Design of an RF-Triggered Hardware Trojan with a Layout-Matched Golden Model via HT-First Place-and-Route

Seong-Jin Chang[1], Dae-Hyeon Lee[2] and Junghee Lee[3]
School of Cyber Security, Korea University
E-mail : [1]use06040@korea.ac.kr

Abstract - **Hardware Trojans (HTs) are malicious circuits that remain dormant under normal operation and activate only when a specific trigger condition is met, making them difficult to detect through conventional testing. This paper presents the design and silicon-level fabrication of an RF-triggered HT integrated into an AES-128 ASIC under a realistic foundry-level supply-chain threat model. The proposed design consists of two key components: (1) an on-chip loop antenna with T-matching network embedded in the M6 metal layer, targeting 5.8 GHz CW excitation, and (2) an HT-first Place & Route (P&R) strategy that preserves the placement and routing of the non-HT logic between the HT-inserted chip and the golden model (GM), so that the two variants are structurally as similar as possible for a controlled comparison. Upon receiving the 5.8 GHz trigger signal, the HT asserts a persistent reset forcing the AES-128 output to zero, causing denial of service (DoS). Both the HT-inserted chip and GM were fabricated simultaneously in a 180-nm process and packaged in identical QFP-64 packages, enabling controlled comparison under identical conditions.**

Keywords—**Hardware Trojan, on-chip antenna, RF Trigger.**

I. INTRODUCTION

The threat of Hardware Trojans (HTs) has intensified with the globalization of hardware supply chains.[1] To contain rising production costs, the industry has embraced a cross-border division of labor in which design, manufacturing, EDA tool development, production equipment, testing, and packaging are handled by different entities.[2] As hardware shifts from a replaceable component to a core strategic technology, economic interests increasingly intersect with political and security concerns. In particular, when adversarial nations participate in outsourcing, mutual distrust arises and products designed or manufactured by an adversary may be suspected of containing HTs[3]-[6].

HTs are malicious circuit modifications that remain dormant during normal operation and activate only under specific trigger conditions. Because those trigger conditions are deliberately rare and the HT logic uses very little silicon area with minimal switching activity, accidental activation during logic testing is unlikely, and post-silicon detection becomes challenging and costly [7]. The risk is particularly high in security-critical platforms, where a malfunction, denial of service (DoS), or information leakage can lead to severe consequences [8],[9].

Among various HT trigger mechanisms, RF-based triggering presents a particularly stealthy threat: an on-chip antenna embedded in the metal layers can receive an externally transmitted signal to activate the HT; because this activation condition is never exercised by standard functional or scan-based production tests, the HT remains dormant and undetected during testing 10].Despite growing concerns, silicon-level experimental validation of RF-triggered HTs remains scarce, leaving open questions about practical feasibility and design constraints at the chip level.

In this work, we address this gap by presenting the design and fabrication of an RF-triggered HT integrated into an AES-128 ASIC. The proposed design makes the following contributions:

(1) On-chip loop antenna with T-matching network: A compact loop antenna is embedded in the M6 metal layer, designed to receive 5.8 GHz CW excitation. The T-matching network achieves 50 Ω input impedance at a center frequency of 5.85 GHz, with a gain of −13.8 dBi and a size reduced to 1/16 of a standard loop antenna design.

(2) HT-first Place & Route strategy: To preserve the layout of the non-HT logic across both variants, the HT is placed and routed first as an independent block. The golden model (GM) layout is then derived by removing HT cells while preserving all non-HT placement and routing, so that the non-HT logic is identically placed and routed across the entire design in both variants, confining the layout difference to the small HT block and the antenna.

(3) Silicon-level fabrication and validation: Both the HT-inserted chip and GM are fabricated simultaneously in a 180-nm process and packaged in identical QFP-64 packages, enabling controlled side-by-side comparison under identical conditions.

II. BACKGROUND

A HT is primarily composed of a Trigger circuit and a Payload circuit, as illustrated in Figure 1 [7]. Since an HT

a. Corresponding author: j_lee@korea.ac.kr
Manuscript Received Jun. 24, 2026, Revised Sep. 16, 2026, Accepted Sep. 17, 2026

This is an Open Access article distributed under the terms of the Creative Commons Attribution Non-Commercial License (http://creativecommons.org/licenses/by-nc/4.0) which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.

must remain hidden under normal conditions, it only activates when specific conditions are met [8]. The Trigger circuit detects whether these conditions have been satisfied, and once activated, the Payload circuit executes the intended malicious operation. Depending on its purpose, an HT can either cause system malfunctions or leak sensitive information [9].

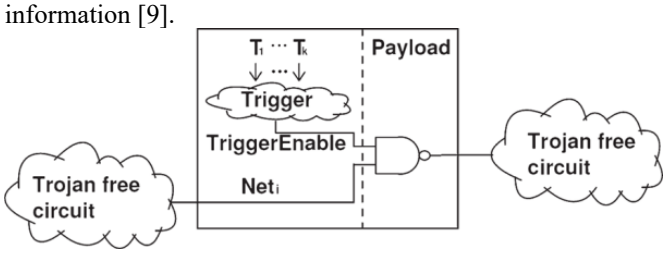

Fig. 1. Typical structure of HT.

HTs can be classified by their physical characteristics, activation method (trigger), operation (payload), and infiltration stage [10]; among these, RF-based external triggers are particularly hard to expose by testing, since the activation condition — reception of a specific RF signal — is never exercised by standard functional or scan-based production tests, so the HT remains dormant and undetected during test. Prior silicon-demonstrated wireless/RF HTs have largely used the RF channel as a leakage path: for example, the secret key of a wireless cryptographic IC is exfiltrated through the margins of a UWB or WLAN transmitter [11], [12], and analog/RF front-ends already present in the host have been exploited to modulate leaked information [13]. These works assume a host that already contains a legitimate RF transmitter and use RF for the payload. In contrast, the present work uses an external RF signal as the trigger for an otherwise non-RF host: a dedicated antenna is embedded in a plain AES-128 ASIC so that an external CW signal activates a DoS payload. To our knowledge, silicon-level validation of such RF-triggered activation in a non-RF host remains scarce.

In this study, we focus on a DoS payload scenario targeting a cryptographic module, under an untrusted foundry threat model in which a foundry-level adversary inserts a compact on-chip antenna during fabrication. The following sections describe the design and implementation of this RF-triggered HT.

III. DESIGN METHODOLOGY

In this study, we implement an RF-triggered HT targeting an AES-128 cryptographic module. The HT consists of two components: a trigger circuit and a DoS payload circuit. The payload is based on the AES-T1800 benchmark provided by Trust-HUB [14], which forces a persistent reset of the AES-128 output upon activation.

Unlike the original AES-T1800 benchmark, which uses a specific 128-bit plaintext pattern as its trigger, we replace the trigger mechanism with an RF-based circuit, enabling activation via an externally transmitted 5.8 GHz CW signal. This replacement makes the HT significantly stealthier, as no specific input pattern needs to be applied to activate it.

TABLE 1. HT to Be Used in the Experiment.

Benchmark	Classification
AES128	Golden Model.
AES128-T1800	Denial of Service.

AES128: This module serves as the golden model, meaning it does not contain any HTs and is used for comparative analysis with other modules. The benchmark is configured to operate as shown in Figure 2. The data generator provides the ciphertext to the ASIC, which then decrypts it and outputs the decrypted result via the serial port.

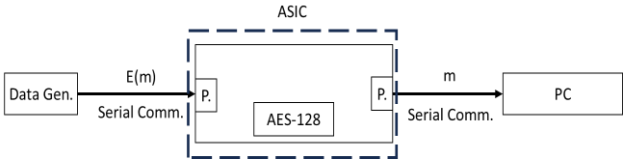

Fig. 2. Golden model scenario.

- Data Gen: Generates encrypted data and transmits it to the ASIC.
- ASIC: Performs AES128 decryption.
- P: Serial port (UART communication).
- m: Plaintext (input).
- E(): AES-128 encryption.
- E(m): Ciphertext.

AES-T1800: In the original benchmark, this HT monitors the 128-bit input of the AES circuit and activates its payload upon detecting a specific 128-bit plaintext, leading to a DoS attack. In this study, we retain only the DoS payload and replace its input-based trigger with an RF-based trigger circuit.

When the HT is activated by the RF trigger, the AES-128 output is forced to zero, causing DoS.

The RF trigger circuit consists of an on-chip loop antenna with a T-matching network, a rectifier, and an op-amp. The antenna receives a 5.8 GHz CW signal at a specific frequency from an external source to activate the HT.

Figure 3 shows the antenna used in this study. The antenna was embedded in the M6 layer to receive a CW signal at the designated frequency. When the signal is received, a 1-bit trigger value switches from 0 to 1, activating the HT payload, which prevents the AES-128 module from functioning.

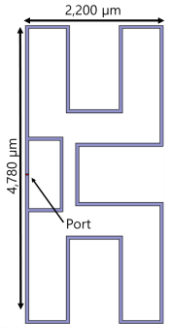

Fig. 3. Small loop antenna with T-matching.

The simulated antenna characteristics are as follows:

- Layer: M6
- Small loop antenna with T-matching
- Size: 2,200 x 4,780 μm2
- Size reduction: 1/16
- Differential feeding
- Input impedance: 50 Ω
- Center frequency: 5.85 GHz
- Gain: -13.8 dBi

The T-matching network achieves the 50 Ω input impedance to minimize signal loss at the target frequency. The rectifier converts the received RF signal into a DC voltage; a four-stage cross-connected differential rectifier based on the DB 180 nm PDK was adopted, using MIM capacitors of 1.05 pF (width: 20 μm, length: 30 μm). Simulation results show that an input of 5.8 GHz at 133 mV produces a DC output converging to 2.2 V, which is sufficient to drive the op-amp and assert the reset signal.

Figure 4 illustrates the schematic representation of the HT implemented in this study. The antenna shown in Figure 3 is embedded into the chip, allowing it to receive a CW signal at the designated frequency from an external signal generator. When the embedded antenna receives this signal, the reset signal remains continuously activated, preventing the AES-128 module from operating properly and disrupting the decryption process.

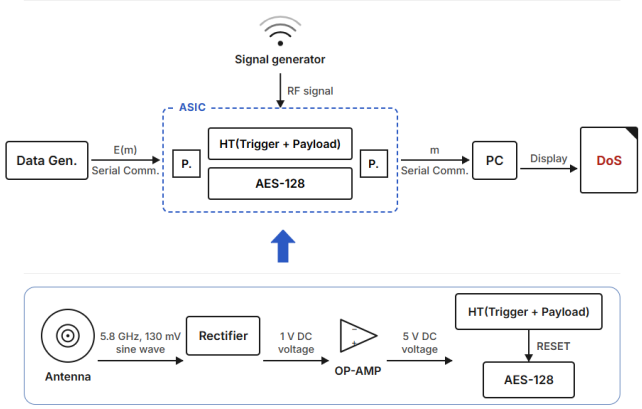

Fig. 4. HT scenario.

A. IC Chip Design with Hardware Trojan

The placement of an HT within a chip significantly affects its detectability. To keep the non-HT logic layout-matched between the two variants, we adopt an HT-first Place & Route (P&R) strategy, described below.

One major challenge in implementing HTs within a circuit is that HTs are defined at the RTL level, requiring modifications to the HDL source code of the original AES circuit. When the modified source code undergoes standard compilation, placement, and routing, the addition of the HT causes the EDA tool to significantly alter the placement and routing of the entire circuit [15]. These extensive changes make HT detection easier, regardless of the actual size or activity of the inserted HT [16].

To make HT detection more difficult, we adopt the following approach. First, we compile, place, and route the circuit with the HT present. After completing these processes, we remove the HT's logic elements and connections to derive an HT-free circuit. This derived circuit is referred to as the Golden Model (GM) and shares nearly identical non-HT placement and routing with the HT-inserted chip, minimizing layout-level distinguishers between the two.

The modularized HT is then inserted into the available empty space within the GM layout while maintaining extremely short connections to the original circuit, producing the final HT-inserted chip. This realistic scenario reflects how an HT could be introduced into a finalized layout in a practical hardware environment.

IV. RESULTS AND DISCUSSION

A. ASIC Result

Following the HT-first Place & Route (P&R) strategy described in Section III, the HT layout was generated independently and prioritized during P&R, while all non-HT cells were placed identically across both the HT-inserted layout and the Golden Layout.

As shown in Figure 5, this strategy produces an HT-inserted design that closely resembles the Golden Layout, making detection through traditional placement analysis significantly more challenging.

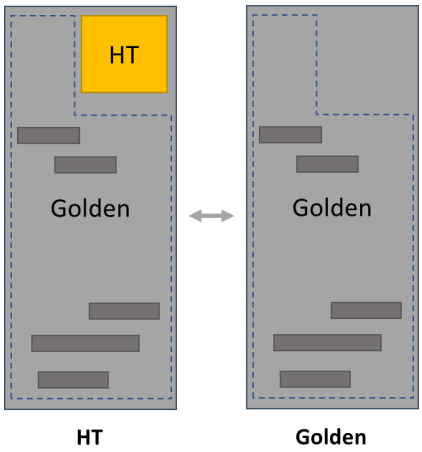

Fig. 5. Schematic representation of GM and HT design.

Using the EDA tool, a GDS file was generated, as shown in Figure 6, and the actual die was fabricated through the DB Hitek 180nm BCDMOS process, as shown in Figure 7.

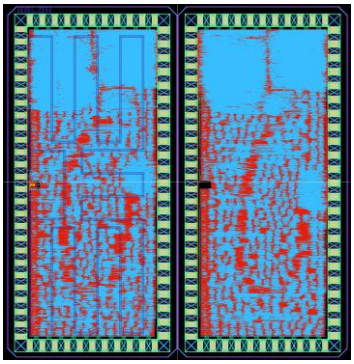

Fig. 6. GDS layout designed in this study

The fabricated die shown in Figure 7 was packaged into a 64-pin Quad Flat Package (QFP) to create an operational environment where the chip could be tested under real-world conditions, as shown in Figure 8.

Each packaged IC underwent functional testing to verify correct operation by applying input signals and monitoring output responses.

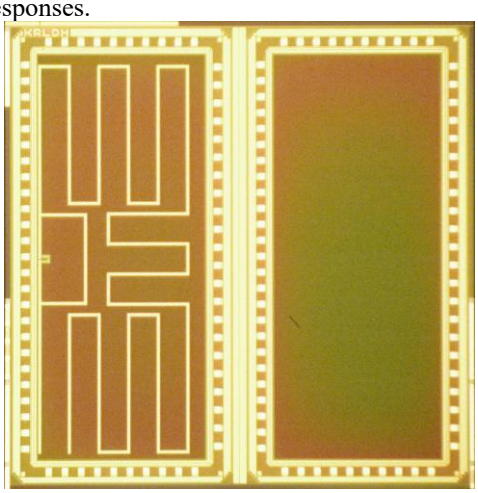

Fig. 7. Die fabricated through the DB HiTek 180nm process.

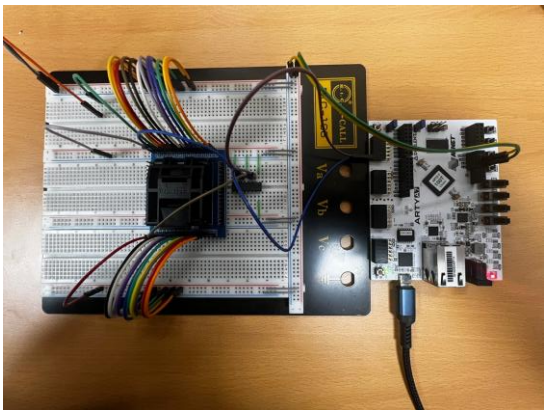

Fig. 8. Operational verification environment for the fabricated chip.

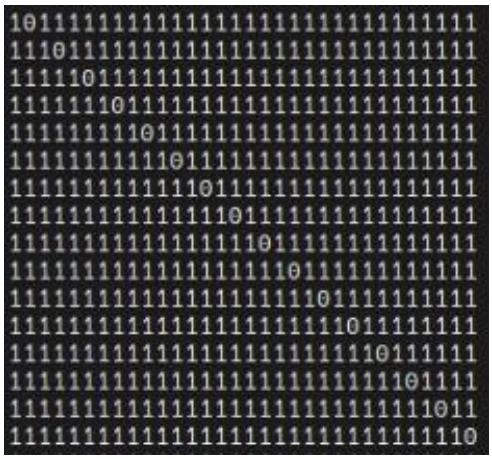

Fig. 9. Normal output results of the chip.

Through these functionality tests, we confirmed that the fabricated chip was operating correctly. If the chip functions as intended, its output should match the expected results, as illustrated in Figure 9. This verification step is crucial in confirming that the manufacturing process was successful and that both the HT-free reference chip (GM) and HT-inserted chip function as designed.

B. Experimental Environment

Various equipment was used to generate, transmit, and verify the 5.8 GHz CW signal and its interaction with the HT-embedded ASIC.

A signal generator was used to generate a stable 5.8GHz CW signal, ensuring precise frequency control for the experiment. For this purpose, the Anritsu MG36221A as shown in Figure 10 was employed, providing high-frequency stability and accurate signal output.

Fig. 10. Signal generator.

To transmit the generated 5.8 GHz CW signal, an electromagnetic compatibility (EMC) probe was utilized. The BEEHIVE ELECTRONICS 100 series EMC probe (Model: 100B, small loop) shown in Figure 11 is a near-field magnetic-field (H-field) loop probe with a loop diameter of 0.15 in. Among several probe types evaluated, the 100B most effectively coupled the 5.8 GHz CW signal to the on-chip loop antenna under near-field conditions, and was therefore selected as the transmit probe. As a magnetic loop probe, it generates a localized field around its tip rather than radiating energy into the far field, which is well matched to the H-field-based on-chip loop antenna.

Fig. 11. transmit probe.

To ensure that the generated 5.8GHz CW signal was properly transmitted and received, several verification tools were employed:

- Near-Field Probe XF1 Set (Model: XF-R 400-1 H-Field Probe), capable of detecting electromagnetic signals in the 30 MHz to 6 GHz range, was used to measure the presence and strength of the CW signal.
- HackRF One, a software-defined radio (SDR) platform, was used to analyze the frequency

spectrum and signal characteristics of the transmitted 5.8GHz CW signal.

- SDR++, a software-based radio receiver application, was employed to monitor and visualize the 5.8GHz CW signal transmission, ensuring that the signal was correctly generated and reaching the intended ASIC target.

C. Results

The HT-embedded ASIC includes an integrated antenna; when it receives a 5.8 GHz CW signal, the trigger activates the payload, preventing normal operation.

The experiment proceeded as follows: a 5.8 GHz CW signal was generated, its power level (dBm) verified, and transmitted via the probe placed on the ASIC surface to observe HT activation, after which the probe distance was varied to analyze its effect on activation.

The experiment successfully generated and transmitted the 5.8 GHz CW signal at the measured power level. When the probe was positioned directly on the ASIC surface, HT activation was observed; when the probe was moved away, activation did not occur, indicating strong dependence on proximity to the chip.

These results confirm that HT activation is highly sensitive to the positioning of the CW signal source, with reliable activation observed only under near-field coupling. The factors contributing to the limited activation distance are analyzed in detail in the Discussion.

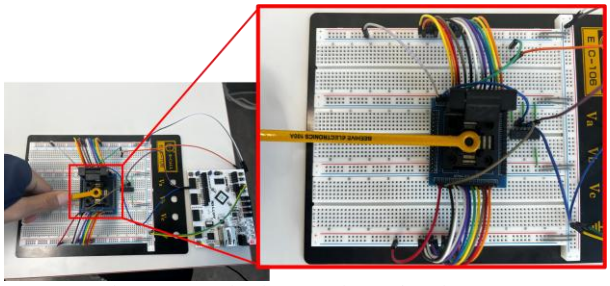

Fig. 12. HT activation experimental environment.

The experimental setup was configured as shown in Figure 12.

For the experiment, the signal generator was configured to operate at a frequency of 5.8 GHz with an output power of 30 dBm. This setting was essential to ensure the generation of a sufficiently strong signal capable of activating the HT embedded within the ASIC.

To successfully trigger the HT, a voltage of 130 mV was required at the circuit level. This corresponds to a signal power of approximately -7.7 dBm, meaning that a relatively weak signal could theoretically activate the HT if properly coupled with the embedded antenna. However, in practice, due to transmission losses and the near-field coupling characteristics of the probe, a much stronger signal—around 30 dBm—was needed to ensure consistent HT activation. This indicates that the HT requires a high-power signal source to reliably function.

As shown in Figure 13, the SDR++ software-defined radio platform confirmed that the signal generator correctly emitted the 5.8 GHz signal at the intended power level.

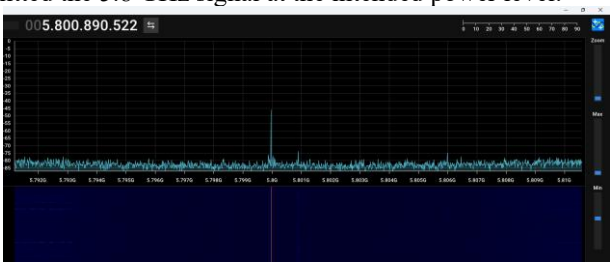

Fig. 13. 5.8GHz signal verification.

Finally, the ASIC output was observed under 5.8 GHz excitation. Whereas it normally outputs its intended functional values, the output became locked at 0 when the CW signal was applied, confirming successful HT activation, as shown in Figure 14.

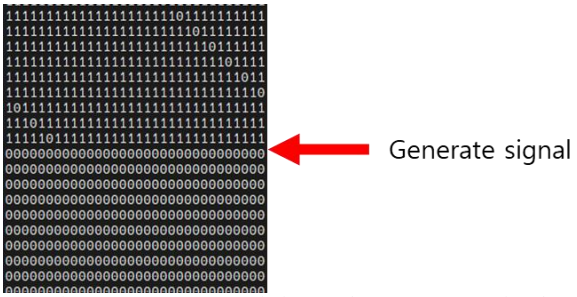

Fig. 14. ASIC output variation results upon 5.8GHz signal transmission.

The antenna and rectifier were characterized by simulation; the silicon-level validation reported here is at the system level (end-to-end RF-triggered DoS under measured near-field excitation).

D. Discussion

Only 42 out of 68 HT ASICs were activated by the CW signal, and activation was possible only under near-field contact with the chip surface. We attribute the fraction of chips that did not activate at all primarily to insufficient RF-to-DC conversion at the trigger — the electrically small on-chip antenna, combined with an insufficiently robust trigger threshold, left too little margin to activate reliably across chips. We attribute this limited activation distance to three factors. First, the transmit probe is a near-field magnetic loop probe rather than a radiating antenna; it generates a field only in its immediate vicinity, similar to NFC, and cannot deliver sufficient power beyond a short distance. Second, polarization mismatch between the transmit antenna and the linearly polarized on-chip antenna reduces coupling efficiency, requiring careful alignment. Third, the doping of the wafer substrate beneath the antenna, which was not accounted for in the antenna design, can degrade efficiency; a low-conductivity process such as silicon-on-insulator (SOI) or metal patterning to raise the effective surface impedance could mitigate this in future designs. Building on this analysis, future work will investigate remote activation using directional radiating antennas (e.g., horn or log-periodic) with proper polarization alignment, and will refine the on-chip antenna and substrate design to improve

coupling efficiency. Furthermore, the co-fabricated, structurally near-identical GM/HT pair is intended to serve as a controlled testbed for HT-detection studies, including side-channel-based approaches.

V. CONCLUSION

This study presented the design and silicon-level fabrication of an RF-triggered HT integrated into an AES-128 ASIC. The proposed design combines an on-chip loop antenna with a T-matching network, targeting 5.8 GHz CW excitation, and an HT-first Place & Route strategy that preserves the layout of the non-HT logic between the HT-inserted chip and the golden model, keeping the two variants layout-matched. Both variants were fabricated together in a 180-nm process under identical conditions. Experimental evaluation confirmed HT activation under near-field CW excitation, validating the feasibility of the proposed design. The observed dependence on near-field coupling was analyzed in terms of probe characteristics, polarization matching, and substrate effects, providing concrete design guidelines for future RF-triggered HT research and for developing corresponding detection and mitigation strategies.

ACKNOWLEDGMENT

This work was supported by the Future Challenge Defense Technology Research and Development Program through the Agency for Defense Development(ADD) grant funded by the Defense Acquisition Program Administration (DAPA) in 2025 (No. UG243060TD). The chip fabrication and EDA tool were support ed by the IC Design Education Center(IDEC), Korea.

REFERENCES

[1] H. Li, Q. Liu, and J. Zhang, “A survey of hardware Trojan threat and defense,” *Integration, the VLSI Journal*, vol. 55, pp. 426–437, 2016.

[2] S. Mitra, H.S.P. Wong, S. Wong, The Trojan-proof chip, *Spectr. IEEE* 52 (2) (2015) 46–51

[3] N. Jacob, D. Merli, J. Heyszl, G. Sigl, Hardware Trojans: current challenges and approaches, Comput. Digit. Techn. IET 8 (6) (2014) 264–273.

[4] Y. Shiyanovskii, F. Wolff, A. Rajendran, C. Papachristou, D. Weyer, W. Clay, Process reliability based Trojans through NBTI and HCI effects, In: NASA/ESA Conference on Adaptive Hardware and Systems (AHS), 2010, pp. 215–222.

[5] G.T. Becker, F. Regazzoni, C. Paar, W.P. Burleson, Stealthy dopant-level hardware Trojans, In: Lecture Notes in Computer Science, vol. 4, no. 1, 2013, pp. 197-214.

[6] G. Qu, Y. Yuan, Design things for the internet of things—an EDA perspective, In: IEEE/ACM International Conference on Computer-Aided Design (ICCAD), 2014, pp. 411–416.

[7] S. Dupuis, P.S. Ba, G. Di Natale, M.L. Flottes, B. Rouzeyre, A novel hardware logic encryption technique for thwarting illegal overproduction and hardware Trojans, In: *IEEE 20th International On-Line Testing Symposium (IOLTS)*, 2014, pp. 49–54.

[8] S. Bhunia, M. S. Hsiao, M. Banga, and S. Narasimhan, “Hardware Trojan attack: Threat analysis and countermeasures,” *Proc. IEEE*, vol. 102, no. 8, pp. 1229–1247, Aug. 2014.

[9] R. S. Chakraborty, S. Narasimhan, and S. Bhunia, “Hardware Trojan: Threats and emerging solutions,” in *Proc. IEEE Int. High-Level Design Validation and Test Workshop (HLDVT)*, San Francisco, CA, USA, 2009, pp. 166–171.

[10] 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, Jan.–Feb. 2010.

[11] Y. Liu, Y. Jin, and Y. Makris, “Hardware Trojans in wireless cryptographic ICs: Silicon demonstration & detection method evaluation,” in Proc. IEEE/ACM Int. Conf. Comput.-Aided Design (ICCAD), 2013, pp. 399–404.

[12] Y. Liu, Y. Jin, A. Nosratinia, and Y. Makris, “Silicon demonstration of hardware Trojan design and detection in wireless cryptographic ICs,” IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 25, no. 4, pp. 1506–1519, 2017.

[13] K. S. Subramani, N. Helal, A. Antonopoulos, A. Nosratinia, and Y. Makris, “Amplitude-modulating analog/RF hardware Trojans in wireless networks: Risks and remedies,” IEEE Trans. Inf. Forensics Security, vol. 15, pp. 3497–3510, 2020.

[14] M. Tehranipoor, R. Karri, F. Koushanfar, and M. Potkonjak, “Trust-Hub,” [Online]. Available: https://www.trust-hub.org/

[15] M. Pérez and S. Pagliarini, “Hardware Trojan insertion in finalized layouts: From methodology to a silicon demonstration,” *IEEE Trans. Computer-Aided Design of Integrated Circuits and Systems*, vol. 42, no. 10, pp. 3289–3302, Oct. 2023.

[16] O. Soll, T. Korak, M. Muehlberghuber, M. Hutter, EM-based detection of hardware Trojans on FPGAs, In: IEEE International Symposium on HardwareOriented Security and Trust (HOST), 2014, pp. 84–87.

Seongjin Chang received the B.S. degree in Department of Cyber Defense from Korea University, Seoul, Korea, in 2025

His research interests include side-channel analysis using electromagnetic and backscattering signals. In particular, he is currently conducting research on hardware security with a focus on side-channel attack methodologies and detection strategies.

Daehyeon Lee received the M.S. degree in the Department of Cybersecurity from Korea University, Seoul, Korea, in 2020, where he is currently pursuing the Ph.D. degree in the Department of Cybersecurity. His current research interests focus on architecture security and hardware trojan detection. His research interests include computer architecture, microprocessor and computer system design, secure design or hardware-assisted security of processors, non-volatile memory, storage, and hardware trojan detection.

Junghee Lee (Member, IEEE) received the B.S. and M.S. degrees in computer engineering from Seoul National University, in 2000 and 2003, respectively, and the Ph.D. degree in electrical and computer engineering from the Georgia Institute of Technology, in 2013. He is currently with the School of Cybersecurity, Korea University, since 2019. From 2003 to 2008, he worked at Samsung Electronics on electronic system level design of mobile system-on-chip. From 2014 to 2019, he was with the Department of Electrical and Computer Engineering, University of Texas at San Antonio, as an Assistant Professor. His research interests include secure design or hardware-assisted security of processor, non-volatile memory, storage, and dedicated hardware.