Nele Mentens
Associate Editor in Chief

Hardware Security in the Era of Emerging Device and System Technologies

In this editor's column, I would like to advocate for putting more research effort in the security of electronic systems that are based on emerging hardware technologies. The reason for existence of these emerging technologies is that they are more efficient than traditional semiconductor technologies with respect to one or more nonfunctional properties, such as the energy consumption, the peak power dissipation, the computational delay, the cost and/or the size of the chip. The requirements of a system determine which of these properties are the most important for that system and whether it is necessary to step away from traditional technologies. For example, a pacemaker chip should consume as little energy as possible because the battery should last as long as possible, while a disposable medical sensor should be as cheap as possible because it cannot be reused. When traditional semiconductor technologies cannot fulfill these requirements, emerging technologies can offer a solution.

To prepare for new systems and applications, it is important to know which opportunities and limitations both traditional and emerging technologies (will) bring in the present and the future. For this purpose, the International Roadmap for Devices and Systems (IRDS) makes predictions with a 15-year horizon to provide guidance to companies and research institutions.[1] The IRDS Executive Summary of 2022, which was recently announced to be still relevant for 2023, mentions different International Focus Teams (IFTs).[2] Traditional technologies are mainly described by the ITF on "More Moore,"[3] which elaborates on the challenges and solutions for the continuation of Moore's law.[4] Moore's law was empirically established in 1965, stating that the number of transistors in an electronic chip would double every two years with a minimal cost increase. Therefore, the "More Moore" IFT mainly focuses on the down-scaling of semiconductor features. Emerging technologies, on the other hand, follow alternative paths that do not necessarily strive toward the continuation of Moore's law. It is mainly in the "More than Moore" IFT[4] and the "Beyond CMOS" IFT[5] that these alternative technologies are projected. Examples are novel memory technologies (e.g., magnetic memories and resistive memories) and novel logic devices (based on, e.g., carbon nanotubes or spin waves). Many of these emerging technologies are already being deployed in commercial products, but research on the hardware security properties of these products is still in its infancy.

©SHUTTERSTOCK.COM/JIJOMATHAIDESIGNERS

So why can't we just use our existing knowledge on traditional technologies to reason about emerging technologies? To understand this, we need to go the fundamental building blocks of hardware security: hardware roots of trust. An interesting overview of the most important hardware roots of trust[6] is given by Synopsys, one of the largest electronic design automation companies in

Digital Object Identifier 10.1109/MSEC.2024.3379768
Date of current version: 10 May 2024

the world and provider of hardware intellectual property cores for security. Among others, hardware cryptographic accelerators, true random number generators (TRNGs) and secure storage are mentioned. We also add physically unclonable functions (PUFs) to this list as an alternative for secure key storage. When we look at these components, we observe that their desired hardware security properties are highly dependent on their physical behavior, which is determined by the underlying technology. In this editor's column, I would like to shed a light on two promising emerging technologies and their suitability for generating hardware roots of trust, which will be needed if commercial products based on these technologies become widespread and need to be secured.

Their resistive nature is entirely different from the semiconductor-based mechanisms on which traditional volatile or nonvolatile memories rely.

In the category of emerging memory devices, resistive memories are nonvolatile memories that consume less power and work faster than traditional Flash memories but are more expensive to fabricate. Especially in high-performance neuromorphic computing, resistive memories have a large potential for improving the computing system. Their resistive nature is entirely different from the semiconductor-based mechanisms on which traditional volatile or nonvolatile memories rely. Therefore, security properties derived for these traditional memories do not necessarily hold for resistive memories. An example of a commercially available resistive memory by Crossbar Inc. already mentions secure storage properties like protection against read-out, unclonability, and the ability to build PUFs.[7] And there are also examples of academic research that present novel ways of designing PUFs based on resistive memories.[8] Nevertheless, I believe that a thorough analysis of the security properties of resistive memories based on open source models of these memories would be desirable before they become widespread.

Another promising technology I would like to highlight is flexible electronics because I expect it to increasingly be the subject of hardware security research in the coming years. Flexible electronic chips are ultrathin and very light. They are built on mechanically flexible substrates such as plastics, metal foil, flexible glass, and paper. The big advantage of flexible electronics is the low cost of the chips (thanks to the low-cost production process) and the short development cycle. Although flexible electronics are not suitable for high-performance systems, they are perfect for Internet of Things devices used in, e.g., wearables, smart packaging, logistics, and product authentication. So what about building hardware roots of trust into flexible electronic chips? For TRNGs and PUFs, flexible electronic chips that are based on inkjet printing can make use of the random dispersion of the ink as a source of randomness or intrinsic variation.[9,10] This is different from traditional silicon chips that use entropy sources like timing jitter and the metastability of electronic

Digital Object Identifier 10.1109/MSEC.2024.3393315

circuits. Nevertheless, randomness and entropy tests have shown that the proposed TRNGs and PUFs offer a promising alternative to their silicon counterparts. Another type of root of trust are cryptographic hardware circuits. In flexible electronics, these have only been demonstrated on metal-oxide thin-film transistors on plastic substrates because that seems to be the only type of flexible technology that can handle the complexity of a cryptographic algorithm. The big challenge here is indeed the reliability of the chip when the circuit size increases. In these chips, secure key storage is difficult to achieve for multiple reasons. First of all, there is no viable solution for nonvolatile memory yet, which means the only way to store a key is to use a one-time programmable (OTP) memory using a laser or ink. In addition, since these chips are much larger than their silicon counterparts, and since they are typically not packaged, it is very easy for an attacker to read out the secret key. Both secure cryptographic circuits and key storage solutions have been proposed in Mentens et al.[11] and Bleier et al.[12] The first multiproject wafer program for flexible electronics has been offered by the company Pragmatic since July 2023.[13] This allows researchers to tape-out low-cost flexible chips with a short fabrication time. I expect that Pragmatic's multiproject wafer program will give academic research on the security of flexible electronics the necessary boost in the near future.

In conclusion, emerging device and system technologies offer interesting opportunities for novel products with unique properties in terms of energy consumption, peak power dissipation, computational delay, cost and/or size of the chip. But more research into the security of hardware roots of trust that rely on these technologies is needed in order to enable their deployment at large scale for a large range of applications. I believe this is an excellent opportunity for researchers in security, hardware design, and emerging technologies to collaborate and make a difference. ■

References

1. "International roadmap for devices and systems," IEEE, Piscataway, NJ, USA, 2024. [Online]. Available: https://irds.ieee.org/
2. "IRDS 2022: Executive summary," IEEE, Piscataway, NJ, USA, 2022. [Online]. Available: https://irds.ieee.org/editions/2022/executive-summary
3. "IRDS 2022: More than Moore," IEEE, Piscataway, NJ, USA, 2022. [Online]. Available: https://irds.ieee.org/editions/2022/irds%E2%84%A2-2022-more-than-moore
4. G. E. Moore, "Cramming more components onto integrated circuits," *Electronics*, vol. 38, no. 8, pp. 1–4, Apr. 19, 1965. [Online]. Available: http://cva.stanford.edu/classes/cs99s/papers/moore-crammingmorecomponents.pdf
5. "IRDS 2023: Beyond CMOS and emerging materials integration," IEEE, Piscataway, NJ, USA, 2023. [Online]. Available: https://irds.ieee.org/editions/2023/20-roadmap-2023-edition/126-irds%E2%84%A2-2023-beyond-cmos-and-emerging-materials-integration
6. A. Elias. "Understanding hardware roots of trust." Synopsys. Accessed: Mar. 8, 2024. [Online]. Available: https://www.synopsys.com/designware-ip/technical-bulletin/understanding-hardware-roots-of-trust-2017q4.html
7. "ReRAM proves resistant to invasive attacks," CrossBar, Santa Clara, CA, USA, 2022. [Online]. Available: https://www.crossbar-inc.com/news/press-releases/2022-04-05-reram-proves-resistant-to-invasive-attacks/
8. K. Chuang, "Highly reliable physically unclonable functions: Design, characterization and security analysis," Ph.D. thesis, KU Leuven, Leuven, Belgium, 2020.
9. A. T. Erozan et al., "Inkjet-printed EGFET-based physical unclonable function—Design, evaluation, and fabrication," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 26, no. 12, pp. 2935–2946, Dec. 2018, doi: 10.1109/TVLSI.2018.2866188.
10. A. T. Erozan, G. Y. Wang, R. Bishnoi, J. Aghassi-Hagmann, and M. B. Tahoori, "A compact low-voltage true random number generator based on inkjet printing technology," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 28, no. 6, pp. 1485–1495, Jun. 2020, doi: 10.1109/TVLSI.2020.2975876.
11. N. Mentens et al., "Security on plastics: Fake or real?" *IACR Trans. Cryptogr. Hardware Embedded Syst.*, vol. 2019, no. 4, pp. 1–16, 2019.
12. N. Bleier et al., "Exploiting short application lifetimes for low cost hardware encryption in flexible electronics," in *Proc. Des., Autom. Test Europe Conf. Exhib. (DATE)*, 2023, pp. 1–6, doi: 10.23919/DATE56975.2023.10137258.
13. "Flexible integrated circuits." Pragmatic. Accessed: Mar. 8, 2024. [Online]. Available: https://europractice-ic.com/technologies/flexible-electronics/