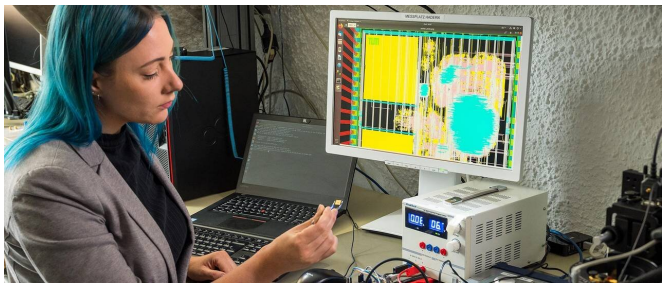
Chip with secure encryption will help in fight against hackers

4 August 2021



A team at the Chair of Security in Information Technology has developed a chip with particularly secure encryption technology. Johanna Baehr heads a second team at the chair that has hidden four hardware Trojans on this chip - malicious functions that are integrated directly into the circuits. Credit: Astrid Eckert / TUM

A team at the Technical University of Munich (TUM) has designed and commissioned the production of a computer chip that implements post-quantum cryptography very efficiently. Such chips could provide protection against future hacker attacks using quantum computers. The researchers also incorporated hardware Trojans in the chip in order to study methods for detecting this type of "malware from the chip factory."

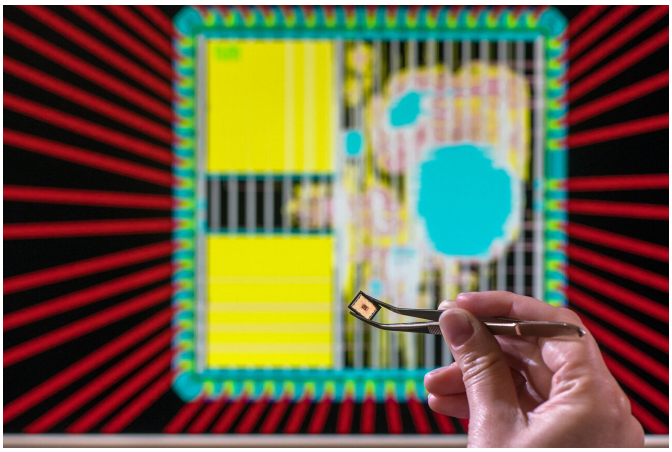
Hacker attacks on industrial operations are no longer science fiction—far from it. Attackers can steal information on production processes or shut down entire factories. To prevent this, communication between the chips in the individual components is encrypted. Before long, however, many encryption algorithms will become ineffective. The established processes that can fight off attacks launched with today's computer technologies will be defenseless against quantum computers. This is especially critical for equipment with a long lifespan such as industrial facilities.

For this reason, security experts around the world are working to develop technical standards for "post-quantum cryptography." One of the challenges is posed by the enormous processing power needed for these encryption methods. A team working with Georg Sigl, Professor of Security in Information Technology at TUM, has now designed and commissioned a highly efficient chip for post-quantum cryptography.

Speed and flexibility through a combination of hardware and software

Professor Sigl and his team took an approach based on hardware/software co-design, in which specialized components and the control software complement one another. "Ours is the first chip for post-quantum cryptography to be based entirely on a hardware/software co-design approach," says Prof. Sigl.

"As a result, it is around 10 times as fast when encrypting with Kyber—one of the most promising candidates for post-quantum cryptography—as compared to chips based entirely on software solutions. It also uses around eight times less energy and is almost as flexible."



The chip relies on a tight combination of hardware and software to apply post-quantum encryption performant

and energy-efficiently. Credit: Astrid Eckert / TUM

Based on an open source standard

The chip is an application-specific integrated circuit (ASIC). This kind of specialized microcontroller is often manufactured in large numbers according to specifications of companies. The TUM team modified an open source chip design based on the open source RISC-V standard. It is used by increasing numbers of chip makers and could replace proprietary approaches of big companies in many areas. The chip's post-quantum cryptography capabilities are facilitated by a modification of the processor core and special instructions that speed up the necessary arithmetic operations.

The design also incorporates a purpose-designed hardware accelerator. It not only supports lattice-based post-quantum cryptography algorithms such as Kyber, but could also work with the SIKE algorithm, which requires much more computing power. According to the team, the chip developed at TUM could implement SIKE 21 times faster than chips using only software-based encryption. SIKE is seen as the most promising alternative if the time comes when lattice-based approaches are no longer secure. Precautions of this kind make sense in applications where chips will be used for extended periods.

Hardware Trojans evade post-quantum cryptography

Another potential threat, alongside the rise in conventional attacks, is posed by hardware Trojans. Computer chips are generally produced according to companies' specifications and made in specialized factories. If attackers succeed in planting trojan circuitry in the chip design before or during the manufacturing stage, this could have disastrous consequences. As in the case of external hacker attacks, entire factories could be shut down or production secrets stolen. What's more: Trojans built into the hardware can evade post-quantum cryptography.

"We still know very little about how hardware trojans are used by real attackers," explains Georg Sigl. "To develop protective measures, we need to think like an attacker and try to develop and conceal our own Trojans. In our post-quantum chip we have therefore developed and installed four hardware Trojans, each of which works in an entirely different way."

Chip to be tested and then dismantled

Over the coming months, Prof. Sigl and his team will intensively test the chip's cryptography capabilities and functionality and the detectability of the hardware trojans. The chip will then be destroyed—for research purposes. In a complex process, the circuit pathways will be shaved off incrementally while photographing each successive layer. The goal is to try out new machine learning methods developed at Prof. Sigl's chair for reconstructing the precise functions of chips even when no documentation is available. "These reconstructions can help to detect chip components that perform functions unrelated to the chip's actual tasks and which may have been smuggled into the design," says Georg Sigl. "Processes like ours could become the standard for taking random samples in large orders of chips. Combined with effective post-quantum cryptography, this could help us to make hardware more secure—in industrial facilities as well as in cars."

More information: Alexander Hepp et al, Tapeout of a RISC-V crypto chip with hardware trojans, *Proceedings of the 18th ACM International Conference on Computing Frontiers* (2021). DOI: 10.1145/3457388.3458869

Debapriya Basu Roy et al, Efficient hardware/software co-design for post-quantum crypto algorithm SIKE on ARM and RISC-V based microcontrollers, *Proceedings of the 39th International Conference on Computer-Aided Design* (2020). DOI: 10.1145/3400302.3415728

Fritzmann, T. et al, J. RISQ-V: Tightly Coupled RISC-V Accelerators for Post-Quantum Cryptography. *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2020). DOI: 10.13154/tches.v2020.i4.239-280

Provided by Technical University Munich

APA citation: Chip with secure encryption will help in fight against hackers (2021, August 4) retrieved 2 July 2022 from https://techxplore.com/news/2021-08-chip-encryption-hackers.html