Probing Attacks on Integrated Circuits: Challenges and Research Opportunities

Huanyu Wang, Domenic Forte, and Mark M. Tehranipoor
University of Florida

Qihang Shi
University of Connecticut

Editor's note:
As a type of invasive physical attacks, probing attacks are able to access and directly monitor security critical nets of an IC and extract sensitive information. In this paper, the authors summarize the state-of-the-art probing and anti-probing technologies and their challenges, and discuss the opportunities in the relevant research.

—Yiran Chen, Duke University

Physical attacks are capable of bypassing the confidentiality and integrity provided by modern cryptography through observation of a chip's silicon implementation. Such attacks are especially threatening to the integrated circuits (ICs) in smartcards, smartphones, military systems, and financial systems relying on processing sensitive information. Unlike noninvasive side channel analysis (e.g., power or timing analysis), probing directly accesses the internal wires of a security-critical module and extracts sensitive information in electronic format. Probing, in unison with reverse engineering and circuit edit, poses a serious threat to mission-critical applications, and thus demands development of effective countermeasures from the research community.

Digital Object Identifier 10.1109/MDAT.2017.2729398
Date of publication: 19 July 2017; date of current version: 13 September 2017.

Probing attacks are already a part of the current reality. The most recent example of it emerged when FBI requested help in defeating the passcode retry counter of the Apple iPhone 5c owned by a terrorist suspect. Researchers reverse engineered the proprietary protocol used by the phone's NAND flash, mirrored (copied) the contents, and then brute forced the passcode in less than a day [11]. While in this case the attack was conducted by researchers, and compromise of military technologies through probing could have catastrophic consequences that cost lives. In such instances, advanced IC failure analysis and debug tools are used to internally probe the ICs. Among such tools, focused ion beam (FIB) is the most dangerous.

FIBs use ions at high beam currents for site-specific milling and material removal. The same ions can also be injected close to a surface for material deposition. These capabilities allow FIBs to cut or add traces to the substrate within a chip, thereby enabling them to redirect signals, modify trace paths, and add/remove circuits. Though FIB was initially designed for failure analysis, a skilled attacker can use it to obtain on-chip keys, establish privileged access to memory, obtain device configuration, and/or inject faults. This can be accomplished by rerouting them to an existing output pin,

Copublished by the IEEE CEDA, IEEE CASS, IEEE SSCS, and TTTC

creating a new contact for probing, or re-enabling IC test mode. Most of these techniques would not be possible without a FIB. While countermeasures against probing such as active meshes, optical sensors, and analog sensors have been proposed, they are clumsy, expensive, and *ad-hoc*. It has been often shown that an experienced FIB operator can easily bypass them via circuit edit. In [10], well-known hacker Christopher Tarnovsky probed the firmware of the Infineon SLE 66CX680P/PE security/smart chip from the frontside (i.e., top metal layer) by rewiring its active mesh and making contact with its buses using FIB.

We expect FIB-assisted probing attacks to increase for a variety of reasons. FIBs are becoming cheaper and easier to access than ever before (e.g., FIB time can be purchased for a couple hundred dollars per hour). Further, as FIB capabilities continue to improve for failure analysis, more powerful attacks will be enabled. In contrast, noninvasive and semi-invasive attacks either do not scale to modern semiconductors with Moore's Law, or can be mitigated by inexpensive countermeasures. As noninvasive and semi-invasive attacks continue to become less effective, one can expect attackers to migrate to FIB. For these reasons, it is of the utmost importance that we stay ahead of attackers and develop more effective countermeasures against FIB-based probing. Since FIB capabilities are almost limitless, the best approaches should make probing as costly, time consuming, and frustrating as possible. A significant challenge in doing so lies in the fact that the time, effort, and cost to design a FIB-resistant chip must remain reasonable, especially to design engineers who are generally not security experts. This could be especially important in the upcoming Internet-of-Things (IoT) era which will likely consist of an abundance of low-end chips that are easily physically accessed.

In this paper, we present state-of-the-art research in the field of circuit edit and antiprobing, highlight the challenges, and offer future research directions for computer-aided design (CAD) and test communities. The rest of the paper is organized as follows. Probing attack fundamentals reviews technical background related to probing attacks. Existing countermeasures and limitations introduces existing countermeasures against probing attacks and their limitations. In current challenges and future research, we elaborate on main challenges and research opportunities in the field.

Probing attack fundamentals

Comprehension of the adversary's goal and the techniques he/she uses to successfully carry out probing is the first step in overcoming this significant threat. In this section, we review technical details of the probing process, and make associations between technical requirements, decisions, and perceived limitations of state-of-the-art techniques.

Probing attack targets

It is essential for both attackers and countermeasure designers to determine which signals are more likely to be targeted in a probing attack. We term such signals as *assets*. An asset is a resource of value which is worth protecting from an adversary [4]. Unfortunately, a more palpable definition of asset has not been proposed or agreed upon. To help illustrate the wide range of possible information that could be assets, here we enumerate a few quintessential examples of assets that are the most likely targets for probing attacks.

Keys

Keys of an encryption module (e.g., private key of a public key algorithm) are archetypal assets. They are usually stored in nonvolatile memory on the chip. If the key is leaked, the root of trust it provides will become compromised, and could serve as a gateway to more serious attacks. An example is original equipment manufacturer keys that are used to grant legitimate access to a product or chip. Leakage of such keys will result in tremendous loss of revenue for the product owner, denial of service, or information leakage.

Firmware and configuration bitstream

Electronic intellectual properties (IPs) such as low-level program instruction sets, manufacturer firmware, and field programmable gate arrays (FPGA) configuration bitstreams are often sensitive, mission critical, and/or contain trade secrets of the IP owner. Once compromised, counterfeiting, cloning, or exploits of system vulnerabilities could be facilitated.

On-device protected data

Sensitive data, such as health and personal identifiable information, should be kept private. Leakage of such information could result in fraud, embarrassment, or property/brand damage for the data owner.

Device configuration

Device configuration data control the access permissions to the device. They specify which services or resources can be accessed by each individual user. If the configurations are tampered with, an attacker could illegally gain access to resources denied to him otherwise.

Cryptographic random number

Hardware generated random numbers, such as keys, nonces, one-time pads, and initialization vectors for cryptographic primitives also require protection. Compromising this type of asset will weaken the cryptographic strength of the digital services on the device.

Essential technologies of a probing attack

A successful probing attack entails a time consuming and sophisticated process. Countermeasure designers are often interested in ways to make this process go astray. For this purpose, we examine the central approaches and technologies used in published attacks in the following subsections.

Front-side versus back-side

Probing attack targets are those metal wires that carry assets, henceforth called target wires. The most common approach to reach target wires is to expose them from the back end of line, i.e., from the top metal layer toward silicon substrate (illustrated in Figure 1a). This is called a front-side probing attack. Exposure of target wires is first facilitated with FIB milling, then an electric connection to the target wire can be established, e.g., by conductor deposition capability of the FIB. Finally, extraction of sensitive information ensues.

A back-side probing attack, i.e., probing that occurs through the silicon substrate, was proposed in [6]. Back-side attack targets are not limited to wires. By exploiting a phenomenon during transistor activity known as photon emission, transistors can also be probed to extract information.

Electrical probing versus optical probing

The method to access assets shown in Figure 1a is typical for electrical probing, i.e., accessing an asset carrying signal via electrical connection. A different approach is optical probing as shown in Figure 1b. Optical probing techniques are often used

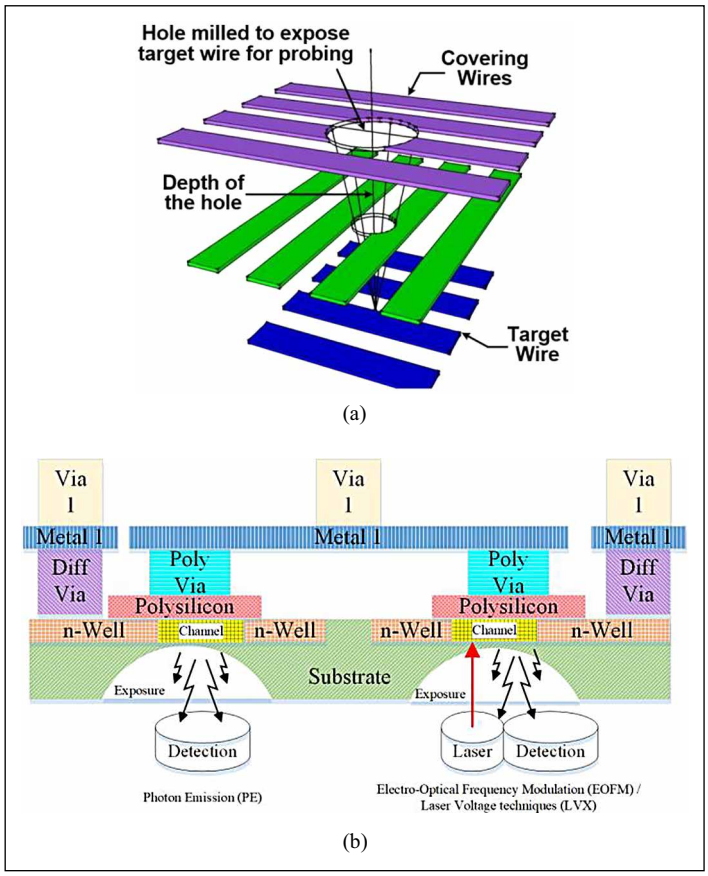

Figure 1. (a) Milling from back end of line through covering wires (purple and green) to reach target wires (blue) [5]. (b) Optical probing: photon emission (PE) and electro-optical frequency modulation or laser voltage techniques are used for passive and active measurements, respectively.

in back-side probing to capture photon emission (PE) phenomena during transistor switching. When transistors are switching, they spontaneously emit photons without external stimuli. By passively receiving and analyzing the photons emitted from a specific transistor, the signal processed by that transistor can be inferred. Compared to electrical probing, the optical approach has the advantage of being a purely passive observation, which makes it very difficult to detect. In addition to PE analysis, laser voltage technique or electro-optical frequency modulation are also used during back-side attacks. These techniques actively illuminate the switching transistors and then infer asset signal values by observing the reflected light.

The primary deficiency of optical probing lies in the fact that photons emitted in these techniques are infrared due to silicon energy band gap, which

has a wavelength of 900 nm or higher [6]. Therefore, the optical resolution between transistors is limited to within one order of magnitude of the wavelength due to Rayleigh criterion.

Essential steps of a probing attack

In this section, we continue our examination of probing attack fundamentals by outlining its essential steps.

Decapsulation

The first stage of the most invasive physical attacks is to either partially or fully remove the chip package in order to expose the silicon die. This requires an adequate practice and expertise in handling harmful chemicals. Acid solutions such as fuming nitric acid combined with acetone at 60 ºC are often used to remove plastic packages [7]. Decapsulation can also be done from the back-side of the chip by removing the copper plate mechanically without chemical etching.

Reverse engineering

Reverse engineering [8] is the process of extracting design information from something, typically to reproduce it. In the case of probing, reverse engineering is used to understand how the chip works, which requires that the layout and netlist be extracted. By studying the netlist, the attacker can identify the assets. One-to-one correspondence between the netlist and layout can then determine the locations of target wires and buses, and in the event where cutting off a wire is unavoidable, determining whether the cut would impact asset extraction. State-of-the-art tools such as ICWorks from Chipworks can perform automatic extraction of netlists from images of each layer taken with optical or scanning electron microscopes shown in Figure 2a, which greatly reduces the attacker's effort.

Locating target wires

Once the probing wire targets have been identified by reverse engineering, the next stage is locating the wires associated with the target on the IC under attack. The crux of the problem here is that while the attacker has located target wires on sacrificial devices during reverse engineering process, he/she now has to find the absolute coordinates of the point to mill blindly. This requires a precise-enough kinematic mount, and fiducial markers (i.e., visual points of reference on the device) to base these absolute coordinates.

Reaching target wire and extracting information

With the help of modern circuit editing tools like FIB (see Figure 2b), a hole can be milled to expose the target wire. State-of-the-art FIBs can remove and deposit material with nanometer resolution, which allows an attacker with a FIB to edit out obstructing circuitry, or deposit conducting paths that may serve as electrical probe contacts. This feature indicates that many countermeasures can be disabled by simply disconnecting a few wires, and that a FIB-equipped attacker could field as many concurrent probes as logic analyzer allows. Once a target wire is exposed and assuming it is contacted without triggering any probing alarm signals from active or analog shields, the asset signals need to be extracted, for example, with a probe station. The difficulty of this step depends on a few factors. First, software and hardware processes might need to be completed before the asset is available. Further, the sensitive information may not be in the same clock cycle; if the chip has an internal clock source to prevent external manipulation, the attacker will need to either disable it or synchronize his own clock with it.

Figure 2. (a) Scanning electron microscope. (b) Focused ion beam. Note that attacker does not need to purchase all these instruments since rent by time is quite low cost.

Existing countermeasures and limitations

In the past decade, researchers have proposed various technologies to protect security-critical circuits against probing attacks. In this section, we review a few representative countermeasures and highlight their limitations. Unfortunately, to date, none of them offer a satisfactory solution. Further, to the best of our knowledge, no method has been proposed to adequately address back-side probing attacks.

Active shields

Active shield is so far the most investigated probing countermeasure. In this approach, a shield which carries signals is placed on the top-most metal layer to detect holes milled by FIB. The shield is referred to as "active" because signals on these top layer wires are constantly monitored to detect if milling has cut them [1]. Figure 3a shows one illustrative example. As shown in the figure, a digital pattern is generated from a pattern generator, transmitted through the shield wires on top-most metal layer, and then compared with a copy of itself transmitted from lower layer. If an attacker mills through the shield wires on top layer to reach target wire, the hole is expected to cut open one or more shield wires, thereby leading to a mismatch at the comparator and triggering an alarm signal to erase or stop generating sensitive information. Despite its popularity, active shields are not without shortcomings. Their biggest problems are that they impose large overheads on the design, but at the same time are very vulnerable to attacks with advanced FIBs, e.g., circuit editing attacks.

Analog shields and sensors

An alternative approach to active shield is to construct an analog shield. Instead of generating, transmitting, and comparing digital patterns, analog shields monitor parametric disturbances with its mesh wires.

In addition to shield designs, the probe attempt detector (PAD) [2] also uses capacitance measurement on selected security critical wires to detect additional capacitance introduced by a metal probe. Compared to active shields, analog shields detect probing without test patterns and require less area overhead. The PAD technique is also unique in remaining effective against electrical probing from the back-side. The problem with analog sensors or shields is that analog measurements are less reliable due to process variations, a problem further exacerbated by feature scaling.

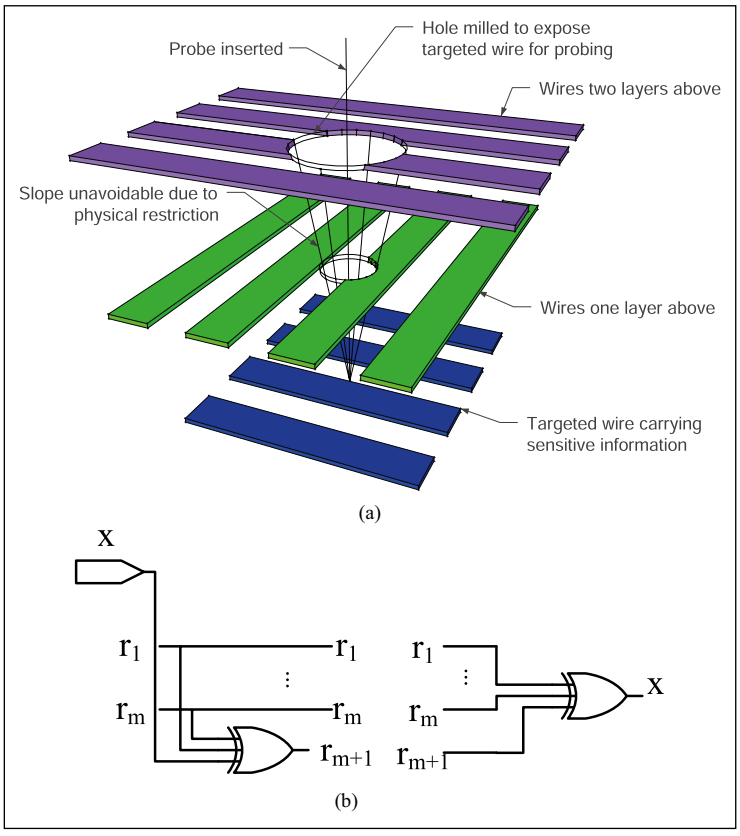

Figure 3. (a) Basic working principle of active shields [5]. (b) Input encoder (left) and output decoder (right) for masking in t-private circuits [3].

t-private circuits

The t-private circuit technique is proposed in [3] based on the assumption that the number of concurrent probe channels that an attacker could use is limited, and exhausting this resource thereby deters an attack. In this technique, the circuit of a security-critical block is transformed so that at least $t + 1$ probes are required within one clock cycle to extract one bit of information. First, masking is applied to split computation into multiple separate variables, where an important binary signal, x, is encoded into $t + 1$ binary signals by XORing it with t independently generated random signals ($r_{t+1} = x \oplus r_1 \oplus \cdots \oplus r_t$) as shown in Figure 3b. Then, computations on x are performed in its encoded form in the transformed circuit. x can be recovered (decoded) by computing

$x = r_1 \oplus \cdots \oplus r_t \oplus r_{t+1}$. The major issue with t-private circuit is that the area overhead involved for the transformation is prohibitively expensive.

Other countermeasure designs

Some other countermeasures are implemented in real ICs but less reported as novel designs because they are more or less dated. One known countermeasure that deters decapsulation stage of probing attacks is light sensor that is sometimes included in a tamper-resistant design. Some other techniques include scrambling wires and avoiding repetitive patterns in shield mesh to impede the locating-target-wire stage of probing attacks. They are not particularly effective as exploits against them have been detailed in [10].

Current challenges and future research

To summarize previous sections, FIB is a formidable technology in the hands of a skilled attacker, which is capable of overcoming sophisticated protections mechanisms. Here, we delineate the main challenges in the field of antiprobing as well as the promising future research directions aimed at overcoming them.

Challenges

Overhead/scalability

Most existing countermeasures assume spacious designs with generous leeway for area and layer overheads. Existing active and analog shield designs need to completely occupy at least one metal routing layer because otherwise it would be hard to determine which wires the shield should cover. This can be quite costly, since fabrication cost scales with the number of layers. Another problem is area overhead, of which the most demanding is the 1-private circuits technique. For instance, a 1-private AND circuit, which only offers protection against an adversary with the ability to probe two nets in every clock cycle, requires four AND gates and four XOR gates to implement the transformed circuit. Similarly, an active shield that uses a small pattern generator runs the risk of being simple enough for attacker to reverse engineer, making it possible for the attacker to disable the shield by feeding it with identical patterns generated from off the chip, a technique known as rerouting attack. To prevent the rerouting attack, the pattern generator has to be cryptographically secure, which in turn necessitates large area overhead. Further, the only countermeasure design among those surveyed in probing attack fundamentals that do not expect large concessions on overheads (the PAD technique) is only deceptively low in overheads: if the attacker was to reconstruct protected signal from unprotected wires through reverse engineering the design, the PAD would be circumvented, and to cover all potentially sensitive wires require even larger overheads.

In addition to cost and performance loss, large area and layer overheads leave devices with tight cost margin (e.g., smartcards) dangerously exposed. Further, most countermeasure designs also assume that the design to protect is an Application-Specific IC (ASIC) or System-on-Chip (SoC), while giving little consideration to reconfigurable devices such as FPGA.

The threat of advanced FIB

A FIB probing attack is powerful for two reasons: it can leave very small footprint when milling; it can remove and deposit metal or dielectric material, which allows the attacker to edit circuit connections at will. Existing countermeasures are often ill-equipped to address either threat. Active and analog shields are often placed on top routing layers, where very large pitch and width for wires make it easier for the attacker to mill a hole so thin that it does not completely cut off any mesh wire (often referred to as a *bypass attack*), especially if a FIB with high aspect ratio (i.e., leaves smaller footprint on top layer). Despite this obvious deficiency, constructing the shield on a lower layer would preclude access to higher layers since they have to cover an entire layer, pose severe restrictions on circuit performance, and may result in larger area overhead to accommodate routing needs. Both shield designs usually assume that the problem is solved after an alarm bit is produced. However, the FIB's circuit edit capability could enable the attacker to disable the shield by simply removing the alarm bit. For analog shields in particular, improved milling precision will lead to less disturbance of analog parameters. For t-private circuit technique, although it is not vulnerable in disabling circuit edit or less-detectable milling, it is nevertheless impacted by the ability of FIB to deposit conducting paths at will, which puts serious concerns on the tenability of the fundamental

assumption of this approach, i.e., the total number of probes is limited.

Existing countermeasures are not holistic

It helps to keep in mind that countermeasure designs do not change after they are put in place. As such, they can be expected to be scrutinized by would-be attackers, and it should be assumed that the weakest link in the system will be attacked. Hence, any countermeasure design is only as secure as its weakest link. Unfortunately, few existing countermeasures are designed with this mentality. Active and analog shields are designed assuming that the attacker is only going to perform a front-side attack. Among detection-based techniques we have surveyed in existing countermeasures and limitations, the PAD is the only technique secure against back-side attacks, but it is not secure when the attacker reverse engineers the design and reconstructs the protected signal from signals on unprotected wires. t-private circuit technique is secure against these problems at rather great cost, but still fails when attacker could deposit metal contacts at will with FIB. Finally, none of the techniques surveyed offers any protection against optic probing from the back-side.

Future research opportunities

We believe that there are three areas the community must put forth more effort to advance countermeasure research and development to address the probing threat:

- There is a clear need to develop innovative countermeasures.
- More types of devices (analog, digital, and FPGA) must be protected.
- The efficiency and applicability of the existing countermeasures require improvement.

Countermeasures innovation opportunities

Methods to protect ICs from probing attacks have much in common with how probing attacks can fail. Existing countermeasure designs cover only some of these techniques, and there are still more opportunities yet to be investigated. Reflecting on the details of probing attack techniques made in essential technologies of a probing attack and essential steps of a probing attack, we have summarized potential ways to foil the probing attacks as shown in Figure 4. Here are some examples:

- Optical probing from the back-side may be hindered by optimizing transistor placement to ensure that photon emissions of key gates are camouflaged by closely placing gates with complementary values.
- Techniques designed for other threats can be employed as a step against probing attacks, e.g., obfuscation techniques such as camouflaged gates and dummy contacts [9] can deter the reverse engineering stage of the probing attacks.
- It may be worthwhile to relocate sensitive wires to lower layers, making it more difficult for attackers to gain access to them.
- Innovative digital or analog detection mechanisms could be developed to improve sensitivity and confidence in detection.

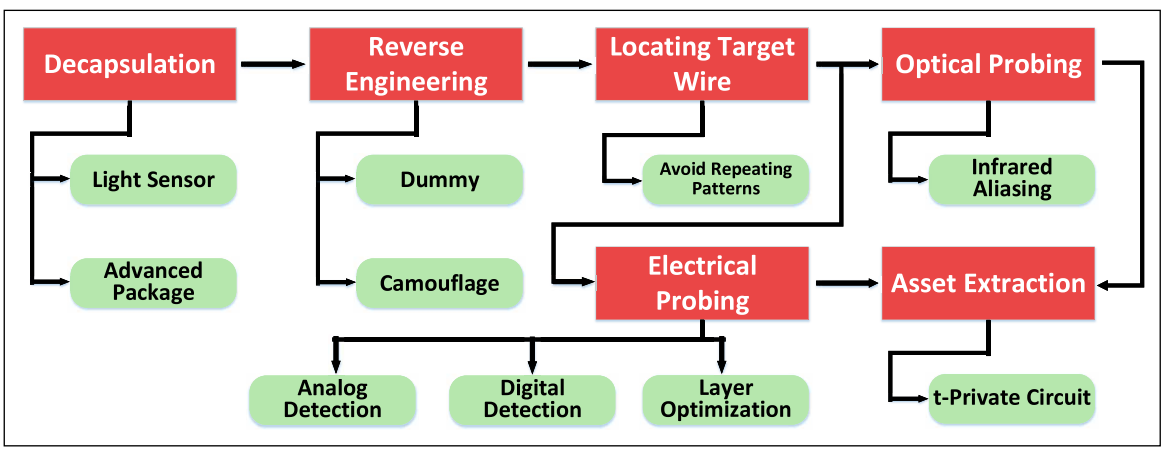

Figure 4. Potential opportunities to foil probing attack at each stage.

- Asset extraction may be deterred with t-private circuits, if the concern regarding high area and performance overhead could be addressed.
- Top layers of devices should avoid displaying features that help attackers locate target wire coordinates, and camouflaging techniques may be able to help.

As can be gathered from Figure 4, not all of these opportunities require a large amount of area or routing layer overhead, are vulnerable to advanced FIB, or can be circumvented by using an alternative technique to attack. For example, camouflaged IC is as secure to an attacker with advanced FIB as to one without. Naturally, IC camouflaging alone is not the answer, since specific attacks against IC camouflaging exist, and mass-produced devices are reverse engineered all the time; nevertheless, existence of essential steps in probing attacks suggest there are ways to obstruct FIB-based probing attack in addition to blocking it head-on.

Existing devices that lack protection

In challenges, we have touched on the problem that most existing countermeasures demand large area and layer overheads and fail to account for devices with tighter margins. This leaves a great opportunity for the future research because not only do the most threatened devices often have limited resources, the proliferation of electronic devices into society (e.g., expansion of IoT) will bring more such devices and more types of devices for which no antiprobing protection has been proposed. Although it is unrealistic to expect a resource-restricted device to beat FIB-based milling, we believe that there can still be two possible approaches to provide protection for resource-strained devices: 1) model the capabilities of likely attackers against such devices (e.g., identity thieves for smartcards) and customize protection for low cost devices accordingly or 2) focusing on foiling attack stages where the advantage of a FIB is not used, e.g., the reverse engineering stage we discussed earlier.

Potential efficiency and applicability improvements

We believe that existing countermeasure design approaches can be made more efficient by establishing probing-aware CAD flows that utilize functional design information to augment countermeasure design. This would enable integration of the functional and countermeasure design in a holistic fashion that balances design constraints and resource limitations. Further, the reliability of countermeasures depends heavily on factors such as process, voltage and temperature variation, which could also benefit from a probing-aware CAD flow. In such a case, the flow should be able to automatically identify the assets at the RTL, identify the respective sensitive nets in the gate-level netlist, and finally ensure these nets are protected and there are effective test mechanisms in place to ensure the probing attack is detected during power-up mode. In addition to reducing overheads and improving reliability, a security-aware CAD flow could further expand existing approaches in two ways: providing security evaluations, and exploring new design techniques. Security evaluations have a number of uses: identifying critical wires, evaluating how probeable certain wires are, evaluating overall overheads, and improving antiprobing security. Metrics need to be developed for all these tasks, which will only be possible with a probing-aware CAD flow. Integrating security evaluation to layout design flow could also make it easier for design teams with less experience in antiprobing countermeasures to improve their designs against potential threats. The flow could also enable previously impossible design choices in existing countermeasure approaches: for example, an internal active shield can be constructed with functional wires carrying nonsensitive information on optimized layers and layout locations, eliminating the dilemma between using undesirable layers and precluding them from design use. This displaces the need to devote entire metal layers to such protection thereby lowering costs further. With a holistic CAD flow, asset carrying wires that may become potential target wires in a probing attack could also be identified and placed under emphasized protection.

Devices other than ASIC or SoC (e.g., FPGA) will likely require further customization of the CAD flow. The innate difference in device architectures will doubtlessly impact countermeasure design methodology greatly. For example, it is unlikely to insert shields into FPGA models without one built-in; on the other hand, the flexible nature of the bitstream might make it possible for wires carrying assets to be harder for attacker to locate.

DUE TO THE PROLIFERATION of IC diagnosis, debug, and failure analysis equipment, the technological

requirements to perform physical attacks on security critical ICs is dramatically declining. Further, considering the powerful capability of FIB-equipped adversaries, probing attacks have become an enormous threat to ICs for security critical applications. In this article, we have reviewed the state-of-the-art and essential stages of probing attacks, as well as existing countermeasure techniques and their limitations. Based on surveyed status of probing countermeasures, we described the most critical challenges and proposed the future research opportunities. We expect this paper to serve as a foundation for motivation and development of future methodologies that protect against probing and possibly other invasive physical attacks. ■

Acknowledgments

This work was supported in part by AFOSR MURI Grant under Award FA9550-14-1-0351 and a Grant from NSF/SRC STARSS Program.

References

[1] J.-M. Cioranesco, et al., "Cryptographically secure shields," in *Proc. 2014 IEEE Int. Symp. Hardware-Oriented Secur. Trust*, May 2014, pp. 25–31.

[2] S. Manich, M. Wamser, and G. Sigl, "Detection of probing attempts in secure ICs," in *Proc. 2012 IEEE Int. Symp. Hardware-Oriented Secur. Trust*, Jun. 2012, pp. 134–139.

[3] Y. Ishai, A. Sahai, and D. Wagner, "Private circuits: Securing hardware against probing attacks," in *Advances in Cryptology-CRYPTO 2003*, D. Boneh, Ed. Berlin, Germany: Springer, 2003, pp. 463–481.

[4] ARM Inc., "Building a secure system using TrustZone Technology." accessed Jul. 13, 2017. [Online]. Available: http://infocenter.arm.com/help/topic/com.arm.doc.prd29-genc-009492c/PRD29-GENC-009492C_trustzone_security_whitepaper.pdf

[5] Q. Shi, N. Asadizanjani, D. Forte, and M. Tehranipoor, "A layout-driven framework to assess vulnerability of ICs to microprobing attacks," in *Proc. IEEE Int. Symp. Hardware Oriented Secur. Trust*, May 2016, pp. 155–160.

[6] C. Boit, C. Helfmeier, and U. Kerst, "Security risks posed by modern IC debug and diagnosis tools," in *Proc. Workshop Fault Diagnosis Tolerance Cryptography*, Aug. 2013, pp. 3–11.

[7] S. Skorobogatov, "Physical attacks on tamper resistance: Progress and lessons," in *Proc. 2nd ARO Special Workshop Hardware Assurance*, Washington, DC, USA, 2011.

[8] S. Quadir, et al., "A survey on chip to system reverse engineering," in *ACM J. Emerg. Technol. Comput. Syst.*, vol. 13, no. 1, Article 6, Apr. 2016.

[9] J. Rajendran et al., "Security analysis of integrated circuit camouflaging," in *Proc. ACM SIGSAC Conf. Comp. Commun. Secur.,* 2013.

[10] C. Tarnovsky, "Security failures in secure devices," in *Proc. Black Hat DC Presentation,* vol. 74, Feb. 2008.

[11] S. Skorobogatov, "The bumpy road toward iPhone 5c NAND mirroring," arXiv preprint arXiv:1609.04327, 2016.

Huanyu Wang has been a PhD student at the Electrical and Computer Engineering Department, University of Florida, since 2016. He received an MS degree in electrical engineering from Northwestern University in 2015. His research interests include hardware security and trust.

Domenic Forte is currently an Assistant Professor with the Electrical and Computer Engineering Department, University of Florida. His research interests include hardware security and investigation of hardware security primitives, hardware Trojan detection and prevention, security of the electronics supply chain, and reverse/antireverse engineering.

Mark M. Tehranipoor is currently the Intel Charles E. Young Preeminence Endowed Professor in Cybersecurity at the University of Florida. His research interests include hardware security and trust, supply chain security, Internet of Things security, and VLSI design test and reliability.

Qihang Shi is currently a PhD student at the Department of Electrical and Computer Engineering, University of Connecticut. He received an MS degree in SoC from Lund University in 2005. His research interests include hardware security and trust and VLSI test and reliability.

■ Direct questions and comments about this article to Huanyu Wang, University of Florida, Gainesville, FL 32611 USA; e-mail: huanyuwang@ufl.edu.