, Physics-based electromigration assessment for power grid networks, in: Proc. Design Automation Conf. (DAC), IEEE, 2014, pp. 1–6.

[16] C. Cook, Z. Sun, E. Demircan, M. D. Shroff, S. X.-D. Tan, Fast electromigration stress evolution analysis for interconnect trees using krylov subspace method, IEEE Trans. on Very Large Scale Integration (VLSI) Systems 26 (5) (2018) 969–980.

[17] X. Wang, Y. Yan, J. He, S. X.-D. Tan, C. Cook, S. Yang, Fast physics-based electromigration analysis for multi-branch interconnect trees, in: Proc. Int. Conf. on Computer Aided Design (ICCAD), IEEE, 2017, pp. 169–176.

[18] X. Huang, V. Sukharev, S. X.-D. Tan, Dynamic electromigration modeling for transient stress evolution and recovery under time-dependent current and temperature stressing, Integration, the VLSI Journal 55 (2016) 307–315.

[19] L. Zhang, Effects of scaling and grain structure on electromigration reliability of cu interconnects, Ph.D. thesis, University of Texas at Austin (2010).

[20] M. Lin, A. Oates, An electromigration failure distribution model for short-length conductors incorporating passive sinks/reservoirs, IEEE Transactions on Device and Materials Reliability 13 (1) (2013) 322–326.

[21] X. Huang, V. Sukharev, T. Kim, 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), IEEE, 2016, pp. 244–249.

[22] T. Smith, V. Mehrotra, D. White, Dummy fill for integrated circuits, U.S. Patent 7 380 220 B2 (May 2008).

[23] R. Jarvis, M. McIntyre, Split manufacturing method for advanced semiconductor circuits, U.S. Patent 2004 0102019 A1 (May 2004).

[24] M. Jagasivamani, P. Gadfort, M. Sika, M. Bajura, M. Fritze, Split-fabrication obfuscation: Metrics and techniques, in: 2014 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), 2014, pp. 7–12. doi:10.1109/HST.2014.6855560.