Lurking in the Shadows: Challenges for X-Ray Inspection to Uncover Electromigration-Based Hardware Trojans in Advanced Packaging

Katayoon Yahyaei*, Susann Rothe‡, Mahmood Vawoo Dawood Naina†, Antika Roy*, M. Shafkat M. Khan*, Ozgur Sinanoglu†, Jens Lienig‡, Johann Knechtel†, Navid Asadizanjani*
*Dept. of Electrical and Computer Eng., University of Florida, Gainesville, FL, USA
†Center for Cyber Security, New York University Abu Dhabi, UAE
‡Institute of Electromechanical and Electronic Design (IFTE), Dresden University of Technology, Dresden, Germany
{ka.yahyaei, antika.roy, m.khan3}@ufl.edu, {mv2532, os22, johann}@nyu.edu, {susann.rothe, jens.lienig}@tu-dresden.de, nasadi@ece.ufl.edu

***Abstract*—We introduce and analyze the notion of electromigration (EM)-based hardware Trojans (HTs) in advanced packaging. Our HTs exploit shadows and imaging artifacts in X-ray inspections, thereby remaining hidden, while severely limiting the lifetime of critical interconnects, i.e., introducing denial-of-service attacks. We conduct a first-of-its-kind case study on a state-of-the-art (SOTA) *CoWoS* interposer system as follows. First, we carefully devise EM-based HTs for the interposer's power delivery network (PDN), a prime target for such HTs. Second, we confirm the HTs' disruptive effects, triggered by EM mechanisms, via SOTA physics-based FEM simulations. Third, we systematically evaluate the conditions under which these HTs remain hidden within the PDN, via commercial tooling for X-ray simulations. We find that our HTs can reduce mean time to failure (MTTF) by two orders of magnitude, while remaining hidden in over 88% of exposures during careful 360-degree X-ray inspection, even under best-case detection conditions, and even for large HTs exploiting upto 97% of the interconnect's width. Ultimately, we find that our HTs represent a practical and severe threat, necessitating further efforts for supply-chain assurance.**

***Index Terms*—Electromigration, Hardware Trojans, Design for Inspection, X-Ray Inspection, Reliability, Hardware Security, Advanced Packaging Technology**

I. Introduction

Advanced Packaging. The surge in artificial intelligence and high-performance computing has driven hardware requirements beyond Moore's Law, leading to the adoption of advanced packaging technologies such as 2.5D and 3D integration. These techniques enable the development of smaller, higher-density systems with enhanced functionality, increased processing speeds, and reduced power consumption [1]. The complexity of these systems, however, with their many stacked layers and various materials, introduces significant challenges to physical inspection. The wide range of potential defects necessitates a meticulous inspection process to ensure connectivity, manufacturing reliability, and integrity [2].

X-Ray Inspection. High-resolution X-ray systems enable non-destructive visualization of advanced packages, which is essential to verify structural integrity and for accurate defect detection, all without the need to physically expose layers [3]. However, even X-ray imaging encounters significant challenges due to increased noise, scatter, and clarity issues arising from the intricate nature of modern transistors and heterogeneous interconnect structures in advanced 2.5D and 3D systems. Such persistent noise and scatter complicate inspection and failure analysis, distort measurements, and increase inspection time and cost [4].

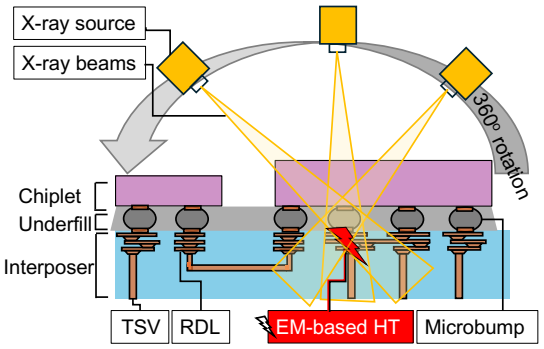

Fig. 1: EM-based HTs in a 2.5D sytem's interposer, embedded within the redistribution layers and hiding in the shadows below the microbumps from X-ray inspection.

Electromigration. At the same time, the complex integration of heterogeneous materials and components makes reliability of such advanced packages a major concern. Electromigration (EM) is one of the significant reliability issues in advanced packaging, especially as device dimensions decrease and current densities within interconnects rise [5]. This process, driven by the momentum transfer between electrons and metal atoms, can result in the formation of voids or hillocks in metal lines, both leading to system failures [6].

Malicious Modifications: Challenges for Inspection. Inspection methods typically address the challenges of X-ray imaging missing *unintended manufacturing defects* which, as outlined, is already challenging in itself [7]. Thus, *intended and malicious modifications* are likely even more challenging to detect, especially once adversaries carefully exploit noise and imaging artifacts observed during the inspection process.

Scope and Contributions of Our Work. We present the first in-depth study of this interdisciplinary and complex threat.

This is the personal version of the paper created by the authors. Please cite as:
K. Yahyaei, S. Rothe, M. Vawoo Dawood Naina, A. Roy, M. Shafkat, M. Khan, O. Sinanoglu, J. Lienig, J. Knechtel, N. Asadizanjani "Lurking in the Shadows: Challenges for X-Ray Inspection to Uncover Electromigration-Based Hardware Trojans in Advanced Packaging," Proc. of the IEEE 2025 Int. Conf. on Physical Assurance and Inspection of Electronics (PAINE 2025), Denver, USA, Oct. 2025

We examine how EM-based hardware Trojans (HTs) can exploit shadows and imaging artifacts that occur during X-ray inspection of complex advanced packages. Figure 1 illustrates the core concept: even with 360-degree rotation around the X-axis for thorough profile views of the redistribution layer (RDL), X-ray inspection may face unexposed areas in an advanced package, which can be exploited for EM-based HTs.

Our contributions are as follows. First, we formulate a threat model that properly frames the scope and implementation of EM-based HTs. Second, we explore the insertion of EM-based HTs for a state-of-the-art (SOTA) CoWoS interposer. Third, using SOTA physics-based FEM and commercial X-ray simulations, we systematically evaluate fundamental trade-offs between the HT's effectiveness and its stealthiness. Finally, we discuss the implications of such advanced HTs for design for inspection (DFI) principles.

II. Background

A. *X-Ray Inspection*

*1) **Basics**:* X-ray inspection is vital for ensuring the quality and reliability of electronic systems [7]. This high-resolution, non-destructive technique can penetrate multiple layers, offering detailed images of internal and buried structures, inspecting stacked components, and ensuring proper alignment for heterogeneous integration, making X-ray inspection an indispensable tool in advanced packaging [3].

*2) **Challenges for Advanced Packaging**:* Beyond conventional noise-related challenges, non-destructive inspection of stacked packages is challenging, particularly for resolving submicron defects within practical acquisition times [8]. Materials with low-k dielectrics require high resolution to detect defects, where balancing trade-offs between resolution, inspection speed, and X-ray dose remains challenging [3]. However, high-energy X-rays ($\sim 100\,\mathrm{kV}$) necessary to penetrate dense samples often obscure defects in low-Z materials, like voids and delamination [9]. Furthermore, application-specific demands for in-line inspection dictate the time and resources available for a particular manufacturing process [10].

*3) **Design for Inspection**:* DFI aims to enhance inspection efficiency, ensuring that advanced packages exhibit high observability for effective post-silicon validation [4]. One DFI-based solution is to quantify the X-ray inspection efficiency for a given design, aiding in design optimization [11]. Further, a framework has been proposed that can predict optimal design specifications by balancing imaging quality with design constraints [4]. Efforts have also been made to develop design guidelines focused on inspection efficiency for advanced packages [12]. Finally, X-ADAPT was introduced as alternative approach for when design revisions are not feasible (e.g., due to stringent performance constraints), improving the inspection process via customized strategies [13].

B. *Electromigration*

*1) **Mechanism and Modeling**:* First, EM mainly affects direct current lines like power delivery networks (PDNs). Second, EM robustness is typically ensured by limiting the maximum current density in a wire. The foundation for this is Black's law [14], which is an empirical equation to calculate the lifetime depending on temperature and current density.

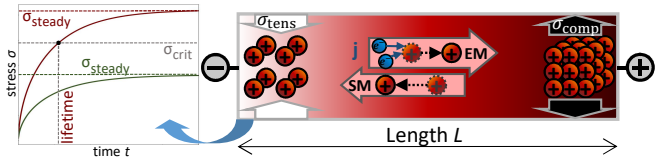

Fig. 2: EM-induced stress in an interconnect (right) [6] and stress evolution at the cathode (left).

While Black's law is still an industry-wide standard, its accuracy is limited, and a more recent approach for physics-based EM modeling is applied in this work [15].[1] Figure 2 illustrates its basics. First, EM pushes atoms from the cathode toward the anode of a wire; thus, hydrostatic stress starts to grow. The resulting stress gradient then drives stress migration (SM), which partly counteracts EM. The stress will build up until an equilibrium of EM and SM is reached, the so-called steady state, or a void nucleates. The latter happens if a critical stress for failure is exceeded. The underlying *Korhonen equation* with boundary conditions (BCs) for a finite single-segment line of length L describes the stress, σ, building up over time, t, as follows:

$$\frac{\partial \sigma}{\partial t} = \frac{\partial}{\partial x}\left[\kappa\left(\frac{\partial \sigma}{\partial x} - \beta j\right)\right], \text{ BCs: } \left.\frac{\partial \sigma}{\partial x}\right|_{x=0,L} = \beta j \quad (1)$$

Here, j is the current density, $\kappa = DB\Omega/k_\mathrm{B}T$, $\beta = e\rho Z/\Omega$, diffusivity $D = D_0 \cdot \exp\left(-E_\mathrm{a}/\left(k_\mathrm{B}T\right)\right)$, B is the Bulk modulus, Ω the atomic volume, k_B Boltzmann's constant, T the Temperature, e the elementary charge, ρ the specific resistivity, Z the electric charge number, D_0 the diffusion constant, and E_a the activation energy.

*2) **EM in Advanced Packages**:* EM becomes increasingly prominent in advanced packages because of complex material transitions across interconnects and higher current densities. For one, electrons pass through a variety of materials, including copper traces, Sn-Ag-Cu (SAC) solder bumps, nickel-based underbump metals, and copper interposer pads. This can ultimately lead to failures in solder joints or RDLs [18], [19]. For another, the high-density nature of advanced packaging significantly reduces the interconnect sizes and, thus, pushes current densities against design-rule limits [5], [16], [18], [20].

Recent studies quantify the EM risks in advanced packages. For instance, EM tests in flip-chip QFN packages, under extreme conditions, revealed that intermetallic compound formation and voiding at Cu/solder interfaces led to rapid resistance increase [18]. Through-silicon vias (TSVs) introduce another dimension of complexity, as they act as both conduits and sources of stress. Electro-thermal-mechanical interactions can degrade lifetime not only within the TSV but also in adjacent copper wiring [21]. Another study [5] focused on different interconnect and bump configurations.

[1]This approach is common for EM research conducted within the last decade [6]. For example, FEM models to accordingly simulate transient stress in interconnects have been published [15], [16] and made available [17].

C. *Hardware Trojans*

HTs describe any malicious modifications of circuits, breaking the fundamental assumption of hardware serving as root-of-trust for secure data processing. Several studies have demonstrated HTs in real silicon [22]–[24]. By design, HTs are minor in extent but severe in fallout [23], [25], [26]. For example, HTs can undermine the reliability of circuits [27], corrupt computation [23], leak privileged data [28], or cause systems to stop working via glitching or denial-of-service (DoS) attacks [29]. Besides, HTs can be introduced at any point in the supply chain, e.g., at design time through 3rd-party modules, at manufacturing time through mask edits, even post-silicon at the package level [30], etc. Finally, most HTs comprise two distinct parts: trigger and payload. The trigger is an activation mechanism, typically based on rare and specific combinational/sequential conditions. Once activated, the payload performs the HT's actual malicious operation.

III. Threat Model

A. *Scope of EM-based HTs*

EM-based HTs aim to decrease the lifetime of interconnects, synonymously defined as mean time to failure (MTTF) in this work. Such HTs realize glitching or DoS attacks that affect the interconnects but ultimately target the whole system [25], [29]. Given the fact that EM predominantly impacts direct current lines, EM-based HTs are most promising for PDNs [27], [31]; we follow the same adversarial approach in this work.

It is important to note that EM-based HTs (i) can be realized at design-time but also via post-silicon modifications of the circuits and/or package itself, e.g., by focused-ion beam (FIB) edits [32]; (ii) only require adversarial edits of the metal layers, rendering them resilient against traditional inspection focused on the active layer [33]; (iii) bypass regular post-silicon circuit testing, as their malicious payload is the delayed but built-in disruption of interconnects; (iv) are trigger-less and zero-gate.

In short, EM-based HTs enable delayed glitching or DoS attacks, while bypassing traditional HT detection.

B. *Implementation of EM-based HTs*

Adversaries can either aim for (i) lowering the critical stress, e.g., by changing the via configuration or removing redundant vias, or (ii) accelerating stress build-up, e.g., by introducing anode reservoirs or locally increasing current density [27], [31]. Note that, for both options, adversaries require detailed technology and design parameters, which can be obtained from technology providers and/or by careful inspection of the circuit design. Which option is more practical also depends on the attack point-in-time, as discussed next.

First, if HTs are implemented at design stage, they will be subject to current-density verification, where modifications to anode reservoirs and via configurations are more promising to remain stealthy. In contrast, implementing modifications at the mask level can be challenging, as this may require significant routing tracks/resources to be available/and or substantial rerouting. The latter may also lead to notable side-effects in power and performance profiles, which could enable detection.

TABLE I: Advanced 2.5D *CoWoS* System: Design Rules

Rule	Value	Rule	Value
Metal layers	4	Metal thickness	1μm
PDN width/spacing	40μm/100μm	Dielectric thickness	1μm
Micro-bump pitch	40μm	Micro-bump height/width	25μm
Die height	200μm	Interposer height	100μm

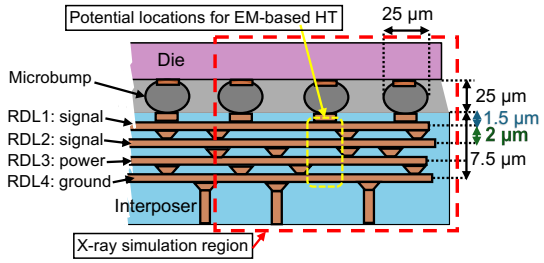

Fig. 3: Region of interest in the 2.5D *CoWoS* system.

Second, if HTs are implemented post-design, it seems promising to narrow down a wire and/or remove redundant vias. Such malicious modifications will increase the maximum current density and, thus, can only be applied in steps following layout verification, e.g., during mask preparation or FIB edits.

IV. Methodology for Experimental Investigation

A. *Setup for Case Study*

Advanced Packaging. For practical relevance, we consider a SOTA, commercial-grade 2.5D system featuring the well-established *CoWoS* interposer technology [34]. See Tab. I for design rules from [34] and further rules defined for our study.

Concept for EM-based HT. Based on Sec. III-B, we devise EM-based HTs that shall locally increase the current density in the PDN, by narrowing down some PDN wire. Such malicious wire modifications can be small and, thus, hard to detect via X-ray inspection, especially when placed strategically under microbumps. We illustrate this key concept of our work in Fig. 3. Importantly, the *CoWoS* system [34] used for our case study utilizes wide power lines that can be easily narrowed down without violating minimal width constraints (0.4 μm) and carry high currents (upto 12 A in total)—such interconnects become prime targets for EM-based HTs.

Without loss of generality, we consider post-design attacks, and we assume attackers have capabilities for post-silicon, metal-only FIB edits of the interposer RDL, specifically of the PDN. To reflect supply-chain cost/throughput and limit detectability, we bound attackers to a per-device budget of a few localized FIB edits at roughly one device per hour. Furthermore, our evaluation targets for an in-field MTTF of upto 10^5 second (i.e., around a day) after inspection.

Challenges for HT Implementation. The main mechanism for the proposed EM-based HT is the combination of high current density and the resulting Joule heating, both accelerating EM (Fig. 4). While powerful in general, adversaries have to carefully implement this concept. First, stress has to build up fast enough (to cause wire degradation within some desired MTTF), whereas excessive heating has to be avoided (to ensure functionality during initial testing). Second, the

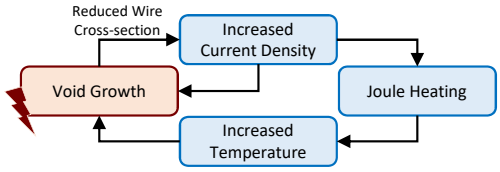

Fig. 4: Self-acceleration of EM-induced void growth [6].

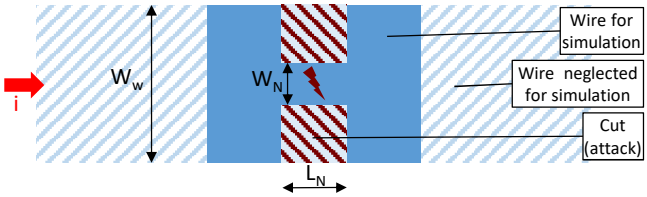

Fig. 5: Geometries for EM-based HTs under FEM simulations.

modifications of the wire should not significantly affect the IR drop and must, thus, be relatively minor. The modifications should also be minor to remain hidden under X-ray inspection. We study all these aspects in depth next.

B. FEM Simulations for HT Concept and Design

Model. To capture stress caused by EM and SM, under Joule heating, we adopt a SOTA coupled structural, thermal, electric, and diffusion simulation model from [15], [17].[2]

Geometries for HT Design. Following Fig. 5,[3] we study the following two cases in detail:

1) *Baseline, no HT.* We model a long wire (of 40μm width, W_W) under a given current load. There is insignificant Joule heating, so MTTF is dictated by EM and SM at a constant temperature. The location of void nucleation is the cathode end of the wire.
2) *With HT.* By narrowing down a short portion L_N of the wire to W_N, the current density will increase locally and, due to current crowding, that narrow portion is heating up. Any increase in temperature accelerates EM and significant stress will build up around this narrow portion. Accordingly, the location of failure will quickly shift from the cathode to the narrow portion.

Simulation Parameters. We consider a typical operating temperature $T_0 = 60\,°C$ for the whole system, including the HT-impacted interconnects. We assume convection from all wire surfaces for heat leakage into the surrounding dielectric/underfill and package [35]. We consider current densities of $0.125\,$MA/cm2, $0.25\,$MA/cm2, and $0.5\,$MA/cm2, respectively, which are typical values for interposer PDNs and in line with the power supply defined for the *CoWoS* system [34]. Furthermore, we set $E_a = 0.8\,$eV.

[2]We consider the moment the critical stress is reached as MTTF. In reality, wires will not fail the very moment a void nucleates; the void has to reach a critical volume first. However, void growth is a fast process compared to the time until critical stress is reached. Also, the process is self-accelerating, as a void further reduces the wire cross-section and, thus, increases current density and Joule heating (Fig. 4).

[3]As shown, we limit the model to a small region of interest. We confirm that regions further away experience only negligible stress build-up.

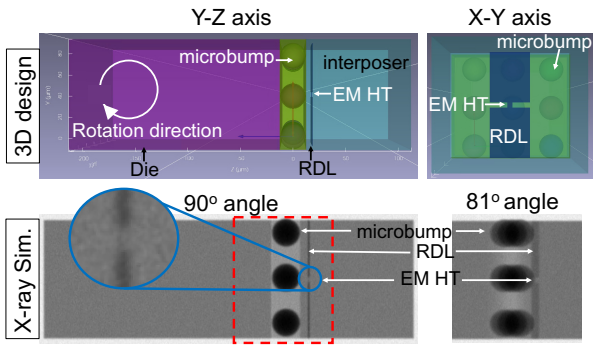

Fig. 6: Simplified *CoWoS* system in 3D design-space and corresponding, exemplary X-ray simulation result.

C. X-Ray Simulations for HT Inspection

Simplifications Toward Best-Case Detection. Following Fig. 3, we simplify the advanced package of the 2.5D *CoWoS* system for X-ray simulations. Doing so enables best-case assessment for HT detection—which is equivalent to worst-case assessment for HT stealthiness—as follows:

- *Exclusion of C4 bumps and packaging structures below.* Large and dense packaging structures like C4 bumps can completely block X-ray beams in significant areas of the interposer. Thus, this simplification mimics scenarios where the interposer is inspected independently, which is not necessarily practical for in-line inspection.
- *Simplification of dies/chiplets.* The die above the region of interest is simplified to a silicon bulk, ignoring thin but dense intra-die metal layers that otherwise contribute to X-ray absorption and scatter.
- *Focus on single RDL.* The interposer is simplified to a silicon bulk except for the RDL with the HT. Doing so eliminates noise and scatter from other RDLs and TSVs.
- *Region of interest at interposer's edge.* Inspecting a region near the edge of the interposer prevents obstruction of view by other microbumps. Furthermore, scatter and attenuation of X-ray beams are less noisy near the edge.

Again, the idea is to limit any X-ray noise and scatter. If EM-based HTs remain hidden even in these conditions, we can conclude they will remain hidden in the full design as well.

Simulation Setup. We use Novi-Sim [36], a SOTA commercial software. Imaging parameters are set such that they do not impose limits for inspecting the RDL in detail against EM-based HT. Specifically, we use a field of view (FOV) of $520\,\mu m \times 130\,\mu m$, an exposure time of $10\,s$, and a resolution of approximately $0.97\,\mu m$. We consider 360-degree rotation in the Y-Z plane, i.e., around the X-axis, for thorough profile views of the RDL. The motivation here is the same as above; once in-line imaging constraints apply, inspection becomes more noisy and limited and, thus, HT detection more difficult.

Geometries for HT Design. We use the same parameters as in the FEM simulation, L_N and W_N (Fig. 5). Furthermore, we model the distance of the RDL to microbumps, D_u. Figure 6 shows the geometry of the simplified package and examples for X-ray inspection around the X-axis, with the same region

Algorithm 1 Systematic Assessment of Stealthiness of EM-based HTs under X-Ray Inspection

Definitions: n: number of projections, γ: RDL grid size
α and β: SNR threshold factor,
S_{R}: signal intensity of region R
Projections at angles $\in \{0, \frac{360}{n}, \frac{2\times360}{n}, \ldots, \frac{(n-1)\times360}{n}\}$
for $i = 1$ to n **in** Projections **do**
  Detect R_r as the exposed RDL region
  Divide R_r into cells of size $\gamma \times \gamma$ each denoted as $r_{r,j}$
  Detect R_b as the background region
  $SNR_r = \left\{ snr_r = \frac{\text{mean}\{S_{r,j}\}}{\sigma_r(S_{Rb})} \text{ for all } r_{r,j} \in R_r \right\}$
  $H_i = 0$ **if** $snr_r < \alpha\,\text{mean}\{SNR_r\}$ **for any** snr_r
  $H_i = 1$ **if** $snr_r > \alpha\,\text{mean}\{SNR_r\}$ **for all** snr_r
end for
$HQM = (\sum_{i=0}^{n} H_i) \times (\frac{100}{n})$

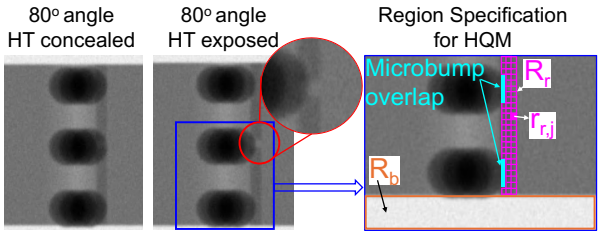

Fig. 7: Examples of inspection against EM-based HTs.

of interest as in Fig. 3 highlighted. Note that, for all subsequent X-ray images, we only show the same region of interest.

Systematic Assessment. To quantify how well EM-based HTs can remain "lurking in the shadows", we introduce a so-called hiding quantification metric (HQM). In Algorithm 1, we calculate HQM for various interposer and HT settings, over 40 projections (n = 40) around the X-axis. More specifically, for each parameter combination (L_{N}, W_{N}, D_{u}), we perform a single deterministic X-ray simulation using a fixed set of 40 projection angles. The microbumps array and HT placement are constant (i.e., no randomization/variance effects), and design parameters were swept deterministically. Consequently, HQM values are reported as point-estimates without confidence intervals.

Some examples following Algorithm 1 are shown in Fig. 7. Considering the feature sizes, we set γ to 0.5 µm. Parameter α can be obtained using a golden reference sample with some known EM-based HT; the actual value must be selected such that it is slightly larger than ($\text{SNR}_{\text{EM-based HT}}/\text{mean}\{\text{SNR}_{\text{r}}\}$). Based on our experiments with various interposer and EM-based HT settings, we find $\alpha = 0.94$ as most suitable.

V. Results for Experimental Investigation

A. *Lifetime: Trojan Effectiveness*

*1) **Impact of** L_{N}:* Our initial FEM simulations showed that L_{N}, the length of the narrow portion, does not significantly affect lifetime. Thus, we set $L_{\mathrm{N}} = 5$ µm, which is short enough to limit the impact on IR-drop (hindering HT detection during circuit testing), yet long enough to comply with technology constraints and to ensure a stable FEM simulation.

As shown in Fig. 8, the narrow portion of the wire experiences significantly higher current densities and, thus, heats up.

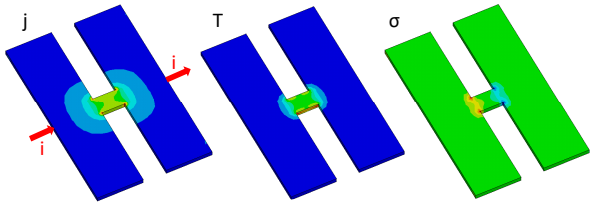

Fig. 8: FEM results for $i = 50$ mA and $W_{\mathrm{N}} = 4$ µm shortly after the critical stress is reached. The maximum temperature is 88 °C, i.e., 28 K higher than T_0. Across all plots, blue corresponds to respective lowest values, whereas red corresponds to respective highest values.

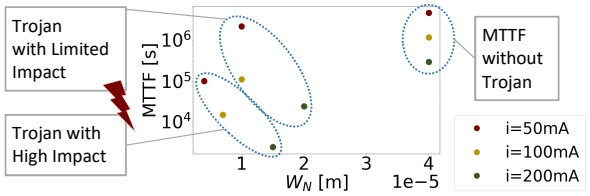

Fig. 9: Effectiveness of various HT configurations.

Accordingly, we can observe that stress builds up fast at the ends of the narrow portion, indicating strong EM degradation, whereas the wide portion does not experience such an impact. Thus, the effectiveness of the proposed EM-based HT is successfully demonstrated.

*2) **Impact of** W_{N}:* In Fig. 9, the results of representative lifetime simulations are shown over varying currents i and varying widths of the narrow portion W_{N}. Note that current values are derived to match the considered current densities (Sec. IV-B) and wire geometries.

For baseline cases without HTs, as expected, lifetime depends on the current that the wire is stressed with. For cases with HTs, our simulations reveal some dependency effects:

1) If the wire is stressed with small currents, Joule heating is limited, and the HT requires a larger reduction of the wire's width to become effective. At the same time, the risk of immediate failure is relatively low.
2) If the wire is stressed with large currents, Joule heating is significant, and the HT becomes effective even if the wire's width is reduced only to some degree. At the same time, the lifetime drops fast and it is challenging to avoid immediate failure.

*3) **Takeaways**:* While the EM-based HT's working is demonstrated, we find that the range of currents for which the HT is both effective and practical is limited. Consequently, attackers need detailed knowledge of technological parameters, specifically the thermal and EM behavior, and the design parameters, specifically the expected currents. As formulated in the threat model (Sec. III-B), such assumptions are practical.

B. *X-Ray Observability: Trojan Stealthiness*

*1) **Impact of** L_{N}:* Following the results from the FEM simulations (Sec. V-A), and without loss of generality, we fix W_{N} at 4 µm. For each possible value D_{u}, we vary L_{N} between 1 µm and 35 µm and track the resulting HQM. Related findings are shown in Fig. 10 and discussed next.

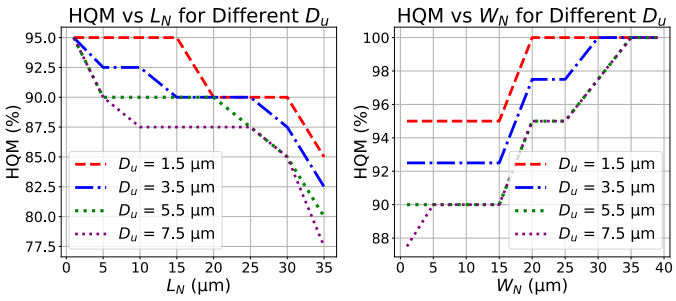

Fig. 10: Effect of varying W_{N} and L_{N} on HQM.

First, for constant D_{u} values, HQM generally decrease as L_{N} increases. Thus, while L_{N} does not impact lifetime (HT effectiveness), it does impact X-ray inspection (HT stealthiness). Second, once L_{N} becomes larger than the microbumps ($25\,\mu m$), the EM-based HT becomes exposed around the microbumps in angles like 72° and 63°. In contrast, as long as L_{N} remains significantly smaller than the microbumps, the HT is only detectable once it emerges from the shadow, like seen for 80° exposure in Fig. 7. This exposure effect increases as L_{N} exceeds the microbumps' width, due to weakening of X-ray beam scatter around the microbumps.

*2) **Impact of** W_{N}:* Here, we set L_{N} to a constant value of 5 µm. For each possible value D_{u}, we vary W_{N} between 1 µm and 39 µm and track the resulting HQM. Related results are also shown in Fig. 10 and discussed next.

First, smaller D_{u} values result in higher HQM. Second, for constant D_{u} values, HQM generally increases with W_{N}. For counterexamples, projections that exposed the HT for W_{N}= 1 µm and D_{u} = 7.5 µm are only found at angles 81°, 90°, 99°, and 270°, out of all the 40 projections. In general, the exposure at 90° (and 270°) is related to the ratio of W_{N} to the RDL width. Here, when $W_{\mathrm{N}} \geq 20$ µm (i.e., half of the RDL width), the EM-based HT is no longer detectable at 90°.

*3) **Takeaways**:* Recall from Fig. 9 that stronger HTs arise from smaller W_{N}. Combining this earlier insight with the ones just discussed above, we find an inverse relationship between the strength/effectiveness and the stealthiness of the EM-based HT. Importantly, however, even the lowest recorded HQM stands notably high at 88%, confirming that the proposed HT remains concealed in most cases.

C. Advanced Trojan Design

The X-ray simulation results showed that the wire edges are particularly sensitive to detection. Thus, to further advance the proposed EM-based HT, we explore how we can keep the edges intact but still efficiently decrease lifetime. As shown in Fig. 11, instead of maliciously manipulating the wire from the edges, we assume cutting a hole into the center. Importantly, we find that the EM results remain the same if the two narrow portions in this new geometry have a width of $W_{\mathrm{N}}/2$ each.

To demonstrate the superior stealthiness of the advanced geometry, we devise a HT design with the following parameters: $W_{\mathrm{N}} = 14$ µm, $D_{\mathrm{u}} = 7.5$ µm, and $L_{\mathrm{N}} = 5$ µm. As before, we vary the angle and examine 40 projections. Representative projections are shown in Fig. 12 and discussed next.

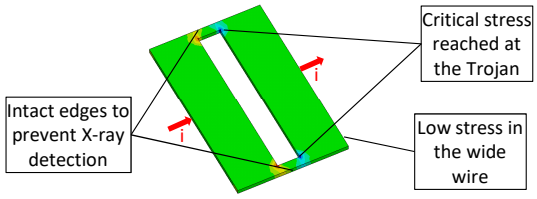

Fig. 11: Advanced geometry/topology for EM-based HT. The same simulations parameters as in Fig. 8 are used here. The results for stress, MTTF, and temperature remain all the same.

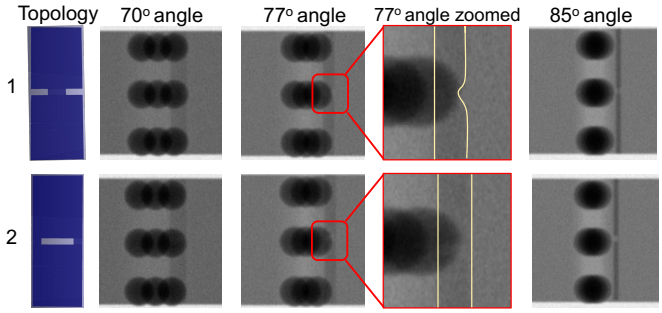

Fig. 12: Impact of different geometries/topologies on stealthiness of EM-based HT against X-ray inspection.

At most angles, like shown for 70° in Fig. 12, there is no observable difference for the X-ray inspection. At some steeper angles, like 85°, there are some differences, whereas the HTs remain exposed in both topologies regardless. Notably, at few specific angles, like 77°, the HT remains completely concealed in the advanced topology but exposed in the initial topology. This is because, for the initial topology, detection occurs at the cut edge of the malicious modification of the RDL, which is subsequently void of Cu, creating a dent shape in the X-ray image. In the advanced topology, in contrast, the X-ray image at the edge of the HT-infested section of the RDL appears as dense as the rest of the RDL, whereas the actual hole in the middle remains "lurking in the shadows" of the microbumps.

VI. Discussion and Conclusion

Our first-of-its-kind study confirms that EM-based HTs are a realistic threat to modern circuits and systems built on advanced packages. We demonstrate that, by subtly narrowing wires in an interposer's RDL, attackers can create time-delayed attacks on the critical PDN that remain stealthy against X-ray inspection. Remarkably, such HTs can be realized by various adversaries in the supply-chain, e.g., via post-manufacturing FIB edits by malicious system integrators.

Our work quantifies some fundamental trade-offs: a highly effective HT with large cuts into the wire can reduce MTTF by over an order of magnitude, but has a limited yet still very high stealthiness rate of ≈90% against thorough X-ray inspection (with idealized settings for minimized noise and scattering, representing a best-case detection scenario). We further propose an advanced HT topology that is even more resilient to edge-based detection at certain angles. In that sense, future work should explore machine learning to advance detection of such HTs, especially with noise and scattering.

Grounded in practical settings, our work supports further discussion. For example, the HTs' impact on IR-drop is relevant for stealthiness during testing and for attack effectiveness. For a typical PDN segment of $100\,\mu\text{m}$ length (Tab. I), a HT as in Fig. 8 and with $W_\text{N} = 10\,\mu\text{m}$ and $L_\text{N} = 5\,\mu\text{m}$, increases the resistance of the segment by 10 %. Importantly, the PDN's redundant mesh structure limits the initial increase in IR-drop to only 0.10 % on average and 1.02 % at most,[4] rendering the HT stealthy. For the same HT and PDN, once the wire under attack fails, the IR-drop increases by 2.15 % on average and 19.03 % at most, which may well suffice for glitching or DoS attacks [25], [29]. Note that the limited initial increase in IR-drop may also allow adversaries to scale up the number of HT instances and tune their locations as needed for more powerful and/or targeted attacks, while still remaining stealthy.[5]

Our findings underscore that hiding EM-based HTs in an interposer's RDL is alarmingly robust. Consequently, assurance cannot be guaranteed by end-of-line inspection alone, but requires further efforts as follows. *Provision for high-resolution X-ray inspection of the interposer individually.* Doing so would remove the option for HTs to remain "lurking in the shadows" in the first place, but requires an additional inspection step and, more importantly, access to a trusted system integrator. *Explore new DFI approaches.* For example, interposer routing could establish keep-out zones under microbumps in general, or support more sophisticated heuristics to avoid routing of high-current wires "in the shadows" based on X-ray inspection-informed geometry and spacing constraints. Naturally, such DFI-enhanced routing should be easier to inspect and could be applied for regular in-line inspection of the fully integrated system, thereby also providing assurance against malicious system integrators.

ACKNOWLEDGMENTS

This work was supported in parts by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Grant No. 525041614, the U.S. National Science Foundation (NSF) under Grant No. 2143591, and the Center for Cybersecurity, New York University Abu Dhabi, UAE. We thank the reviewers for their constructive feedback.

REFERENCES

[1] Y. Li *et al.*, "The applications of simulation and artificial intelligence in advanced packaging," in *IPFA*, 2024, pp. 1–5.
[2] W. Chein *et al.*, "Advancements in metrology for advanced semiconductor packaging," in *Proc. SPIE*, 2024, p. 129970R.

[4]This is based on first-order SPICE simulations exploring all PDN segments for HT insertion, while assuming the same typical $T_0 = 60\,^\circ\text{C}$, nominal sheet resistivity, and power sources/sinks as defined and arranged in the *CoWoS* PDN [34]. Future work should consider full parameter modeling (R, L, G, and C), and also cover various temperature corners, to more thoroughly assess IR-drop and bound the resulting stealthiness and effectiveness of the HTs.

[5]In fact, for two instances of the same HT incorporated, the initial increase in IR-drop is still similar, namely 0.10 % on average and 1.68% at most. Once the two attacked wires fail, the IR-drop increases more significantly, namely by 37.27 % at most (and by 2.47 % on average), confirming the scalability of the HTs. Furthermore, since the HT-induced changes in resistivity impact the current flow in the PDN right away, a detailed study of potentially premature EM-based failures for multiple HTs arranged nearby vs. afar, considering all currents and coupled Joule heating, should be the scope of future work.

[3] D. Bernard, "X-ray advances in support of advanced packaging – today and tomorrow," *IMAPSource Proc.*, vol. 2018, pp. 409–414, 2018.
[4] K. Yahyaei *et al.*, "From design to inspection: Can inspection-aware design enhance reliability in advanced packaging?" in *VTS*, 2025.
[5] J. Xu *et al.*, "An assessment of electromigration in 2.5d packaging," in *ECTC*, 2019, pp. 2150–2155.
[6] J. Lienig *et al.*, *Fundamentals of Electromigration-Aware Integrated Circuit Design*, 2nd ed. Springer, 2025.
[7] A. Roy *et al.*, "Applications and challenges of AI in PCB x-ray inspection: A comprehensive study," *JETC*, vol. 21, 2024.
[8] N. Varshney *et al.*, "Challenges and opportunities in non-destructive characterization of stacked IC packaging: insights from SAM and 3D x-ray analysis," 2024, p. 76.
[9] S. Lau *et al.*, "Decoupling sub-micron resolution and speed from sample size in 3D x-ray imaging," in *IPFA*, 2022, pp. 1–6.
[10] B. Peterson *et al.*, "Optimizing x-ray inspection for advanced packaging applications," *Int. Symp. Microelectron.*, vol. 2020, pp. 165–168, 2020.
[11] M. S. M. Khan *et al.*, "CMx-ray: An x-ray compatibility metric for advanced packages to facilitate design-for-inspection," in *PAINE*, 2023.
[12] K. Yahyaei *et al.*, "Design guidelines for in-line x-ray inspection in advanced packaging technology: A CoWoS case study," *IMAPS*, 2025.
[13] ——, "X-ADAPT: AI-driven design-based strategy to address x-ray compatibility challenges in advanced packaging metrology," in *SPIE Adv. Litho. + Patterning*, 2025, p. 134264C.
[14] J. R. Black, "Electromigration – a brief survey and some recent results," *IEEE Trans. Electron Devices*, vol. 16, no. 4, pp. 338–347, 1969.
[15] S. Rothe *et al.*, "Temperature-aware stress-based migration modeling in IC design: Moving from theory to practice," *AEU*, vol. 200, 2025.
[16] ——, "Stress-based electromigration modeling in IC design: Moving from theory to practice," in *SMACD*, 2024.
[17] S. Rothe. (2024) Simulation scripts used in this work. [Online]. Available: https://github.com/IFTE-EDA/EMinPractice
[18] L. Peters. (2024) Electromigration concerns grow in advanced packages. Semiconductor Engineering.
[19] C. Liang *et al.*, "Electromigration reliability of advanced high-density fan-out packaging with fine-pitch 2-/2-um l/s cu redistribution lines," *TCPMT*, vol. 10, no. 9, pp. 1438–1445, 2020.
[20] Y. Wang *et al.*, "Research on the reliability of advanced packaging under multi-field coupling: A review," *Micromachines*, vol. 15, no. 4, 2024.
[21] J. Pak *et al.*, "Modeling of electromigration in through-silicon-via based 3d IC," 2011, pp. 1420–1427.
[22] M. Muehlberghuber *et al.*, "Red team vs. blue team hardware Trojan analysis: Detection of a hardware Trojan on an actual ASIC," in *HASP*.
[23] K. Yang *et al.*, "A2: Analog malicious hardware," in *SP*, 2016.
[24] S. Ghandali *et al.*, "Side-channel hardware Trojan for provably-secure SCA-protected implementations," *TVLSI*, vol. 28, no. 6, 2020.
[25] J. Knechtel, "Hardware security for and beyond CMOS technology," in *ISPD*, 2021.
[26] J. Knechtel *et al.*, "Trojan insertion versus layout defenses for modern ICs: Red-versus-blue teaming in a competitive community effort," *TCHES*, vol. 2025, no. 1, pp. 37–77, 2024.
[27] J. Lienig *et al.*, "Toward security closure in the face of reliability effects," in *ICCAD*, 2021, pp. 1–9.
[28] T. Perez *et al.*, "Side-channel Trojan insertion - a practical foundry-side attack via ECO," in *ISCAS*, 2021, pp. 1–5.
[29] H. Zhu *et al.*, "PCBench: Benchmarking of board-level hardware attacks and trojans," in *ASP-DAC*, 2021, p. 396–401.
[30] J. Harrison *et al.*, "On malicious implants in PCBs throughout the supply chain," *Integration*, vol. 79, pp. 12–22, 2021.
[31] C. Cook *et al.*, "Reliability based hardware trojan design using physics-based electromigration models," *Integration*, vol. 66, pp. 9–15, 2019.
[32] C. Boit *et al.*, "From IC debug to hardware security risk: The power of backside access and optical interaction," in *IPFA*, 2016.
[33] E. Puschner *et al.*, "Red team vs. blue team: A real-world hardware Trojan detection case study across four modern CMOS technology generations," in *SP*, 2023, pp. 763–781.
[34] J. Kim *et al.*, "Chiplet/interposer co-design for power delivery network optimization in heterogeneous 2.5-d ICs," *TCPMT*, vol. 11, no. 12, 2021.
[35] S. Rothe *et al.*, "Combined modeling of electromigration, thermal and stress migration in AC interconnect lines," in *ISPD*, 2023, p. 107–114.
[36] D. Neffati *et al.*, "Novi-sim: A fast x-ray tomography simulation software for laboratory and synchrotron systems to generate training databases for deep learning applications," in *iCT*, vol. 28, no. 3, 2023.