International Journal of Security and Its Applications
Vol. 13, No. 3 (2019), pp.17-28
http://dx.doi.org/10.33832/ijsia.2019.13.3.03

IMPROVING THE PHYSICAL SECURITY OF MICROCHIPS

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. In scope of this paper, it means especially hindering of physical attacks on the chips.**

***Keywords*— Hybrid Integrated Circuits, Integrated Circuits, Reverse Engineering, Security, Three-Dimensional Integrated Circuits**

1. INTRODUCTION

This paper deals with the physical aspects of security of the chips, and provides realistic and also a near-futuristic view of the hardening physical attacks on microchips. We intentionally use the word "hardening" instead of "avoiding" or "disabling," because almost every countermeasure can be overcome. The target is to make the attack as disadvantageous for adversaries as possible.

Recently, we have seen many papers covering 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 physical examination of chips. Methods employing recent technologies like 3D integration, MEMS, integrated energy source, etc. will be introduced.

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, price always significantly influences the final design and many decisions made along the way to market. As we do not want to present a concrete example where it would be possible to assess adequacy of a particular countermeasure, let us propose and describe various possibilities for increasing security of microchips, regardless of its price.

A background for this paper is provided through a brief insight into a reverse-engineering scenario in Chapter 2. Chapters 3, 4, and 5 present the main contribution of

Received: June 3, 2019
Reviewed: August 14, 2019
Accepted: September 4, 2019

this work; proposals for security enhancements. A short conclusion and a follow-up promise are stated in Chapter 6.

2. REVERSE-ENGINEERING SCENARIO INTRODUCTION

For a long time, reverse engineering attacks had been neglected through deceptive feelings of the inherent security of microchips. With up-to-date knowledge, we know that adversaries can be very well equipped, as some of the attacks might be of national interest and thus with a strong financial backing and desire for results [7]. Moreover, there are not only cutting-edge chips available on the market, there are very many chips produced with older technological nodes, due to financial reasons or even overhauled outdated specimens secretly used in places where nobody expects them [8-17]. This also allows for many amateur-like adversaries (*e.g.*, up to Level 2, as described in [18], or up to Level MODL, according to [19]) to perform cheap partial reverse-engineering process with success.

Let us assume a scenario where an adversary has several pieces of a chip that is supposed to be partially or fully reverse engineered. During our research, we have proceeded in a similar scenario with high-tech international partner companies. We have learned along the way what countermeasures these partners recognized tough, or sometimes even nearly impossible, to break. Our proposals presented in the following chapters are based on this apprenticeship.

This scenario is about detaching the chip from a system, the decapsulation of the outer packaging, and further examination of the chip out of operation, that means delayering, acquiring images, and analyzing the acquired image data [20-22].

3. TECHNOLOGICAL NODE

The more advanced that the technological node used for the fabrication of a particular chip is, the more advanced equipment is needed for successful deprocessing. Hand in hand with advanced equipment, a deeper knowledge is required from the personnel operating the appliances. The later chips typically express progress in technology by providing more powerful features that are achieved by utilizing a higher number of smaller transistors, more metal layers, different materials used for conductive lines, and also insulation.

Our recommendation is to employ the latest possible matured technology for the production of security-aware ICs. With this measure, we can trim down the range of potential adversaries to those with access to the appropriate technologies. Needless to say, the price for the necessary equipment for deprocessing advanced nodes is at least in hundreds of thousands of US dollars, but it can easily get into the millions of US dollars.

This first recommendation is a very basic and rationally expectable one. However, in the following chapters, we will show that it is not always ideal to use the latest technologies everywhere. As we have learned during our study visit in TESCAN Laboratories, the idea that everything can be delayered just with the latest FIB machine is not correct. Each technological node is specific and thus requires a specific approach, e.g., for older nodes (above 100 nm) it is far from convenient to use the very recent FIB tools, which are focused on the smallest structures around 10 nm.

In other research articles [23-27], we have found statements that universities and similar institutions usually have some of the necessary equipment available. Therefore, it should be possible to rent these expensive tools at a relatively low hourly-rate basis. We tried this recommended approach by renting a very advanced FIB machine. Nevertheless, without a thorough training on how to use all of the required features of that particular machine, with its hundreds of settings, the adversary or researcher is hardly able to reach high-quality results. For achieving an output of a decent quality, it is necessary to rent the machine together with the erudite personnel. Furthermore, the latest chips are spatially large, and so removing all of the layers and acquiring images of the whole chip structure is not matter of days, mostly not even weeks, but months, unless we aim for a very specific area of interest only.

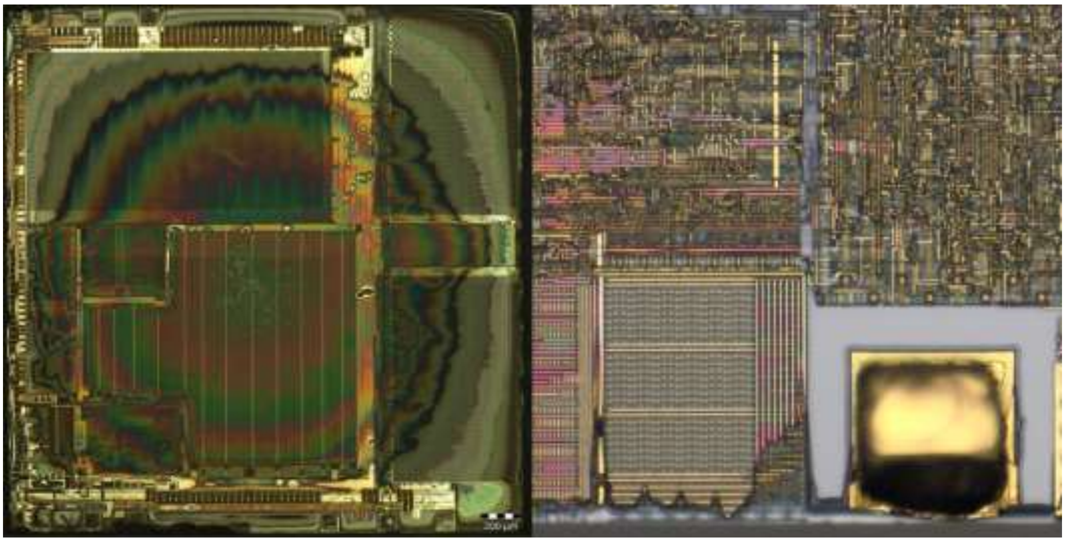

Fig. 1 Planarization problem after layer polishing (left). An underetching problem after several layers are removed (right).

4. COMPLEX INTEGRATION AND CAMOUFLAGING

2.5D and 3D integration is a substantial contribution to a possible security increase in IC fabrication. These chip composition techniques are emerging especially in relation with split fabrication processes that should assure the genuineness of IC production in offshore foundries [1-6]. Solving supply chain issues is not an aim of our work, and so we will refer readers to the above-mentioned papers for more information on that subject.

Our intention with the employment of 3D integration is to harden delayering and the consequent analysis of the inspected specimen. Delayering is already complicated with current state-of-the-art 2D integration – e.g. avoiding unintended cross planar grinding or underetching is tough enough with the recent nodes; see **Error! Reference source not found.**.

Removing all layers down to the silicon is usually feasible with chemical etching. Nevertheless, transistors express only a part of the IC blueprint, the same importance lies in the interconnection that add semantics to the whole circuit. Thus, obtaining images of transistors is, in a vast majority of cases, not sufficient. Therefore, adversaries have to concentrate on extracting all of the needed information – transistors and interconnections. And this exactly can be aggravated with use of 3D integration. Let us name several possible measures on how to make reverse engineering more challenging.

4.1. HETEROGENEOUS INTEGRATION

Heterogeneous integration of dies made with different technology will certainly make planarization issues much deeper. It would be ideal to utilize a combination of materials at the same plane levels that have very different grinding resistivity, so that to keep grinding absolutely planar across the whole heterogeneous plane will strictly require equipment that allows for perfect control over the grinding process. Wet or plasmatic etching will be even more difficult, especially when the layers will be wisely combined in order to ensure underetching or even direct damage to the adjacent layers. In **Error! Reference source not found.**, see the dielectric layer that is a combination of two different materials with a dissimilar resistance to chemicals – the green parts endure much longer before dissolving, which enables yellow dielectric trenches to initiate underetching. The passivation layer can be of different thickness across the die to make the decomposition harder from the very beginning.

4.2. UNREADABLE NON-VOLATILE MEMORY TYPES

Vastly used cheap masked ROM memories can literally be read out after the proper delayering of a device [7, 20, 28, 29]. To deflect an information breach, we recommend complete abandoning of using masked ROM memory types and types with similar features (readability of stored values, *e.g.*, [7, 30, 28]; impossible to erase/rewrite content). This step will help us to keep the stored information as optically unreadable and will also give us the opportunity to employ a defense scenario presented in Chapter 5.

Employment of memory encryption might be seemingly enough for protecting the plain content stored in memory cells. Unfortunately, frauds can find a way how to decipher the stored information [31, 32] – either finding the right key or reading out the data after it is decrypted by the device itself. Generally, one more step towards security would be not to disclose the memory content at all, regardless of the encryption used.

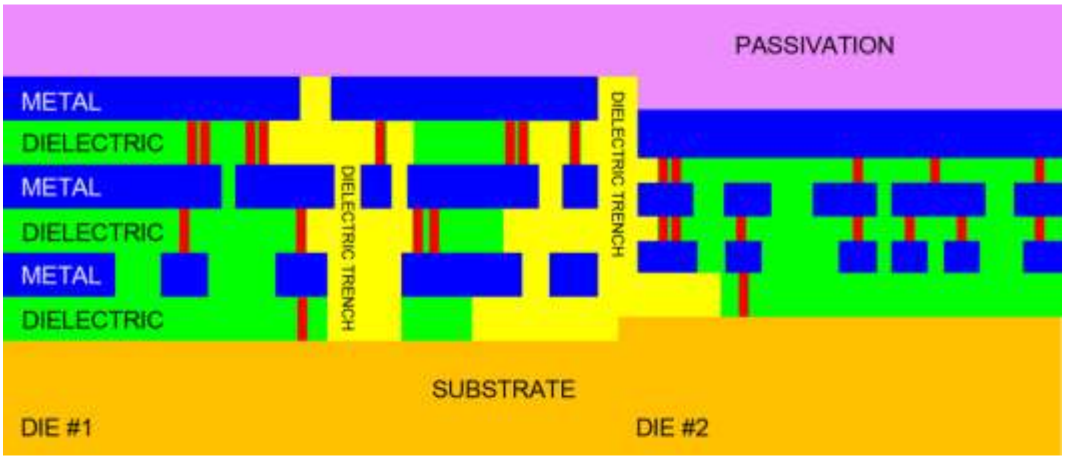

Fig. 2 Heterogeneous integration. We illustrate the heterogeneous integration of a chip. Various metal and dielectric layers thicknesses are placed at different levels. Dielectric trenches supporting underetching. Different thicknesses of the passivation layer

4.3. CELL CAMOUFLAGING

Cell camouflaging or circuit obfuscation are known techniques described in several research papers [33-39], [7, 6, 40]. 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 design time [2, 37, 36, 35, 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 really connected and which are just fake. Such advanced cross-sectioning is achievable with FIB milling or with X-rays [7, 41, 42, 43].

Let us introduce a 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. Camouflaged cells are spacious even with physical contacts, so there is not much of a difference. With wise design, we might get to the same spatial needs and potentially a similar camouflage effect. The fake contacts will then 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 due to its drawbacks [44-47]. Nevertheless, it would mean one more measure against physical reverse engineering.

4.4. 3D INTEGRATION WITH DUMMY DIES

There are many unused or recycled old dies available on the market (which are vastly used by fraudster foundries in fallaciously new integrations [8-17]). These can be wisely used for increasing the complexity of 3D integrations. Although this artificial complexity bloat will not prevent adversaries from performing decomposition and analysis, the intricacy of the integration can be risen. The time consumed for the determination of the dummy part might help to discourage adversaries.

We propose to use dies with diverse technological nodes for 3D integration. Each node requires a distinct approach for delayering and analysis. This approach will make reverse engineering more unfriendly. 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. 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 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 very 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.

5. ACTIVE TAMPER DETECTION

When adversaries perform reverse engineering, the chip is destined for physical destruction. It is detached from its package and from the power source. The latter does not have to be necessarily true in the very near future, due to discoveries and the successful development of micro batteries suitable for direct integration into ICs [48, 49, 50]. 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 alive solely the protective functionality, this might result in a decent time for active tamper detection endurance, even without external power source. Moreover, recent endeavors in the field of energy generation can lead us to mechanisms that are able to refill the integrated battery and hence allow for the exceptional endurance of active tamper detection. Let us name especially VEH (Vibration Energy Harvest) based on MEMS (Micro-Electro-Mechanical Systems) [51-53], Thermoelectric generation based on parasitic load of the device [54, 53] and Photovoltaic solar power generation [53, 55, 56] which can be at the same time sensing package decapsulation.

Integrated non-volatile memory is very often targeted because of its content. Therefore, our aim is to protect the chip from the tampering, intrusion, or analysis of its physical structure revealing the internal arrangement, especially the memory content. In this chapter, we propose the employment of active tamper detection in order to detect undesirable manipulation with a chip, and also measures protecting memory content from being disclosed in two different scenarios.

After tamper detection, the target will be to reliably remove memory contents (Chapter 5.1.) and/or to damage the circuit itself (Chapter 5.2.). With successful tamper detection and consequent memory erasure, the examined chip might be of a significantly decreased value.

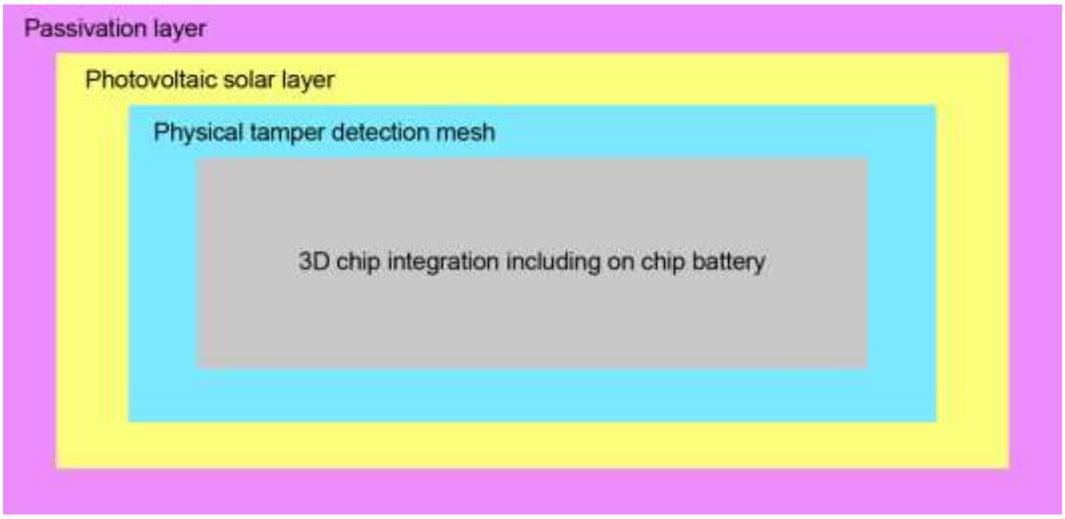
Passivation layer
Photovoltaic solar layer
Physical tamper detection mesh
3D chip integration including on chip battery

Fig. 3 Simplified composition of a chip with active tamper detection

5.1. ACTIVE TAMPER DETECTION WITH ACTIVE MEMORY PROTECTION

An active tamper detection shield should consist of several layers aimed at the possible ways of intrusion. Partial or complete decapsulation is one of the first steps when targeting chips invasive investigation. After opening a package, there should be natural light entering and interacting with the chip's surface. Therefore, the very first detector would be a light-sensing layer on the top of the chip. It should, ideally, be covering 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 for any modifications that could possibly lead to the restriction of active shield functionality, memory bus exposure, etc. This layer should be actively powered by a battery to regularly check the integrity of the mesh. Due to the fact that reverse engineering is not a fast process, the check can be set to be run after a certain period. This interval has to be designed with respect to the power demands of the whole active shield circuit and capacity of the integrated battery. It can be expected that the parameters of the batteries will significantly improve over the next years. Then, this active shield use case will be supported even more.

In **Error! Reference source not found.**, we provide a simplified view of a chip structure with respect to the proposed active protection. As there are many attacks led from “backside” of a chip, we recommend using 3D integration with a back-to-back connection to have a 3D chip with only the frontal part facing all the edges of the packaging. Passivation, photovoltaic detection/generation, and physical tamper detection layers are used all around the chip's structure. A battery is expected to be integrated 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 be a battery-powered action.

In cases when the attackers are somehow able to disable the photovoltaic layer, their next step will be layer-by-layer removal. Once the physical layer tamper detection mesh is touched, the same memory-erase signal shall be triggered.

Memory modules should have low energy demand in order to enable this protection scenario with battery-powered memory erasure. 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 or in the case of malfunction.

In various scenarios, we can more or less rely on the battery re-charging mechanisms (TEG, VEH, Photovoltaic *etc.*), and thus prolong 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, it is automatically re-charging the battery because of the integrated VEH system. If the document is used, it is re-charged as well, with power obtained from the document reader and because of the heat produced by the chip (thermoelectric generation). The worst scenario is when the document is stored in a drawer and never used in 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. When we go 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 whether the passport needs to be recharged in order to keep it valid for as long as possible.

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 [57-59]. 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 the biometric characteristics of the holder and will be able to detect counterfeit attempts.

5.2. FPGA EMPLOYMENT WITH ACTIVE BITSTREAM PROTECTION

Protecting a chip against 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 known attacks against such implementations [7, 60, 61], focusing on the reconstruction of the FPGA configuration bitstream, thus essentially gaining a netlist of the circuit.

To avoid these attacks, we have to protect the main memory that holds the configuration information and buses from micro probing, FIB editing, *etc*. Our proposal is to physically protect the chip in the same way as described in the previous chapter with an active-tamper detection shield. Whenever there is an alarm triggered by the active shield, 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 and no notion as to its configuration.

6. CONCLUSION

Possible enhancements for improving the security of microchips were presented. This paper was primarily aiming for hindering invasive attacks, especially with regards to reverse engineering. As it can be concluded, there are available ways of further securing microchips. It can also be expected that all of the 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 all newly implemented protection mechanisms.

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, 2016, vol. 2., no. 2, 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), 8 2013, p. 495–510. ISBN 978-1-931971-03-4.

[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), 5 2016, p. 69–74. ISBN: 978-1-4503-4274-2. 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), 5 2017, p. 321–326. ISBN: 978-1-4503-4972-7. 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), 5 2016, p. 347–352. ISBN: 978-1-4503-4274-2. 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), 11 2016, p. 30:1–30:8. ISBN: 978-1-4503-4466-1. DOI: 10.1145/2966986.2967014

[7] 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

[8] 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

[9] 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

[10] 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

[11] 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

[12] 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

[13] 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

[14] 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

[15] 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

[16] 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

[17] 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

[18] National Institute of Standards and Technology. Security Requirements for Cryptographic Modules (FIPS 140-2). 69 pages. [Online] Cited 2019-01-31. Available at: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf

[19] Abraham, D. G., Dolan, G. M., Double, G. P., Stevens, J. V. Transaction security system. IBM Systems Journal - Special issue on cryptology, 1991, vol. 30, no. 2, p. 206 –229. DOI: 10.1147/sj.302.0206

[20] 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.

[21] Malčík, D., Drahanský, M. Microscopic Analysis of Chips. In Proceedings of the Future Generation Information Technology Conference. Jeju Island (KR), 2011, p. 113–122. ISBN: 978-3-642-27188-5. DOI: 10.1007/978-3-642-27189-2_12

[22] Malčík, D., Drahanský, M. Microscopic Analysis of Chips. International Journal of Security and Its Applications, 2016, vol. 2016, no. 11, p. 47–66. DOI: 10.14257/ijsia.2016.10.11.05

[23] Nohl, K., Evans, D., Starbug, S., Plötz, H. Reverse-engineering a Cryptographic RFID Tag. In Proceedings of the 17th USENIX Security Symposium. Berkeley (CA, USA), 2008, p. 185–193.

[24] Skorobogatov, S., Woods, C. Breakthrough Silicon Scanning Discovers Backdoor in Military Chip. In Proceedings of the 14th International Conference on Cryptographic Hardware and Embedded Systems (CHES 2012). Berlin (DE), 2012, p. 23–40. DOI: 10.1007/978-3-642-33027-8_2

[25] Oswald, D., Paar, C. Breaking Mifare DESFire MF3ICD40: Power Analysis and Templates in the Real World. In Proceedings of the 13th International Conference on Cryptographic Hardware and Embedded Systems (CHES 2011). Berlin (DE), 2011, p. 207–222. DOI: 10.1007/978-3-642-23951-9_14

[26] Schobert, M. All Chips Reversed. 20 pages. [Online] Cited 2019-01-31. Available at: https://ds.ccc.de/pdfs/ds094.pdf

[27] 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

[28] 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

[29] Kryszczuk, K., Richiardi, J. Encyclopedia of Cryptography and Security. 2nd ed. Springer US, 2011. ISBN 978-1-4419-5906-5

[30] 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

[31] 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

[32] 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

[33] 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

[34] 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

[35] 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

[36] 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

[37] 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

[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] 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. 09–114. ISBN: 978-1-4799-8606-4. DOI: 10.1109/DFT.2015.7315145

[41] 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.

[42] 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

[43] 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

[44] 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

[45] 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

[46] 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

[47] 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

[48] 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, p. 359–362. DOI: 10.1109/POWERENG.2009.4915179

[49] 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, 2013, vol. 25, no. 33, p. 4539–4543. DOI: 10.1002/adma.201301036

[50] 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, 2015, vol. 112, no. 21, p. 6573–6578. DOI: 10.1073/pnas.1423889112

[51] 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, p. 1–4. DOI: 10.1109/RSM.2015.7354963

[52] 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), 6 2013, p. 1336–1339. ISBN: 978-1-4673-5983-2. DOI: 10.1109/Transducers.2013.6627024

[53] 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

[54] Fahad, H., Hasan, M., Li, G., Hussain, M. Thermoelectricity from wasted heat of integrated circuits. Applied Nanoscience, 2013, vol 3., no. 3, p. 175–178. ISSN 2190-5517. DOI: 10.1007/s13204-012-0128-2

[55] 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.

[56] 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, p. 1–5. DOI: 10.1109/HNICEM.2015.7393174

[57] 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

[58] 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

[59] 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

[60] 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

[61] 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.