International Journal of Advanced Science and Technology
Vol.127 (2019), pp.13-24
http://dx.doi.org/10.33832/ijast.2019.127.02

IMPROVING THE PHYSICAL SECURITY OF MICROCHIPS AGAINST SIDE-CHANNEL ATTACKS

Dominik Malčík and Martin Drahanský

Department of Intelligent Systems, Faculty of Information Technology, Brno University of Technology, Božetěchova 2, 612 66 Brno, Czech Republic
imalcik@fit.vutbr.cz, drahan@fit.vutbr.cz

***Abstract*— Nowadays, microchips are virtually everywhere, from simple home devices to confidential military equipment. We must not forget the medical systems that have a great impact on our quality of life as well. As can be seen, the importance of these tiny integrated circuits is immense. Preserving the reliability of these devices and the confidentiality of data these devices are processing is absolutely substantial. The integrated circuit (IC) industry has been rapidly evolving in recent decades and employing ICs is becoming normal and inevitable in nearly all aspects of our lives. The initial IC evolution era paid attention primarily to the technological evolution itself. Aspects like security were always one step back due to the fallacious feeling of the inherent security of these very tiny components. After realizing that the opposite is true, we have to focus on securing the critical devices against tampering, information theft, counterfeiting, etc.**

***Keywords*— Integrated circuit, 3D IC, physical security, reverse engineering, side-channel attack, FPGA**

1. INTRODUCTION

This paper is devoted to providing proposals on hardening a subset of possible hardware-oriented attacks on microchips. As our main area of interest is the protection of personal documents that employ a kind of cryptographic hardware, the primary objective of this paper is to proceed with propositions on improving the physical security of microchips against a subset of so-called semi-invasive attacks that are widely used against cryptographic hardware and smartcards.

Recently, we have seen many papers covering the split manufacturing process that allows building reliable and trustworthy devices, at least from the producers' perspective [1-6]. In this paper we would like to propose possible techniques for hindering attempts on gaining knowledge from the physical examination of chips. With employing recent technologies like 3D integration, MEMS, integrated energy source, etc., we would like to display the possibilities in making the chips more secure against commonly-used semi-invasive analysis techniques.

We will not consider the price aspect in the following chapters, because what is expensive for one use case, may be acceptable for another one. At the end of the day, the price always significantly influences the final design and many decisions made along the way to the market. As we do not want to present a concrete example where it would be possible to assess the adequacy of a particular countermeasure, let us propose and describe various possibilities for increasing the security of microchips, regardless of their respective prices.

Received: March 21, 2019
Reviewed: May 29, 2019
Accepted: June 6, 2019

ISSN: 2207-6360 IJAST

An abrupt background for this paper is provided through a brief introduction into side-channel attacks in Chapter 2. Chapters 3, 4, 5, 6, and 7 present the main contribution of this work; proposals for security enhancements. A short conclusion is stated in Chapter 8.

2. SIDE-CHANNEL ATTACKS

Side-channel attacks, a subset of non-invasive or semi-invasive attacks [7], [8] are among favorite attack types due to relative simplicity of their execution compared to invasive attacks. This does not imply that performance of such attacks is in all cases effortless. In some scenarios it might not be necessary to decapsulate the observed specimen. The specimen can be powered on encapsulated in its original package and measurements of examined quantities, *e.g.*, heat radiation, power consumption, radiation in general, acoustic analysis, can be carried out. However, some of the observation schemes require full or at least partial decapsulation. For example, backside imaging, microprobing or more precise measurements of the formerly mentioned quantities.

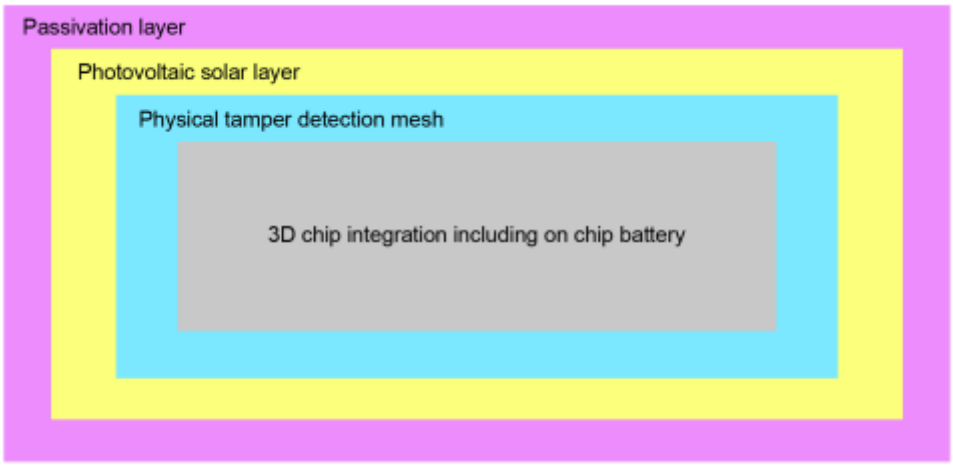

Fig. 1 Simplified Composition of a Chip with Active Tamper Detection

3. ACTIVE DEFENSE AGAINST MICROPROBING

Targets in a microprobing attack are mostly internal buses or signals that are not freely accessible via standard contact pads. When connecting to these internal signals, adversaries can reveal signals and data that are meant to be shielded from the outside world. Before employing microprobing, the chip has to be at least partially decapsulated and then appropriately tampered. First, an analysis should take place in order to figure out the areas of interest, simply put, to figure out where exactly to place the needles. After a successful analysis, the aimed contacts have to be exposed for the microneedles.

Our aim is to protect the chips from tampering attempts, intrusion, or the analysis of its physical structure that reveals its internal arrangement. In Chapter 3.1, we propose the employment of active tamper detection in order to detect undesirable manipulation with a chip as well as measures protecting the data processed inside the chip from being disclosed.

The countermeasures proposed in the upcoming chapters have the following stages – the first stage is the active tamper detection mechanism and the consequent stage is then the reliable removal of the memory contents (Chapter 3.1) and/or damaging the circuit itself (Chapter 5). With successful tamper detection and consequent memory erasure, the examined chip might have a significantly decreased value for adversaries. To be able to remove memory contents, masked-

ROM, and other similar inerasable memory types should be avoided in the chip's design.

3.1. ACTIVE TAMPER DETECTION WITH ACTIVE MEMORY PROTECTION

An active tamper detection shield should consist of several physical layers aimed at the possible ways of intrusion. Partial or complete decapsulation is one of the first steps when targeting invasive investigation of chips, such as microprobing. After opening a package, there should be natural or artificial light entering and interacting with the chip's surface. Therefore, the very first detector would be a light-sensing layer on top of the chip. Ideally, it should cover the whole chip surface to ensure that even partial openings trigger the alarm.

The second anti-tamper layer should be a fine-pitch sensing mesh against attempts of penetration into the chip. Even small-sized FIB editing has to be detectable by this layer in order to not allow any modifications that could possibly lead to the restriction of active shield functionality, memory bus exposure, etc.

The anti-tamper layer can be actively powered by a battery to regularly check the integrity of the mesh, even while it is unpowered. Discoveries and the successful development of micro batteries suitable for direct integration into ICs with optimization of ICs power consumption [9-12] will allow us to do just that. Due to the growing complexity of chips, we do not expect batteries to be capable of powering the whole chip for an exceptionally long time. Nevertheless, if we focus strictly on keeping only the protective functionality alive, this might result in a decent time for active tamper detection endurance, even without an external power source. Furthermore, recent endeavors in the field of energy generation can lead us to mechanisms that are able to refill the integrated battery and hence allow the exceptional endurance of active tamper detection. Let us name especially VEH (Vibration Energy Harvest) based on MEMS (Micro-Electro-Mechanical Systems) [13-15], Thermoelectric generation based on parasitic load of the device [16-15] and Photovoltaic solar power generation [15], [17], [18], which can be sensing package decapsulation at the same time. Due to the fact that decapsulation and chip preparation for microprobing (or reverse engineering in general) is not a fast process, the check can be set to always run after a certain period. This interval has to be designed with respect to the power demands of the whole active shield circuit and the capacity of the integrated battery. It can be expected that the parameters of the batteries will be significantly improved over the coming years. Therefore, this active shield use case will be supported even more. As microprobing is performed under load, this battery-backed active sensing is not absolutely necessary for defense against it due to the present power source during examination. However, for some use cases or other attack scenarios (*e.g.*, reverse engineering), this might be a way to go.

In Figure 1, we provide a simplified view of a chip structure with respect to the proposed active protection. As there are many attacks led from the "backside" of a chip, we recommend using 3D integration with a back-to-back connection to have a 3D chip with only the frontal portion facing the packaging. Therefore, passivation, photovoltaic detection/generation, and physical tamper detection layers are used around the entire structure of the chip. A potential battery is expected to be placed inside the 3D integration.

As soon as the outer package is (partially) removed, the photovoltaic solar layer produces energy. This should be the signal to immediately remove memory content. Memory content removal should ideally be a battery-powered action. When considering no battery in the chip layout, at least an erasure flag should be set immediately and the memory has to be erased directly after powering the chip. In cases when the attackers are somehow able to disable the photovoltaic layer, their next step would be tampering with the device in order to prepare spots for placing microneedles for microprobing. Once the

physical layer tamper detection mesh is touched, the same memory-erase signal shall be triggered.

For enabling the battery-powered memory erasure scenario, the used memory modules should have low energy demand. When the battery reaches its critical low level of charge (the minimum charge needed for memory erasure), it should automatically erase the memory content in order to devalue the chip. This low-charge status can occur when the battery is not recharged via any of the implemented mechanisms or if it is malfunctioning.

In various scenarios, we can more or less rely on the battery's recharging mechanisms (TEG, VEH, Photovoltaic or simply when powered on by external power supply), thus prolonging active shield durability.

Considering our previous work where we dealt with personal e-documents and chips inside those (e-passports, ID cards, ILR, …), let us provide a whole scenario for a battery-powered active tamper detection use case. Our theoretical assumption might be that we are able to power the active tamper shield with an IC-integrated battery for at least n years. If the document is on the move with its holder, the battery is automatically recharged because of the integrated VEH system. If the document is used, it is recharged as well, with power obtained from the document reader and because of the heat produced by the chip (thermoelectric generation). The worst-case scenario is when the document is stored in a drawer and never used during the n year period. In this case, the battery slowly discharges. When it reaches its low charge limit, the chip itself should trigger the command for memory erasure, making the document invalid. Going even further, there might be a battery status indicator (low, mid, high), based on e-ink technology (low power consumption, only when switching states), showing the user if the personal document chip needs to be recharged in order to keep it valid for longer time period.

Furthermore, due to the very rapid development of technologies, it can be expected that such chips for holding e-documents will be implanted into human bodies soon [19-21]. It can be as easy as implanting an RFID chip under the human skin. Such a chip will have direct access to a power source in the form of the heat produced by a human body. Under these circumstances, we will not have to think about the endurance of the internal battery that much, because of the constant power that is available. As soon as there is no thermal power, the chip will assume extraction from the body and shall start its memory erasure procedure based on the internal battery power. Aside from that, the body implanted chips will have direct access to biometric characteristics of the holder and will be able to detect counterfeit attempts.

4. DISABLING BACKSIDE OBSERVATIONS

Backside imaging can be considered an easy way of almost directly accessing the transistor layer with further scanning possibilities realized by photon-emission microscopy, laser voltage probing, laser voltage imaging, IR imaging, thermal emission imaging, *etc.*, [22-26].

The typical first step towards such backside observations is to decapsulate the back side of the chip, either by using wet etching or in this case employing the polishing technique. It is usually not necessary to remove the whole packaging, thus polishing is very suitable. Furthermore, when examining chips connected as a flip chip, it is very convenient to consider backside access.

Subsequently, there might be some obstacles in the form of various pads placed below the silicon part of the chip. These pads, whatever they are made of, have to be removed. Consequently, the silicon substrate has to be thinned down according to the chosen scanning technique (100 µm - 50 nm) [22-26]. After preparation as stated above, backside observations can take place.

Because the recent chips are becoming very complex in terms of layer count and the advanced level of materials used for metal and dielectric layers, results of many observation techniques may become meaningless in such a tangle of metallic and nonmetallic structures. Therefore, ideas to inspect transistors directly from the backside while preserving the whole chip structure above it were presented. This allows active observations with specimens to be in full operation, while only the backside is exposed.

Our proposal for disabling the techniques using backside access is to employ 3D integration, as mentioned in Chapter 3.1, so that there is no real backside of a chip directly accessible (see Figure 1). Ideally, there should always be the frontal part of the chip facing the outer world from all angles. Let us assume a realistic 3D setup with back-to-back bonded chips. In this chip layout, there is no backside exposed or easily accessible. One can object that one of the chips in the 3D layout can be removed and thus the backside of the other chip might be exposed. Nevertheless, the removal of one of the chips from the 3D layout makes active backside observations of a specimen under operation practically impossible, because the chip setup is designed to operate as whole, not separately.

This is also another proposal to design the chips to work only when correctly interconnected. When a chip is taken out of a 3D layout, it should be able to detect it due to missing signals, different delays of signals, etc. In 3D back-to-back design, through silicon vias (TSV) are very likely to be in place in order to interconnect the particular chips. These vias can ensure the integrity of the whole layout - physical properties of particular TSVs can be checked by the chips, and thus the chip can recognize a tamper attempt. In such cases, the observed chip can either completely refuse operation or it can intentionally operate in a different mode to confuse adversaries.

Backside protection mechanisms can be combined together with mechanisms proposed in this paper to provide as complex protection as possible. Let us name active tamper detection mechanisms and use FPGA for critical functionality. These mechanisms can serve as a fuse for incidents when the backside protection fails. Then, the adversary does not gain anything more than a less standard FPGA without a configuration file or bitstream.

5. ACTIVE DEFENSE AGAINST X-RAY OBSERVATION TECHNIQUE

Lately, X-ray has become a serious technology used in the observation of advanced chips [27], [28], [29]. As chips are turning into unimaginably complex devices, the classic method of invasive reverse engineering is becoming harder to be successfully performed. With the recent progress of X-ray technology itself, it seems that reverse engineering is no longer practical compared to X-ray imaging. As a conclusion, we have to consider all chip structures disclosed at any time, even without being physically penetrated.

Protecting a chip against X-ray exploration, which is basically a kind of non-invasive reverse engineering, by implementing its key parts inside a fully integrated FPGA circuit is not a novel idea in principle. The concept is based on the fundamental presumption that FPGA is composed of visually similar cells that change their behavior according to the configuration loaded upon power up. However, there exist attacks against such implementations [30-32], focusing on the reconstruction of the FPGA configuration bitstream, thus essentially gaining a netlist of the circuit. In fact, reading out the structure of the FPGA without its configuration is practically worthless. And that is also our aim, to allow attackers to freely read out the chip structure without leaking any relevant information.

In order to avoid these attacks, we have to protect the main memory that holds the FPGA configuration data and buses against information leakage. We propose using active tamper detection with active memory protection that was presented in Chapter 3.1.

Protection against X-rays or against ionizing radiation has to also employ a protection mechanism against these non-invasive observation techniques. Either radiation detectors have to be placed inside the chip structure [33, 34], or according to recent research in physical chemistry, it is possible to turn X-ray radiation directly into electricity through the use of nanomaterial. This might be used as a sensing technique for triggering proposed memory erasure procedures in a similar way as in Chapter 3.1.

Regardless of the practical implementation of X-ray sensing, the described setup should ensure that when radiation exceeds a given threshold, an alarm is triggered. Whenever there is the alarm triggered, all configurations of the key functionality implemented in FPGA has to be reliably deleted. The attackers then gain a worthless chip with general purpose FPGA.

6. PASSIVE DEFENSE AGAINST X-RAY

For hardening radiation-based techniques, standard passive methods like cell camouflaging [35], [30], [36], [37], [6], [38], [39], [40], previously described FPGA employment, and more can be used. The presumption for using these approaches is that it is possible to make cells visually similar, thus allowing an attacker to display their physical representation might be acceptable. As stated before, protection against X-ray imaging is not unlike the protection against physical reverse engineering.

Among others, it is possible to use materials that are used in general for radiation hardening, especially in space industry, *e.g.*, borophosphosilicate glass [41]. The chip package can be constructed from materials that will make X-ray scanning difficult (however, this research field is not covered in this paper). Therefore, it would be needed to decapsulate the chip first. At this point, active tamper detection presented in this paper can be used for package intrusion detection.

6.1. VISUALLY UNREADABLE NON-VOLATILE MEMORY TYPES

Vastly used, cheap masked ROM memories can literally be read out after proper imaging with an X-ray or after delayering a device [30], [42], [43], [44]. To deflect an information breach, we recommend to completely abandon using masked ROM memory types and those with similar features (readability of stored values, *e.g.*, [30], [45], [43]; impossible to erase/rewrite content). This step will help us keep the stored information as optically unreadable and will also give us the opportunity to employ the defense scenario presented in Chapter 3.1 and Chapter 5.

The implementation of memory encryption might seemingly be enough for protecting the plain content stored in memory cells. Unfortunately, fraudsters can often find a way to decipher the stored information [46], [47], [48] – either by finding the right key or reading out the data after it is decrypted by the device itself with the use of microprobing. Generally, one more step towards security would be to not disclose the memory content at all, regardless of the encryption used.

6.2. CELL CAMOUFLAGING

Cell camouflaging and circuit obfuscation are known techniques described in several research papers [36], [37], [49], [35], [40], [38], [39], [30], [6], [50]. It is known that this technique is expensive because of the aerial demands, and so it is impossible to camouflage the whole IC. Moreover, the security impact can be of a much lower extent than expected during the design process [2], [40], [35], [49], [39]. Furthermore, it is possible to observe obfuscated cells through a series of cross-section slices with a properly set milling step. With this approach, it can be determined which contacts are actually connected and which ones are just fake. Such advanced cross-sectioning is achievable with FIB milling or with X-rays [30], [51], [28], [27].

Let us introduce the possibility to disable this cross-sectional analysis of camouflaged cells with the employment of inductive or capacitive contactless connections, where some of the contacts in the camouflaged cell can be fake without showing any visual difference. This potential enhancement also has its drawbacks, *e.g.*, spatial and power requirements, heat dissipation, and side-channel attack support. However, camouflaged cells are spacious even with physical contacts. With wise design, we might get to the same spatial needs and a potentially similar camouflage effect. The fake contacts will be visually indistinguishable from the real ones. It is clear that the use of this type of obfuscation in a single die has to be very limited because of its drawbacks [52], [53], [54], [55]. Nevertheless, it would be one more measure against potential adversaries.

The drawbacks of the above-mentioned wireless connections can be paradoxically turned into active defensive mechanisms against side-channel attacks. This approach will be presented in Chapter 7.

6.3. 3D INTEGRATION WITH DUMMY DIES

There are many unused or recycled old dies available on the market (which are widely used by fraudster foundries in fallaciously new integrations [56-65]) and these can be used for increasing the complexity of 3D integrations. Although this artificial complexity bloat will not prevent adversaries from performing an analysis of the chips, the intricacy of the integration can be raised. The time consumed for the determination of the dummy part might help discourage adversaries.

We propose to use dies with diverse technological nodes for 3D integration. Each node requires a distinct approach for observation and analysis. The interconnection between the dummy part of the integration with the truly used segments of the chip will be important. When connected sloppily, an attacker might suspect the fake part. The correct employment of this measure requires thoughtful placement and linking within the 3D IC.

The disadvantages of this solution are mainly technological. Because thermal management is one of the most important aspects to be dealt with in 3D integration, adding more unnecessary dies into integration makes the situation even worse. When we consider connecting the dummy part electrically to confuse the attackers as much as possible, more power will be consumed and more heat radiated into the 3D IC. Therefore, the implementation of this measure has to be carefully judged at the design stage. On the other hand, increasing security is in some use cases so valuable that it might be worth spending the extra effort on camouflaging the design with dummy parts.

7. POWER, THERMAL, AND TIMING CAMOUFLAGING

The chips are very often analyzed in a way of reading out power consumption, thermal emissions or time spent within the performance of some operations [66], [67], [68]. The better control over the input parameters, the better starting point for the analysis.

As a prerequisite to the ability to influence values obtained from such analyses, the chip has to be able to generate truly random events. The second precondition would be to place several inductive and/or capacitive contactless connections (as mentioned in Chapter 6.2) into the chip layout. Not only do we contribute to the physical camouflaging, with this employment we can also influence side-channel outputs. Some parts of the important functionality can then be physically realized in multiple traces – direct, with longer conductive lines, with contactless connections. Unfortunately, the design phase will get to a new level of complexity due to variable delays, consumption, thermal properties, spatial requirements, production price, etc. However, if the designers manage usability of the worst trace of each function, then the chip might respond in a pseudo-random way to the same inputs. We use pseudo-random, because implementation in hardware will give us limited amounts of interconnections, thus only pseudo-

randomity. Nevertheless, by using few contactless connections, we may introduce a portion of noise into the measured side-channel signals. This can provide more ambiguity into the signal interpretations and measurements.

We recommend going even further to implement several segments of an operation in multiple ways, so that the final operation will consist of several segments, whereas each segment will have several implementations with various features. In every segment, the trace could be independently chosen on the fly based on the random generator. This would give us many combinations for one functionality with hard-to-distinguish and map side-channel signals.

Another possibility for the application of a similar principle would be to employ FPGA and reconfigure, or partially reconfigure, the FPGA in random times, so that the same operation will use different FPGA cells for the same functionality; the effect may be alike. The reconfiguration should be ideally based on random event generation and thus achieving a potentially larger state space. This can lead to a quite complex solution primarily limited by the size of the FPGA.

8. CONCLUSION

This paper presented enhancements for improving the security of microchips. Our proposals were primarily aimed at hindering so-called semi-invasive attacks, especially the subset of side-channel attacks. Novel ways of securing microchips are available. But on the contrary, it can be also expected that all proposed measures might be at some point broken and recognized as insufficient. Improving security is simply an endless fight with adversaries that are tirelessly investigating every newly implemented protection mechanism.

ACKNOWLEDGMENTS

This work was supported by The Ministry of Education, Youth and Sports of the Czech Republic from the National Programme of Sustainability (NPU II); project IT4Innovations excellence in science – LQ1602 and the BUT project Secure and Reliable Computer Systems FIT-S-17-4014.

REFERENCES

[1] Xie, Y., Bao, C., Serafy, C., Lu, T., Srivastava, A., Tehranipoor, M., “Security and vulnerability implications of 3D ICs”, IEEE Transactions on Multi-Scale Computing Systems, vol. 2, no. 2, (2016), p. 108-122. DOI: 10.1109/TMSCS.2016.2550460

[2] Imeson, F., Emtenan, A., Garg, S., Tripunitara, M., “Securing computer hardware using 3D integrated circuit (IC) technology and split manufacturing for obfuscation”, In Proceedings of the 22nd USENIX Security Symposium (USENIX Security 13). Washington D.C. (USA), ISBN 978-1-931971-03-4, 8, (2013), pp. 495-510.

[3] Dofe, J., Yu, Q., Wang, H., Salman, E., “Hardware security threats and potential countermeasures in emerging 3D ICs”, In Proceedings of the 2016 International Great Lakes Symposium on VLSI (GLSVLSI). New York (USA), ISBN: 978-1-4503-4274-2, 5, (2016), pp. 69-74, DOI: 10.1145/2902961.2903014.

[4] Dofe, J., Gu, P., Stow, D., Yu, Q., Kursun, E., Xie, Y., “Security threats and countermeasures in three-dimensional integrated circuits”, In Proceedings of the on Great Lakes Symposium on VLSI 2017. New York (USA), ISBN: 978-1-4503-4972-7, 5, (2017), pp. 321-326, DOI: 10.1145/3060403.3060500

[5] Gu, P., Li, S., Stow, D., Barnes, R., Liu, L., Xie, Y., Kursun, E., “Leveraging 3D technologies for hardware security: opportunities and challenges’, In Proceedings of the 26th edition on Great Lakes Stmposium on VLSI (GLSVLSI’16). New York (USA), ISBN: 978-1-4503-4274-2, 5, (2016), pp. 347-352, DOI: 10.1145/2902961.2903512.

[6] Shakya, B., Asadizanjani, N., Forte, D., Tehranipoor, M., “Chip editor: Leveraging circuit edit for logic obfuscation and trusted fabrication”, In Proceedings of the 35th International Conference on Cumputer-Aided Design. New York (USA), ISBN: 978-1-4503-4466-1, 11, (2016), pp. 30:1-30:8, DOI: 10.1145/2966986.2967014.

[7] Skorobogatov, S. P., "Semi-invasive Attacks - A New Approach to Hardware Security Analysis (technical report)", 144 pages. [Online] Cited 2019-01-31. Available at: https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-630.pdf
[8] Fievrea, A. M. P., Rogersb, A.-A. A., Bhansalia, S., "Integrated circuit security: an overview", Journal of Institute of Smart Structures and Systems (ISSS), ISSN 2319-6408, vol. 4, no. 1, (2015), pp. 18-37.
[9] Carmo, J. P., Rocha, R. P., Silva, A. F., Goncalves, L. M., Correia, J. H., "Integrated thin-film rechargeable battery in a thermoelectric scavenging microsystem", In Proceedings of the 2009 International Conference on Power Engineering, Energy and Electrical Drives. Lisbon (Portugal), 3, (2009), pp. 359-362, DOI: 10.1109/POWERENG.2009.4915179.
[10] Ke, S., Teng-Sing, W., Yeop, A. B., Yoon, S. J., Dillon, S. J., Lewis, J. A., "3D Printing of interdigitated li-ion microbattery architectures", Advanced Materials, vol. 25, no. 33, (2013), pp. 4539-4543, DOI: 10.1002/adma.201301036.
[11] Ning, H., Pikul, J. H., Zhang, R., Li, X., Xu, S., Wang, J., Rogers, J. A., King, W. P., Braun, P., "Holographic patterning of high-performance on-chip 3D lithium-ion microbatteries", In Proceedings of the National Academy of Sciences of the United States of America, vol. 112, no. 21, (2015), pp. 6573-6578, DOI: 10.1073/pnas.1423889112.
[12] Tamta, A., Arya, R., "A review on various leakage power reduction techniques in deep submicron technologies in CMOS VLSI circuits", In Proceedings of the International Journal of Energy Technology and Management, vol. 1, no. 2, (2017), pp. 17-22, DOI: 10.21742/ijetm.2017.1.2.03.
[13] Ali, I., Khir, M. H. M., Baharudin, Z., Ashraf, K. CMOS-MEMS multiple resonant vibration energy harvester for wireless sensor network. In Proceedings of the 2015 IEEE Regional Symposium on Micro and Nanoelectronics (RSM). Kuala Terengganu (Malaysia), 8, (2015), pp. 1-4, DOI: 10.1109/RSM.2015.7354963.
[14] Cottone, F., Basset, P., Guillemet, R., Galayko, D., Marty, F., Bourouina, T., "Non-linear MEMS electrostatic kinetic energy harvester with a tunable multistable potential for stochastic vibrations", In Proceedings of the 2013 Transducers Eurosensors XXVII: The 17th International Conference on Solid-State Sensors, Actuators and Microsystems (TRANSDUCERS EUROSENSORS XXVII). Barcelona (Spain), ISBN: 978-1-4673-5983-2, 6, (2013), pp. 1336-1339., DOI: 10.1109/Transducers.2013.6627024.
[15] Dini, M., "Nano-Power Integrated Circuits for Energy Harvesting", 115 pages (doctoral thesis). [Online] Cited 2019-01-31. Available at: http://amsdottorato.unibo.it/6947/1/dini_michele_tesi.pdf.
[16] Fahad, H., Hasan, M., Li, G., Hussain, M., "Thermoelectricity from wasted heat of integrated circuits", Applied Nanoscience, ISSN 2190-5517, vol. 3, no. 3, (2013), pp. 175-178, DOI: 10.1007/s13204-012-0128-2.
[17] Carvalho, C., Paulino, N., "CMOS Indoor light energy harvesting system for wireless sensing applications", 1st ed. Cham (Switzerland): Springer International Publishing, (2016), ISBN: 978-3-319-37360-7.
[18] Sabarillo, R. M., Mocorro, C. O., "Indoor light energy harvesting system for battery recharging and wireless sensor networks implemented in 90nm CMOS technology", In 2015 International Conference on Humanoid, Nanotechnology, Information Technology, Communication and Control, Environment and Management (HNICEM). Cebu City (Philippines), 12, (2015), pp. 1-5, DOI: 10.1109/HNICEM.2015.7393174.
[19] Wikipedia contributors. Microchip Implant (Human) — Wikipedia, The Free Encyclopedia, [Online] Cited 2019-01-31. Available at: https://en.wikipedia.org/w/index.php?title=Microchip_implant_(human)&oldid=892461589
[20] Udalagama, C. J. Electrical energy generation from body heat. In Proceedings of the 2010 IEEE International Conference on Sustainable Energy Technologies (ICSET). Kandy (Sri Lanka), 2010, p. 1–5. DOI: 10.1109/ICSET.2010.5684932
[21] Perakslis, C., Michael, K., Michael, M. G., Gable, R. Perceived barriers for implanting microchips in humans: A transnational study. In Proceedings of the 2014 IEEE Conference on Norbert Wiener in the 21st Century (21CW). Boston (MA, USA), 2014, p. 1–8. DOI: 10.1109/NORBERT.2014.6893929
[22] Boit, C., Schlangen, R., Glowacki, A., Kindereit, U., Kiyan, T., Kerst, U., Lundquist, T. R., Kasapi, S., Suzuki, H. Physical IC debug - Backside approach and nanoscale challenge. Advances in Radio Science - Kleinheubacher Berichte, 2008, vol. 6, no. 5, p. 265–272. DOI: 10.5194/ars-6-265-2008
[23] Chen, S., Shinseki, B., Barutha, C., Kha, T. Infrared imaging and backside failure analysis techniques on multilayer CMOS technology. In Proceedings of the 1997 6th International Symposium on the Physical and Failure Analysis of Integrated Circuits. Singapore, 1997, p. 17–20. ISBN: 0-7803-3985-1. DOI: 10.1109/IPFA.1997.638066
[24] Skvortsov, D., Ng, Y.S., Lundquist, T., Liao, J., Kasapi, S., Marks, H. Laser Voltage Imaging: A New Perspective of Laser Voltage Probing. In Proceedings of the 36th International Symposium for Testing and Failure Analysis (ISTFA 2010). Texas (USA), 2010, p. 5–13. ISBN: 9781615030415
[25] Thorne, S., Ippolito, S., Eraslan, M., Goldberg, B., Unlu, M. S., Leblebici, Y. High resolution backside thermography using a numerical aperture increasing lens. In Proceedings of the 29th International Symposium for Testing and Failure Analysis. Santa Clara (USA), 2003, p. 3.

[26] Vigil, K., Lu, Y., Yurt, A., Abanoz Cilingiroglu, T., Bifano, T. G., Unlu, M. S., Goldberg, B. B. Integrated circuit super-resolution failure analysis with solid immersion lenses. Electronic Device Failure Analysis, 2014, vol. 16, no. 2, p. 26–32.
[27] Guizar-Sicairos, M., Holler, M., Odstrcil, M., Raabe, J. High resolution 3D imaging of integrated circuits by x-ray ptychography. In Proceedings of the Image Sensing Technologies: Materials, Devices, Systems, and Applications V, Orlando (USA), 2018, p. 8. DOI: 10.1117/12.2304835
[28] Courtland, R. 3D X-ray tech for easy reverse engineering of ICs. IEEE Spectrum, 2017, vol. 54, no. 5, p. 11–12. DOI: 10.1109/MSPEC.2017.7906884
[29] Courtland, R. X-rays Map The 3D Interior of Integrated Circuits. [Online] Cited 2017-3-17. Available at: https://spectrum.ieee.org/nanoclast/semiconductors/processors/xray-ic-imaging
[30] Quadir, S. E., Chen, J., Forte, D., Asadizanjani, N., Shahbazmohamadi, S., Wang, L., Chandy, J., Tehranipoor, M. A Survey on Chip to System Reverse Engineering. ACM Journal on Emerging Technologies in Computing Systems (JETC), 2016, vol. 13, no. 1, p. 6:1–6:34. DOI: 10.1145/2755563
[31] Fyrbiak, M., Strauß, S., Kison, C., Wallat, S., Elson, M., Rummel, N., Paar, C. Hardware reverse engineering: Overview and open challenges. In Proceedings of the 2017 IEEE 2nd International Verification and Security Workshop (IVSW). Thessaloniki (Greece), 2017, p. 88–94. DOI: 10.1109/IVSW.2017.8031550
[32] Moradi, A., Barenghi, A., Kasper, T., Paar, C. On the vulnerability of FPGA bitstream encryption against power analysis attacks: extracting keys from xilinx Virtex-II FPGAs. In Proceedings of the 18th ACM Conference on Computer and Communications Security. New York (NY USA), 2011, p. 111–124. DOI: 10.1145/2046707.2046722
[33] Pikhay, E., Roizin, Y., Nemirovsky, Y. Ultra-low power consuming direct radiation sensors based on floating gate structures. Journal of Low Power Electronics & Applications, 2017, vol. 7, no. 3, p. 20–22. DOI: 10.3390/jlpea7030020
[34] Kwon, I. Integrated Circuit Design for Radiation Sensing and Hardening (dissertation thesis). 107 pages. [Online] Cited 2019-01-31. Available at: https://deepblue.lib.umich.edu/bitstream/handle/2027.42/111548/iykwon_1.pdf?sequence=1&isAllowed=y
[35] Rajendran, J., Sam, M., Sinanoglu, O., Karri, R. Security analysis of integrated circuit camouflaging. In Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security. New York (NY USA), 2013, p. 709–720. ISBN: 978-1-4503-2477-9. DOI: 10.1145/2508859.2516656
[36] Bi, Y., Shamsi, K., Yuan, J.-S., Gaillardon, P.-E., Micheli, G. D., Yin, X., Hu, X. S., Niemier, M., Jin, Y. Emerging technology-based design of primitives for hardware security. Journal on Emerging Technologies in Computing Systems, 2016, vol. 13, no. 3, p. 3:1–3:19. DOI: 10.1145/2816818
[37] Cocchi, R. P., Baukus, J. P., Chow, L. W., Wang, B. J. Circuit camouflage integration for hardware IP protection. In Proceedings of the 2014 51st ACM/EDAC/IEEE Design Automation Conference (DAC). San Francisco (CA, USA), 2014, p. 1–5. ISBN: 978-1-4799-3017-3. DOI: 10.1145/2593069.2602554
[38] Wang, X., Gao, M., Zhou, Q., Cai, Y., Qu, G. Gate Camouflaging-Based Obfuscation. 1st ed. Cham (Switzerland): Springer International Publishing, 2017, pp. 89–102. ISBN: 978-3-319-49018-2. DOI: 10.1007/978-3-319-49019-9_4
[39] Vijayakumar, A., Patil, V. C., Holcomb, D. E., Paar, C., Kundu, S. Physical design obfuscation of hardware: a comprehensive investigation of device and logic-level techniques. IEEE Transactions on Information Forensics and Security, 2017, vol. 12, no. 1, p. 64–77. DOI: 10.1109/TIFS.2016.2601067
[40] Shakya, B., Tehranipoor, M. M., Bhunia, S., Forte, D. Introduction to Hardware Obfuscation: Motivation, Methods and Evaluation. 1st ed. Cham (Switzerland): Springer International Publishing, 2017, p. 3–32. ISBN: 978-3-319-49018-2
[41] Yu, F.-X., Jia-Rui, L., Zheng-Liang, H., Hao, L., Zhe-Ming, L. Overview of radiation hardening techniques for IC design. Information Technology Journal, 2010, vol. 9, no. 6, p. 1068–1080. DOI: 10.3923/itj.2010.1068.1080
[42] Torrance, R., James, D. The state-of-the-art in semiconductor reverse engineering. In Proceedings of the 2011 48th ACM/EDAC/IEEE Design Automation Conference (DAC). New York (NY, USA), 2011, p. 333–338. ISBN: 978-1-4503-0636-2.
[43] Courbon, F., Skorobogatov, S., Woods, C. Reverse engineering flash EEPROM memories using scanning electron microscopy. In Proceedings of the 15th Smart Card Research and Advanced Application Conference (CARDIS 2016). Cannes (FR), 2017, p. 57–72. ISBN: 978-3-319-54668-1. DOI: 10.1007/978-3-319-54669-8_4
[44] Kryszczuk, K., Richiardi, J. Encyclopedia of Cryptography and Security. 2nd ed. Springer US, 2011. ISBN 978-1-4419-5906-5
[45] Courbon, F., Skorobogatov, S. Direct charge measurement in floating gate transistors of flash EEPROM using scanning electron microscopy. In Proceedings of the 42nd International Symposium for Testing and Failure Analysis (ISTFA). Texas (USA), 2016, p. 9. DOI: 10.17863/CAM.7629
[46] Skorobogatov, S. How microprobing can attack encrypted memory. In Proceedings of the 2017 Euromicro Conference on Digital System Design (DSD). Vienna (Austria), 2017, p. 244–251. ISBN: 978-1-5386-2146-2. DOI: 10.1109/DSD.2017.69

[47] Gueron, S. Attacks on encrypted memory and constructions for memory protection. In Proceedings of the 2016 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC). Santa Barbara (CA, USA), 2016, p. 1–3. ISBN: 978-1-5090-1108-7. DOI: 10.1109/FDTC.2016.20
[48] Han, S.-S, Cho, S.-J. NAND flash main memory database index management technique using the T* tree segment mapping log. In Proceedings of the International Journal of Urban Design for Ubiquitous Computing, 2018, vol. 6, no. 2, p. 7–12. DOI: 10.21742/ijuduc.2018.6.2.02
[49] Forte, D., Bhunia, S., Tehranipoor, M. M. Hardware Protection Through Obfuscation. 1st ed. Cham (Switzerland): Springer Publishing Company, 2017. ISBN: 978-3-319-49018-2. DOI: 10.1007/978-3-319-49019-9
[50] Chen, S., Chen, J., Forte, D., Di, J., Tehranipoor, M., Wang, L. Chip-level anti-reverse engineering using transformable interconnects. In Proceedings of the 2015 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFTS). Amherst (MA, USA), 2015, p. 109–114. ISBN: 978-1-4799-8606-4. DOI: 10.1109/DFT.2015.7315145
[51] Bajura, M., Boverman, G., Tan, J., Wagenbreth, G., Rogers, C., Feser, M., Rudati, J., Tkachuk, A., Aylward, S., Reynolds, P. Imaging integrated circuits with x-ray microscopy. In Proceedings of the 36th GOMACTech Conference. Orlando (FL, USA), 2011, p. 2.
[52] Davis, W. R., Wilson, J., Mick, S., Xu, J., Hua, H., Mineo, C., Sule, A. M., Steer, M., Franzon, P. D. Demystifying 3D ICs: the pros and cons of going vertical. IEEE Design Test of Computers, 2005, vol. 22, no. 6, p. 498–510. ISSN: 1558-1918. DOI: 10.1109/MDT.2005.136
[53] Drost, R. J., Hopkins, R. D., Ho, R., Sutherland, I. E. Proximity communication. IEEE Journal of Solid-State Circuits, 2004, vol. 39, no. 9, p. 1529–1535. ISSN: 1558-173X. DOI: 10.1109/JSSC.2004.831448
[54] Mick, S., Wilson, J., Franzon, P. 4 Gbps high-density AC coupled interconnection. In Proceedings of the IEEE 2002 Custom Integrated Circuits Conference (Cat. No.02CH37285). Orlando (FL, USA), 2002, p. 133–140. ISBN: 0-7803-7250-6. DOI: 10.1109/CICC.2002.1012783
[55] Kanda, K., Antono, D. D., Ishida, K., Kawaguchi, H., Kuroda, T., Sakurai, T. 1.27-Gbps/pin, 3mW/pin Wireless Superconnect (WSC) Interface Scheme (conference presentation). 20 pages. [Online] Cited 2019-01-31. Available at: http://lowpower.iis.u-tokyo.ac.jp/~kawapy/publications/ISSCC03WSCslides.pdf
[56] Guin, U., Huang, K., Dimase, D., Carulli, J. M., Tehranipoor, M., Makris, Y. Counterfeit integrated circuits: a rising threat in the global semiconductor supply chain. Proceedings of the IEEE, 2014, vol. 102, no. 8, p. 1207–1228. ISSN: 1558-2256. DOI: 10.1109/JPROC.2014.2332291
[57] Guin, U., Zhang, X., Forte, D., Tehranipoor, M. Low-cost on-chip structures for combating die and IC recycling. In Proceedings of the 2014 51st ACM/EDAC/IEEE Design Automation Conference (DAC). San Francisco (USA), 2014, p. 1–6. ISBN: 978-1-4799-3017-3. DOI: 10.1145/2593069.2593157
[58] Guin, U., Dimase, D., Tehranipoor, M. Counterfeit integrated circuits: detection, avoidance, and the challenges ahead. Journal of Electronic Testing, 2014, vol. 30, no. 1, p. 9–23. DOI:10.1007/s10836-013-5430-8
[59] Pecht, M., Tiku, S. Bogus: electronic manufacturing and consumers confront a rising tide of counterfeit electronics. IEEE Spectrum, 2006, vol. 43, no. 5, p. 37–46. ISSN: 1939-9340. DOI: 10.1109/MSPEC.2006.1628506
[60] Powell, D. Finding Solutions to China's E-waste Problem. p. 1. [Online] Cited 2019-01-31. Available at: https://unu.edu/publications/articles/assessing-and-improving-chinas-e-waste-problem.html
[61] Rajendran, J., Sinanoglu, O., Karri, R. Is split manufacturing secure? In Proceedings of the 2013 Design, Automation Test in Europe Conference Exhibition (DATE). Grenoble (France), 2013, p. 1259–1264. ISBN: 978-1-4673-5071-6. DOI: 10.7873/DATE.2013.261
[62] Villasenor, J., Tehranipoor, M. The Hidden Dangers of Chop-Shop Electronics. p. 1. [Online] Cited 2019-01-31. Available at: https://spectrum.ieee.org/semiconductors/processors/the-hidden-dangers-of-chopshop-electronics
[63] Watson, I. China: The Electronic Wastebasket of the World. p. 1. [Online] 2019-01-31. Available at: https://edition.cnn.com/2013/05/30/world/asia/china-electronic-waste-e-waste/index.html
[64] Zhang, X., Tehranipoor, M. Design of on-chip lightweight sensors for effective detection of recycled ICs. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2014, vol. 22, no. 5, p. 1016–1029. ISSN: 1557-9999. DOI: 10.1109/TVLSI.2013.2264063
[65] Zhang, X., Tuzzio, N., Tehranipoor, M. Identification of recovered ICs using fingerprints from a light-weight on-chip sensor. In Proceedings of the 49th Annual Design Automation Conference. New York (NY USA), 2012, p. 703–708. ISBN: 978-1-4503-1199-1. DOI: 10.1145/2228360.2228486
[66] Ambrose, J. Power Analysis Side Channel Attacks: The Processor Design-level Context. 1st ed. Saarbrücken (Germany): VDM Verlag Dr. Müller, 2010. ISBN: 978-3836485081.
[67] Hutter, M., Schmidt, J.-M. The temperature side-channel and heating fault attacks. In Proceedings of the International Conference on Smart Card Research and Advanced Applications. Berlin (Germany), 2013, p. 219–235. DOI: 10.1007/978-3-319-08302-5_15
[68] Kocher, P. C. Timing attacks on implementations of diffie-hellman, RSA, DSS, and other systems. In Proceedings of the 16th Annual International Cryptology Conference on Advances in Cryptology. London (UK), 1996, p. 104–113. ISBN: 3-540-61512-1. DOI: 10.1007/3-540-68697-5_9.

