International Journal of High Speed Electronics and Systems
Vol. 32, Nos. 2–4 (2023) 2350015 (17 pages)

DOI: 10.1142/S0129156423500155

World Scientific
www.worldscientific.com

PCB Security Modules for Reverse-Engineering Resistant Design

Shuai Chen* and Lei Wang

Department of Electrical and Computer Engineering,
University of Connecticut, Storrs, CT 06269, USA
**shuai.chen@uconn.edu*

Received 15 April 2023
Accepted 28 May 2023

As the crisis of confidence and trust in overseas foundries arises, the industry and academic community are paying increasing attention to Printed Circuit Board (PCB) security. PCB, the backbone of any electronic system hardware, always draws attackers' attention as it carries system and design information. Numerous ways of PCB tampering (e.g., adding/replacing a component, eavesdropping on a trace and bypassing a connection) can lead to more severe problems, such as Intellectual Property (IP) violation, password leaking, the Internet of Things (IoT) attacks or even more. This paper proposes a technique of active self-defense PCB modules with zero performance overhead. Those protection modules will only be activated when the boards are exposed to the attacks. A set of PCBs with proposed protection modules is fabricated and tested to prove the effectiveness and efficiency of the techniques.

1. Introduction

An article from Bloomberg Businessweek in 2018 stupendously claimed that overseas foundries had developed back doors to servers built for Amazon, Apple and others by inserting millimeter-size chips into circuit boards, as shown in Fig. 1. The companies involved and the U.S. Department of Homeland Security have run deep examinations and refuted the claims in the article.

Although those claims are proven to be inaccurate, the anxiety about hardware supply chain security swept the industry and academic community. People started to focus on the uncertainty of overseas foundries and tried to introduce authorization mechanisms or protections to secure the board and chips fabricated overseas [3, 4, 5].

Among all the electronic components fabricated overseas, PCBs are the most vulnerable because their large feature size makes them easy to be probed, brute force copied, or even revised for Trojan implantations and back door insertions. As a result, PCB design has been a place of no law for a long time. Competitors usually brute force copy a PCB for a shorter turn-around time (TAT) and lower design cost. In industry, the turn-around time of copying a six layers board can be as low as 24 hours; and the cost of the

*Corresponding author.

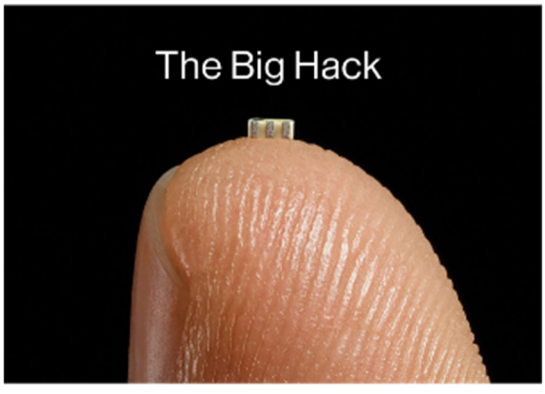

Fig. 1. Illustration of PCBs Trojan.

reverse engineering is usually marked as less than one cent per soldering point. Attackers can apply reverse engineering to PCBs to acquire the internal structure for further Trojan implantations or hacking actions. Also, as the metal traces in PCBs sometimes carry important design information, sensitive data, or critical control signals on a running device, attackers can eavesdrop, control, or disable the device.

Due to the lack and inefficiency of IP protection mechanisms and techniques, designers implicitly agreed that the design logic in PCBs is unprotected from attackers and rivals for design copying and revisions, although the design always carries important design and system information. Those PCB-based attacks and tampering are discussed in Section 2.

To deal with PCB hardware IP infringements, some countermeasures have been proposed. In [6], Paley and his co-authors introduced an active monitoring and prevention design for PCBs to defend against physical tampering. Piliposyan, Khursheed and Rossi also proposed a new power analysis method to detect alien components on a PCB, which can be regarded as a potential Hardware Trojan [7]. Yu designed an authentication system for PCBs to prevent counterfeits created by cloning or recycling [9]. In [10], the authors proposed a security module to protect circuit components from unauthorized access. Zhang introduced an authentication methodology to form a unique signature for each PCB, which can reflect the process variations in PCB traces and overall impedance using a PCBs Trace-Based Ring Oscillator [11]. The ROPA can provide both IC and PCBs authentication independently of external equipment and allows remote authentication for the user.

To the best of our knowledge, little effort has been made to counter PCB-level reverse engineering because the large feature size of PCBs' metal traces makes it extremely easy for attackers to apply reverse engineering.

Thus, this paper proposes a technique of active self-defense PCB modules based on transformable vias against reverse engineering. Those modules are realized by adding vias material pairs (magnesium (Mg) and magnesium oxide (MgO)) to the fabrication process of PCBs. Magnesium defines conducting vias, and magnesium oxide is regarded as a part of insulator vias for different metal layers. The mechanism will act from delayering through

imaging, during which Mg will be oxidized into MgO, and all the vias material pairs will be identified as MgO [17, 18, 14]. Thus, attackers are unable to distinguish MgO from Mg, which will lead to a routing pattern with extra metal traces. A specific application is to place extra metal traces near a high-frequency bus line. When attackers reverse-engineer the board and mis-identify the MgO vias as conductive vias, the extra metal traces will act as the receptor of the high-frequency metal trace to generate noise in the new routing pattern (see details in Sections 3 and 4). Note that since these extra metal traces are connected to the real circuit nodes (by MgO vias), attackers will not be able to detect them as non-functional.

The remainder of this paper is briefly organized as follows: Section 2 identifies the attack models. Sections 3 and 4 explain the design of transformable-based PCBs design and its feasibility. Section 5 presents the noise-generating model. Section 7 shows the experimental result of a fabricated PCB. Section 8 draws the conclusion.

2. Attack Models

2.1. *PCBs Brute Force Copying*

Generally, the layout drawings or Gerber files, the design files for reproducing, are extracted via PCBs-level reverse engineering. The framework is shown in Fig. 4 as follows:

(1) Bare PCBs can provide some physical information, e.g., physical sizes, number of layers and accurate test points.
(2) Different methods will be conducted to acquire the layers' images. Attackers sometimes destructively remove the material of each layer to image the routing patterns underneath. Figure 2 illustrates an example of a destructive method of delayering [12]. Other approaches for material removal include wet/plasma etching, grinding and polishing. Also, X-ray scanning can serve as a non-destructive method for imaging. Figure 3 is an illustration of X-ray images of PCBs.
(3) Identify metal traces, vias and dielectric materials in the images.
(4) Translate the information identified from the images into a CAD file.
(5) Run DRC (Design Rule Check) to cancel any violation in the design file.
(6) Output the Gerber design file for PCBs reproduction.

Note that attackers can repeat each step listed above for a desirable result before the next steps.

2.2. *PCBs Hacking*

Altered component replacement: The schematic usually reflects the designer's intent and logic most accurately. However, the circuit on the PCBs is much more complicated. A minor component variation on the board can cause serious problems, such as performance drop, overheating, or even power failure.

Attackers can use a maliciously altered version of the component in production to expect damage. This attack is hard to detect as the counterfeit components look similar to

the real ones. Here's an example in Fig. 5, this pair of FT232RL USB to serial UARTs seems quite similar. Still, the one on the right is a counterfeit based on a mask-programmable microcontroller and only works with older drivers [15] — a desirable result before the next steps.

Additional components/Trojan Insertion: Hardware hacks might need the inclusion of an extra, surreptitious component. The framework of Trojan insertion using non-destructive Imaging method is shown in Fig. 7. In that case, a spot on the board with many small components is the place to hide it. Modern passive components can be mere

Fig. 2. Example of Destructive Imaging method.

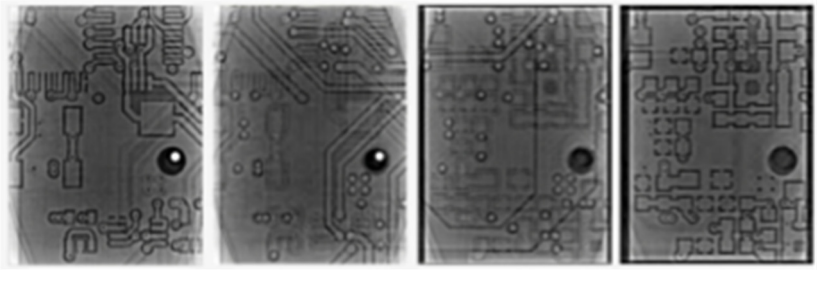

Fig. 3. Example of Non-Destructive Imaging method.

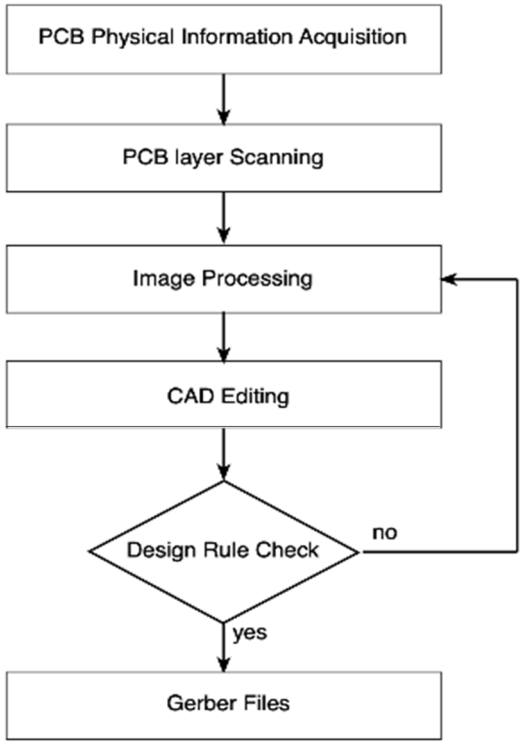

Fig. 4. PCB-Level Reverse Engineering Framework.

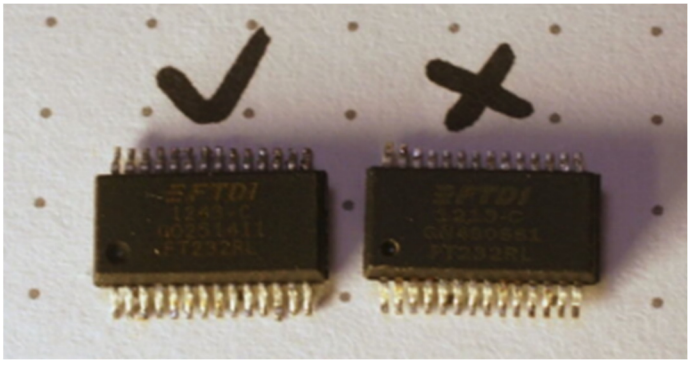

Fig. 5. Normal Chip and Counterfeit Chip.

millimeters in size and invisible to the unaided eyes. Here, the motherboard in Fig. 6 [13] is used as an example. The massive passive components area in Fig. 8(a) [13] can be the camouflage for Trojan or additional components. The report that triggered the community's anxiety, as shown in the figure, is an excellent example of Additional components/ Trojan Insertion.

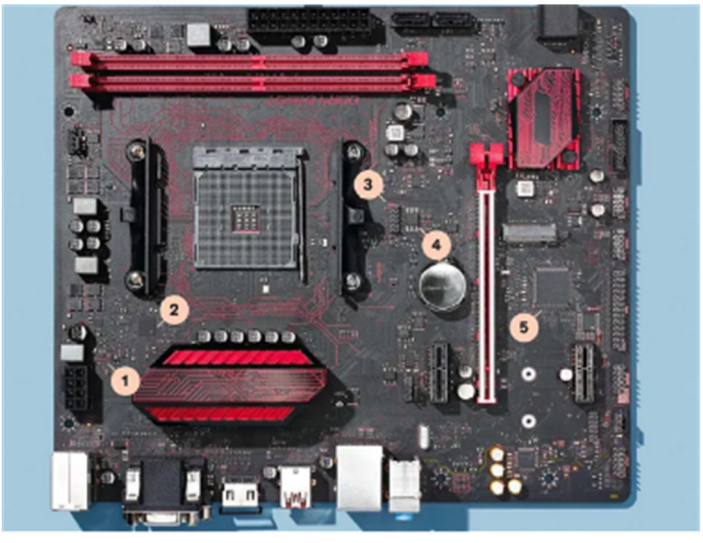

Fig. 6. Illustration of a Motherboard

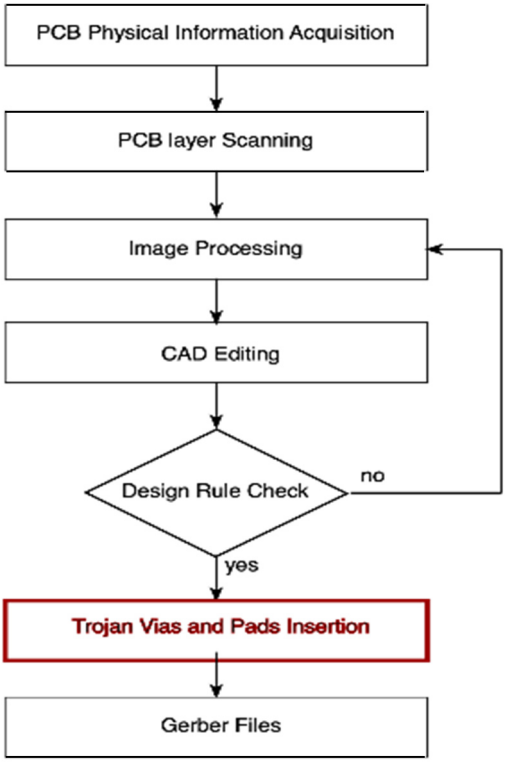

Fig. 7. Example of Trojan Insertion Using Non-destructive Imaging Method

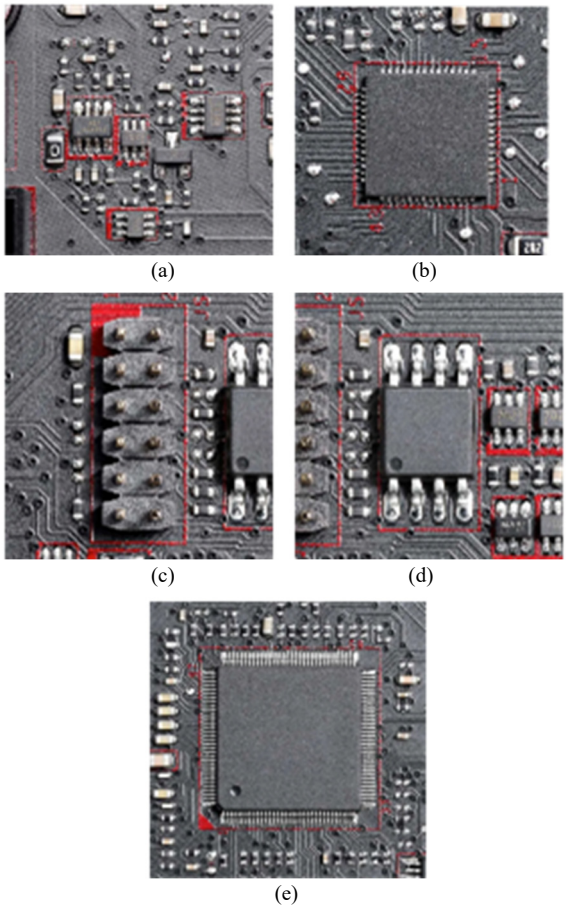

Fig. 8. Tempting Targets of the Board for Hacking: (a) Massive Passive Components Area. (b) Power Controller of the Board. (c) Low Pin Count Bus of the Board. (d) BIOS Flash Memory of the Board. (e) Super I/O Chip of the Board.

Taking control of and eavesdropping on certain data buses: Data buses usually carry important design and system information at runtime. Taking control of or eavesdropping on certain data buses means taking control of the whole system. Here, we still use Fig. 6(a) [13] as the example:

(1) The Power Controller in Fig. 8(b) [13] is a particularly fruitful target because it controls all of the DC voltages that power the CPU, the graphics card and more. It is under the control of the System Management Bus. So, if a hack enables people to seize control of the SMBus, they could reset voltages to damage a computer or limit its operation.

(2) The connector is attached to the LPC bus in Fig. 8(c) [13], which can link the CPU to specific legacy devices and the fans and physical switches on the chassis. Perhaps just

as important to hackers, the LPC bus can connect to a secure microcontroller called a Trusted Platform Module (TPM), which deals with encryption keys and various other security functions.

(3) The Basic Input/Output System (BIOS) flash memory in Fig. 8(d) [13] holds the data needed to initialize hardware during boot-up. It sits on the Serial Peripheral Interface (SPI) bus. Seizing control of the SPI bus would enable a hacker to alter hardware configurations so that a path would be open to inserting malicious code into the computer.

(4) The Super I/O chip in Fig. 8(e) [13] controls the inputs to various low-bandwidth devices, sometimes including keyboards, the mouse, specific sensors, fans and floppy disks. The chip sits on the Low Pin Count (LPC) bus. Seizing control of the LPC bus could let hackers reduce the fan speed so that a computer will overheat.

3. PCB Attacks and Reverse Engineering

To our best knowledge, reverse engineering serves as the footstone of all the PCB attack models discussed in Section 2.

In PCBs brute force copying, reverse engineering provides the attacker with exact physical information of the board to retrieve the Gerber files. In PCBs hacking, reverse engineering gives attackers insight into the schematic's design logic when attackers apply altered component replacement attacks and additional components/Trojan Insertion attacks. Furthermore, attackers can gain physical information on the metal traces using reverse engineering for Additional components/Trojan Insertion and Taking control of and eavesdropping on certain data buses; those spatial position relations are critical for busline probes setups [16].

Especially for those boards with more than four layers, the layouts of each layer are critical for the attacker. However, the top layer and bottom layers are the natural protections for the layers in between. Reverse engineering is the only way for the attackers to revive the contents of those sandwiched layers.

Our proposed technique is to create protection mechanisms for PCBs against reverse engineering, which will protect PCBs from all attacks. Note that there's no way to stop the attackers from applying reverse engineering to the board as the boards are to be distributed. However, our protection mechanisms (see Section 3) can significantly introduce problems/ errors and create cost overheads for the attackers.

4. Transformable-vias Structure in PCBs

Figure 9 shows that PCBs with more than two layers typically have three kinds of vias: through vias, buried vias and blind vias. The proposed technique exploits the "trans-formable" property of the Mg/MgO pair as a countermeasure to PCBs' reverse engineering. Buried vias material is replaced by Mg. MgO vias are deliberately placed in some locations with Cu metal traces.

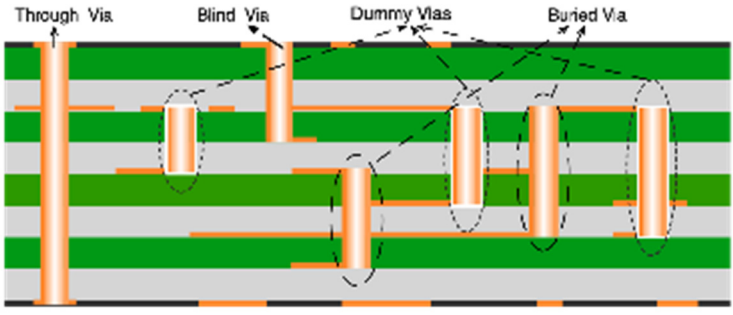

Fig. 9. Cross-Section of a PCB.

Note that the resistivity of Mg is 44.7 nΩ·m, which displays excellent electrical conductivity. And MgO is a dielectric material with a resistivity larger than 1000 Ω·cm. [18]. Thus, Mg Via can serve as normal via material, and Cu traces connected by MgO will be disconnected from the circuit regularly.

The layer imaging process will trigger the defense mechanism itself.

Suppose attackers apply a destructive imaging method to the board. Mg buried vias will oxidize into MgO and blend with the deliberately placed MgO vias. In the following imaging process, the oxide film formed on Mg has a dense morphology at the nanoscale resolution. This will conceal the original morphology of Mg material.

If attackers scan the PCBs with an X-ray, the best way to identify the presence and absence of material is to distinguish the brightness difference of the dielectrics and via material [1]. As shown in Fig. 10, the vias surrounded by bright shadows are those connected to theinterconnects, and those without the shadows are unconnected to the circuit. However, according to [19], little brightness difference between Mg and MgO is expected when exposed to X-ray.

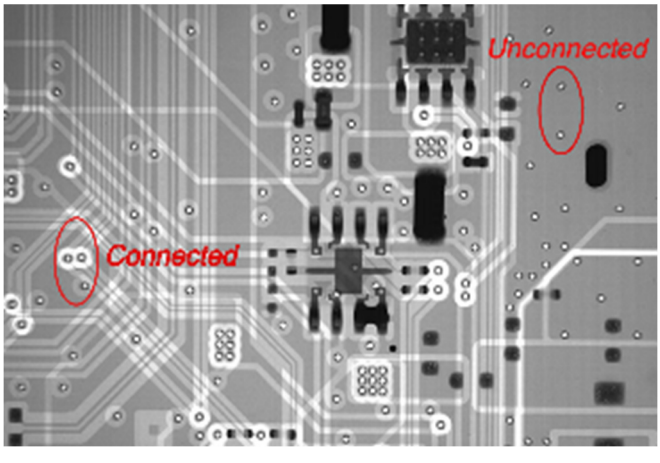

Fig. 10. Vias Identification of a PCB.

This means the original non-conductive MgO vias will blend with Mg buried Vias and mislead the attacks to another routing pattern [20, 8] as those MgO will be identified as conductive vias.

5. PCB Security Modules Using Transformable-Vias Structure

This section gives a specific application of the misleading routing pattern after reverse engineering: the "extra metal traces" will increase the crosstalk between high-frequency signals.

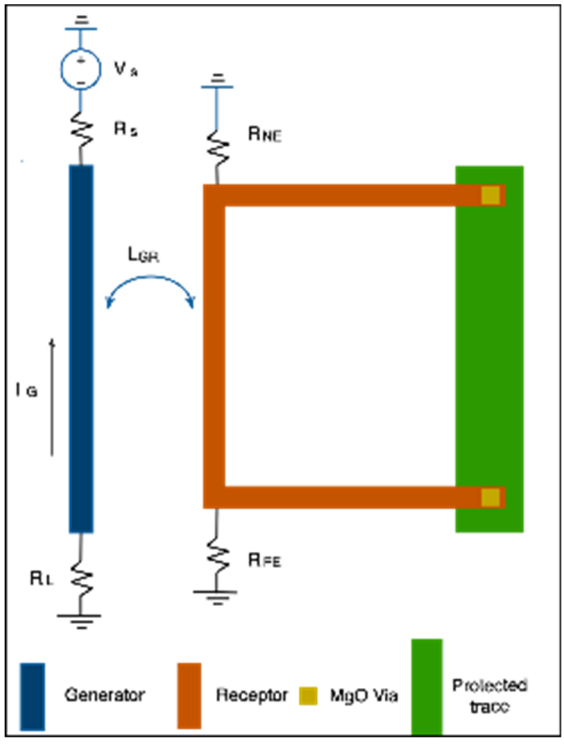

Fig. 11. Diagram of Crosstalk between Metal Traces Created by Transformable-vias.

In Fig. 11, the blue and green metal traces are in the original design. The orange trace is the green trace protection module connected with MgO vias, which disconnects it from the working circuit. The orange trace is deliberately placed near the blue high-frequency signal trace. Once exposed to reverse engineering, the circuit will include the orange trace in the design. The blue metal trace(generator) will generate noise in the orange trace(receptor); the near-end and far-end voltage can be expressed as Equations (1) and (2):

$$V_{NE}(t) = \frac{R_{NE}}{R_{NE}+R_{FE}} L_{GR} \frac{DI_G}{dt} + \frac{R_{NE}R_{FE}}{R_{NE}+R_{FE}} C_{GR} \frac{DV_G}{dt}, \quad (1)$$

$$\boldsymbol{V_{FE}(t)} = \frac{\boldsymbol{R_{FE}}}{\boldsymbol{R_{NE}+R_{FE}}}\boldsymbol{L_{GR}}\frac{\boldsymbol{DI_G}}{\boldsymbol{dt}} + \frac{\boldsymbol{R_{NE}R_{FE}}}{\boldsymbol{R_{NE}+R_{FE}}}\boldsymbol{C_{GR}}\frac{\boldsymbol{DV_G}}{\boldsymbol{dt}}. \quad (2)$$

The generator is driven by Vs with the impedance R_S and connected with a load resistor R_l; the far-end and near-end load resistors are R_{FE} and R_{NE}, respectively; I_G is the current in the generator; mutual inductance and capacitance are modeled as L_{GR} and C_{GR}, respectively.

As generator is the high-frequency signal trace, $V_G(t)$ and $I_G(t)$ can be expressed in Equations (3) and (4):

$$\boldsymbol{V_G(t)} = \frac{\boldsymbol{R_L}}{\boldsymbol{R_S+R_L}}\boldsymbol{V_s(t)}, \quad (3)$$

$$\boldsymbol{I_G(t)} = \frac{\boldsymbol{1}}{\boldsymbol{R_S+R_L}}\boldsymbol{V_s(t)}. \quad (4)$$

Therefore, V_{NE} (t) and V_{FE} (t) are given as in Equations (5) and (6):

$$\boldsymbol{V_{NE}(t)} = \left(\frac{\boldsymbol{R_{NE}}}{\boldsymbol{R_{NE}+R_{FE}}}\boldsymbol{L_{GR}}\frac{\boldsymbol{1}}{\boldsymbol{R_S+R_L}} + \frac{\boldsymbol{R_{NE}R_{FE}}}{\boldsymbol{R_{NE}+R_{FE}}}\boldsymbol{C_{GR}}\frac{\boldsymbol{R_L}}{\boldsymbol{R_S+R_L}}\right)\frac{\boldsymbol{dV_s(t)}}{\boldsymbol{dt}}, \quad (5)$$

$$\boldsymbol{V_{FE}(t)} = \left(-\frac{\boldsymbol{R_{FE}}}{\boldsymbol{R_{NE}+R_{FE}}}\boldsymbol{L_{GR}}\frac{\boldsymbol{1}}{\boldsymbol{R_S+R_L}} + \frac{\boldsymbol{R_{NE}R_{FE}}}{\boldsymbol{R_{NE}+R_{FE}}}\boldsymbol{C_{GR}}\frac{\boldsymbol{R_L}}{\boldsymbol{R_S+R_L}}\right)\frac{\boldsymbol{dV_s(t)}}{\boldsymbol{dt}}. \quad (6)$$

Thus, intuitively, the higher the frequency signal in the generator, the higher the inductive and capacitive couplings will perform better protection modules.

6. Eye Diagram Analysis and Q Factor

We use Eye Diagram Analysis and Q Factor to evaluate the noise disturbance over the system.

The eye diagram provides a visual indication of how noise might impact system performance, as shown in Fig. 12, where μ1 and μ1 mean values of the signal levels for a "0" and a "1", and σ0 and σ1 represent the sum of the noise values at those two signal levels assuming Gaussian noise and the probability of a "0" and "1" transmission being equal.

The Q factor can be expressed as Equation (7), which measures the quality of a transmission signal in terms of its signal-to-noise ratio (SNR). It considers physical impairments to the signal, which can degrade it and cause bit errors.

$$\boldsymbol{Q} = \frac{|\boldsymbol{\mu_1-\mu_0}|}{\boldsymbol{\sigma_1+\sigma_0}}. \quad (7)$$

Q-Factor represents the quality of the SNR in the "eye" of a digital signal, the "eye" being the human eye-shaped pattern on an oscilloscope that indicates transmission system performance. The best place for determining whether a given bit is a "1" or a "0" is the

sampling phase with the most significant "eye-opening." The larger the eye-opening is, the more significant the difference between the mean values of the signal levels for a "1" and a "0" is. The more significant that difference is, the higher the Q factor and the better the BER performance.

In the industry or practical circuit design, a system's maximum Q factor must be smaller than 6% (raw BER of 10^{-9}) [2]. We will use the Q factor to evaluate the effectiveness of implanted protection modules in Section 4.

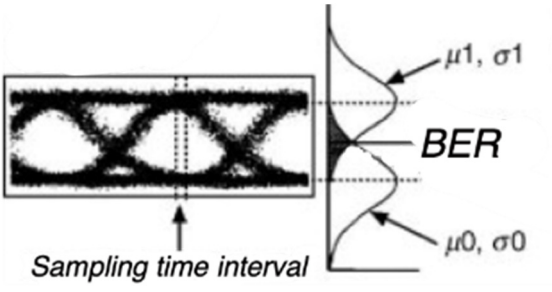

Fig. 12. Eye Diagram Example.

7. Experimental Results

We fabricated and tested the PCBs with the protection modules to prove the effectiveness and efficiency of the proposed protection modules. The fabricated board is shown in Fig. 15.

The board's parameters are as follows: the core thickness is 1.5 mm, the metal trace width is 0.1778 mm, the minimum PCB trace spacing is 0.1778 mm, and the metal layer thickness is 0.075 mm.

Here, we define the unprotected metal trace as the control group and the protected metal trace in the same physical parameters with protection modules as the protection group. Thus, the noise introduced by the protection modules can be measured as the difference between the protection and control groups.

As discussed in Section 5, to maximize the noise introduced by the protection modules, we used switchback routings to maximize the inductive and capacitive couplings for the test, illustrated in Fig. 15. Note that switchback routing is usually used for signal integrity and signal delay adjustment in PCBs, which makes protections legitimate from the attackers' perspective.

During the test, the frequency of the protected signal and generator signals in the test is set to 10MHz and 3MHz–15MHz, respectively. Testing results are shown in Figs. 14, 17 and 19. Significant noise can be observed in the figure. To better evaluate the noise introduced, we generated square waves using the sine waves in the protection groups and compared them with those generated from the control groups. The threshold voltage is set as 0.73VDD.

Figure 13 shows the schematic of Group 1 in Fig. 15. The protection metal traces are wired parallel to the protected trace. The square waves are shown in Fig. 14, and the Q factors are listed in Table 1. As mentioned in Section 6, the design with dummy metal length of 5.08 mm will fail with a Q factor larger than 6%. The protections with lengths of 11.43 mm and 60.96 mm can significantly protect the information carried in the metal trace.

Figure 16 shows the schematic of Group 2 in Fig. 15. The protection metal traces are wired vertically to the protected trace. The square waves are shown in Fig. 17, and the Q factors are listed in Table 2. All four lengths of protection will fail the system if attackers copy the board design.

Figure 18 shows the schematic of Group 3 in Fig. 15. The protection metal traces are spirally wired in nearby layers to the protected trace. The square waves are shown in Fig. 19 and the Q factors are listed in Table 3. All three lengths of protection will fail the system if attackers copy the board design.

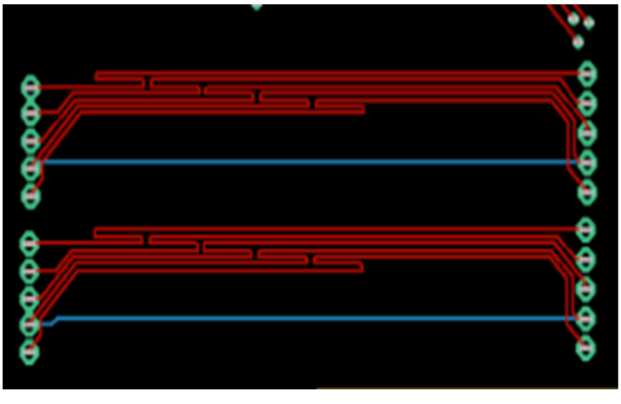

Fig. 13. Schematic of Group 1.

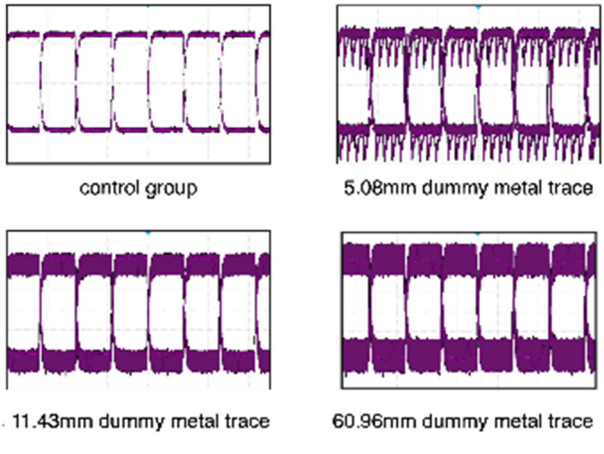

Fig. 14. Results of Module 1 with Different Length.

Table 1. Q factors of Module 1

Dummy Metal length	0	5.08 mm	11.43 mm	60.96 mm
Q factor	40.32%	8.3%	4.2%	3.8%

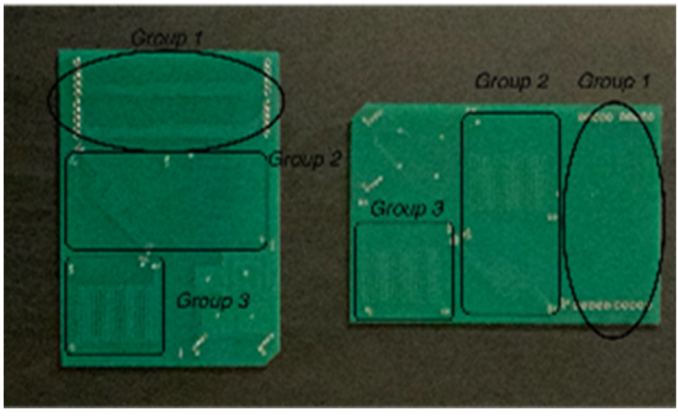

Fig. 15. The PCBs Fabricated for Protection Module Testing.

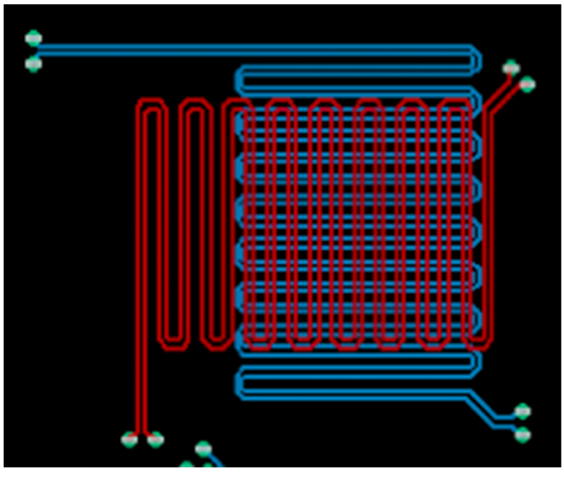

Fig. 16. Schematic of Group 2.

Table 2. Q factors of Module 2

Dummy Metal length	0	10.16 mm	17.78 mm	25.40 mm	40.46 mm
Q factor	40.32%	4.48%	3.80%	1.70%	1.45%

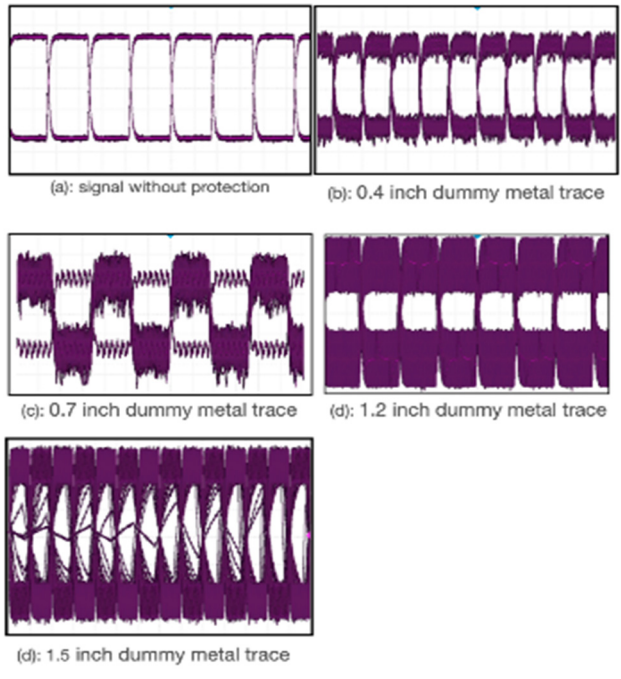

Fig. 17. Results of Module 2 with Different Length.

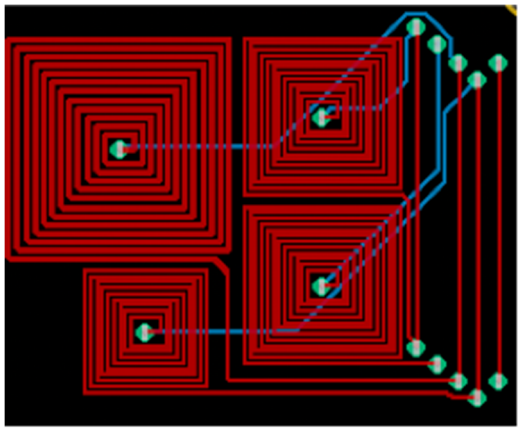

Fig. 18. Schematic of Group 3.

Table 3. Q factors of Module 3

Dummy Metal length	0	20.32 mm	30.48 mm	45.72 mm
Q factor	40.32%	3.92%	3.20%	1.35%

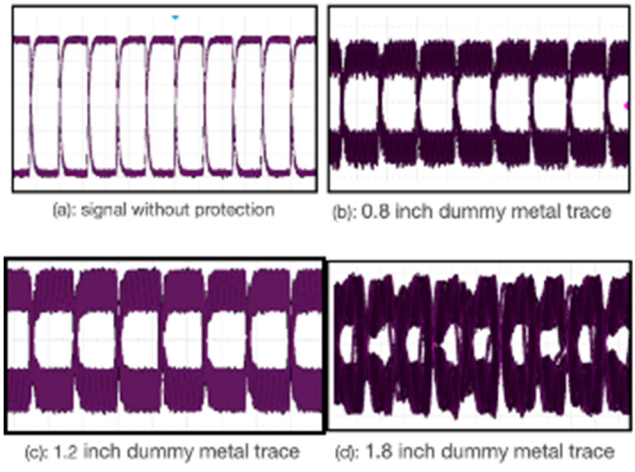

Fig. 19. Results of Module 3 with Different Length.

8. Conclusion

Transformable vias (MgO vias and Mg vias) based self-defense modules for PCBs design and their feasibility has been elucidated. Protection modules using the crosstalk model to protect sensitive data are proposed and analyzed. The experimental result of the fabricated PCBs is presented. Future work will focus on more protection module development to cause different failures for attackers, such as power failure, Electro Magnetic Interference (EMI) failure, and overheating.

References

1. N. Asadizanjani, M. Tehranipoor and D. Forte, "PCB Reverse Engineering Using Nondestructive X-ray Tomography and Advanced Image Processing," in IEEE Transactions on Components, Packaging and Manufacturing Technology, vol. 7, no. 2, pp. 292–299, Feb. 2017, doi:10.1109/TCPMT.2016.2642824.
2. https://www.itu.int/rec/T-REC-O.201/en
3. N. Vashistha, M. L. Rahman, M. S. U. Haque, A. Uddin, M. S. U. I. Sami, A. M. Shuo, P. Calzada, F. Farahmandi, N. Asadizanjani, F. Rahman and M. Tehranipoor, ToSHI-Towards Secure Heterogeneous Inte- gration: Security Risks, Threat Assessment, and Assurance. Cryptology ePrint Archive, 2017.
4. F. Ganji, S. Tajik, J. P. Seifert and D. Forte, Blockchain- enabled cryptographically-secure hardware obfuscation. Cryptology ePrint Archive, 2019.
5. V. Gohil, H. Guo and S. Patnaik, ATTRITION: Attacking Static Hardware Trojan Detection Techniques using Reinforcement Learning. arXiv:2208.12897, 2022.
6. S. Paley, T. Hoque and S. Bhunia, Active protection against PCB physical tampering. 2016 17th International Symposium on Quality Electronic Design (ISQED), Santa Clara, CA, 2016, pp. 356–361, doi:10.1109/ISQED.2016.7479227.

7. G. Piliposyan, S. Khursheed and D. Rossi, "Hardware Trojan Detection on a PCB Through Differential Power Monitoring," IEEE Transactions on Emerging Topics in Computing, doi:10.1109/TETC.2020.3035521.
8. S. Chen and L. Wang, Reverse engineering resistant ROM design using transformable via-programming structure. 2016 IEEE International Symposium on Circuits and Systems (ISCAS), IEEE, 2016, pp. 2627–2630.
9. A. Hennessy, Y. Zheng and S. Bhunia, JTAG-based robust PCB authentication for protection against counterfeiting attacks. 2016 21st Asia and South Pacific Design Automation Conference (ASP-DAC), Macau, 2016, pp. 56–61, doi:10.1109/ASPDAC.2016.7427989.
10. M. T. Enevoldsen et al., Security module for protection circuit components from unauthorized access. U.S. Patent No. 10,009,995. 26 June 2018.
11. D. Zhang, Q. Ren and D. Su, "A Novel Authentication Methodology to Detect Counterfeit PCB Using PCB Trace-Based Ring Oscillator," in IEEE Access, vol. 9, pp. 28525–28539, 2021, doi:10.1109/AC- CESS.2021.3059100.
12. J. Grand, Printed circuit board deconstruction techniques. 8th USENIX Workshop on Offensive Technologies (WOOT 14). 2014.
13. S. H. Russ and J. Gatlin, "Ways to hack a printed circuit board: PCB production is an underappreciated vulnerability in the global supply chain," in IEEE Spectrum, vol. 57, no. 9, pp. 38–43, 2020, doi:10.1109/MSPEC.2020.9173902.
14. S. Chen and L. Wang, "Transformable electronics implantation in ROM for anti-reverse engineering," in International Journal of High Speed Electronics and Systems, vol. 28, no. 03n04, p. 1940021, 2019.
15. https://arstechnica.com/gadgets/2021/06/chip-shortages-lead-to-more-counterfeit-chips-and-devices/
16. J. S. Go¨tte and B. Scheuermann, "Can't touch this: Inertial HSMs thwart advanced physical attacks," in IACR Transactions on Cryptographic Hardware and Embedded Systems, pp.69–93, 2022.
17. S. Chen, J. Chen and L. Wang, "A chip-level anti-reverse engineering technique," in ACM Journal on Emerging Technologies in Computing Systems (JETC), vol. 14, no. 2, pp. 1–20, 2018.
18. S. Chen *et al*., "Chip-level anti-reverse engineering using transformable interconnects." 2015 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFTS), IEEE, 2015.
19. S. Durdu, A. Aytac and M. Usta, "Characterization and corrosion behavior of ceramic coating on magnesium by micro-arc oxidation, in Journal of Alloys and Compounds, vol. 509, no. 34, pp. 8601–8606, 2011.
20. W. Stark, S. Chen and L. Wang, "Reverse engineering protection using obfuscation through electromagnetic interference," in International Journal of High Speed Electronics and Systems, vol. 31, no. 01n04, p. 2240003, 2022.