RUHR-UNIVERSITÄT BOCHUM

RUB

RUBIN

SCIENCEMAGAZINE

SPECIAL ISSUE

IT SECURITY

Three tough nuts for quantum computers to crack

This is how artificially generated images reveal their true colours

Start-up: Ready for the new generation of mobile communications

#33 Volume

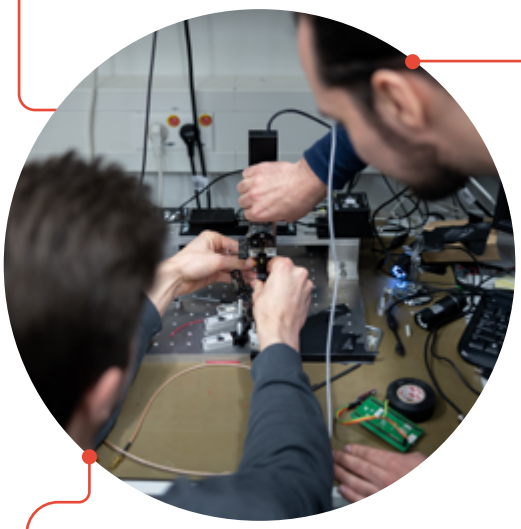
Special Issue 2023

Side-Channel Attacks

WHEN THE **CHIP** NEEDS A COOLING BREAK

Many encryption algorithms are mathematically proven to be one hundred per cent secure. Nevertheless, they sometimes fail to protect confidential data. This is because encryption doesn't happen merely in theory.

An electronic chip is a bit like a person who has to solve a complicated problem under extreme time pressure. Many people know what it feels like when the brain is working at full throttle and the head starts to overheat. You may also get a craving for sweets, because you feel you need more energy. Deep in thought, you might even start muttering under your breath. An electronic chip that is tasked with



Nicolai Müller (on the left), David Knichel (on the right) and their colleagues develop tools that help manufacturers make electronic circuits more secure.

encrypting data works in a similar way. While it's doing its job, it may get warm, its power consumption may increase, and it may emit acoustic signals. And all this can pose a security risk. Namely, if the changes to the physical parameters reveal something about the data that the chip is in the process of encrypting.

It has repeatedly been shown that this can happen. In such cases, researchers use the term side-channel attacks, because it is not the encryption algorithm itself that is cracked, but additional information is used to read out confidential data. ▸

The research team: Nicolai Müller, Pascal Sasdrich, David Knichel and Amir Moradi (from left)

The time alone that it takes to encrypt certain data can tell us something about the content of the data itself. "Such attacks don't require a lot of effort at all," says Dr. Pascal Sasdrich from the Horst Görtz Institute for IT Security at Ruhr University Bochum. "It's not something that can only be done by organisations like the NSA. Theoretically, anyone can carry out side-channel attacks from their garage. The necessary equipment only costs around 200 euros." Targets may include transponder keys, card readers and smart home technologies, to name but a few.

Pascal Sasdrich is conducting research at the Faculty of Computer Science in the Emmy Noether Junior Research Group "Computer-Aided Verification of Physical Security Properties" (CAVE). Together with colleagues from Professor Amir Moradi's Implementation Security group, he is focusing on how to find out whether an electronic component is protected against side-channel attacks – and how to build a secure electronic circuit. "When implementing cryptographic processes, manufacturers often want chips to be as small as possible, as efficient as possible or as fast as possible," lists Pascal Sasdrich. Security is usually not their top priority. In addition, a single careless mistake in the implementation of the encryption technology is enough to open a gateway to attackers. The Bochum-based team is therefore developing tools to help manufacturers implement encryption technology.

To this end, it must first be possible to determine whether an existing electronic circuit is secure or not. The group has developed the so-called SILVER method for this purpose. The acronym stands for Statistical Independence and Leakage Verification. This name already reveals what the key to success is: statistical independence. SILVER checks whether the observable physical parameters such as power consumption and temperature during encryption are statistically independent of the data that is being encrypted. In case of statistical independence, no inferences can be drawn from the physical parameters as to the content of the data.

"Traditionally, other criteria used to be applied for the verification of secure circuits, rather than statistical independence," says Pascal Sasdrich. "The methods were based on hypotheses or estimates and sometimes produced false negative results." In other words, methods were classified as insecure, even though they were in fact not insecure at all. Such errors don't occur with the SILVER method.

"SILVER is one hundred per cent secure, because it is based on a highly comprehensive analysis," stresses Amir Moradi, adding, however, that "it doesn't yet work for larger circuits, because the workload would skyrocket." For large circuits, the Bochum-based researchers are currently using simulation-based methods, which prove to be efficient even for complex systems. "However, they aren't one hundred per cent secure," admits Moradi. His team is now looking for feasible options to verify the security of larger circuits with a high degree of reliability.

Couldn't we simply break down these more complex systems into several components and check them one by one? "You can look at individual parts and prove that they are secure. But if you then put them together, that doesn't mean that the entire circuit is secure, too," explains Pascal Sasdrich. This is because the interfaces between the components can constitute a gateway for attackers.

David Knichel and Nicolai Müller, likewise members of the Implementation Security research group in Bochum, are working on solutions to this problem. The IT experts are developing modules for electronic circuits that can be securely combined with each other in such a way that the assembled circuit, too, is guaranteed to be resistant to side-channel attacks. These individual modules are referred to as gadgets. "You don't need many different gadgets to build a circuit," explains David Knichel.

The gadgets map, for example, certain logical operations, such as the multiplication of two bits – a frequently needed

i BITS

A bit is the smallest unit of information used by conventional computers. It has the values "0" and "1". Complex information is made up of a large number of bits, which are linked together by logical operations during computing processes.

The researchers develop tools that support manufacturers to improve the security of electronic cirtuits.

operation. However, if a separate gadget were used for every logical operation that has to run in the circuit, the whole structure would take up an extremely large amount of space. The reason is that many bits have to be multiplied together in the encryption process. David Knichel and his colleagues are therefore working on expanding the range of functions of individual gadgets, for example so that one gadget can multiply several bits simultaneously. This would make the circuit faster and smaller.

The gadgets developed by the Bochum-based team aren't components that physically exist, however, but are available as code instead. "We use a common hardware description language," says Knichel. This means that he and his colleagues provide a construction manual for manufacturers, so to speak.

Still, protecting electronic circuits from side-channel attacks manually is a tedious task. "We have therefore developed a tool called AGEMA, which can convert an unprotected circuit into a verifiably secure one at the push of a button," points out Nicolai Müller. AGEMA stands for Automated Generation of Masked Hardware. The tool checks which logical operations exist in a circuit and replaces insecure components with the secure gadgets. "We can also take specific preferences into account, i.e. optimise the circuit for speed and size, for example," adds Müller.

The tools developed so far represent the first steps in basic research, rather than solutions that can be used on an industrial scale. After all, a lot of research is still being invested in the automated protection of electronic circuits against side-channel attacks. The IT experts in Bochum will also dedicate much of their efforts to developing optimised solutions – only taking an occasional cooling break.

text: jwe, photos: ms

> THEORETICALLY, ANYONE CAN CARRY OUT SIDE-CHANNEL ATTACKS FROM THEIR GARAGE.
>
> Pascal Sasdrich

The gadgets developed by the team from Bochum are based on a modular design and provide a basis for secure electronic circuits.

EDITOR'S DEADLINE

The rabbits in the CASA Universe are startled: the seemingly well-secured access to Rabbit Mark's carrot stash has been hacked and all winter supplies have been stolen. The brave bunny Betty then starts looking for support at the nearby CASA Hub C – a mysterious place that is supposed to hold solutions for digital security. Thus begins the adventure of Betty the bunny, the protagonist of the first science comic from the Cluster of Excellence CASA. Along with Betty, the readers explore the Research Hub and learn about the research priorities and challenges that the scientists in the Research Hub C "Secure Systems" deal with on a daily basis. Find out how to read this and more CASA comics at no cost at:

↗ *casa.rub.de/en/outreach/science-comics*

Answers
DEEP FAKE-QUIZ
The following faces are real:
1a, 2a, 3b, 4a, 5b, 6a

LEGAL NOTICE

PUBLISHER: Cluster of Excellence CASA at the Horst Görtz Institute for IT Security at Ruhr University Bochum in collaboration with the Corporate Communications Department at Ruhr University Bochum (Hubert Hundt, v.i.S.d.P.)

EDITORIAL ADDRESS: Corporate Communications Department, Editorial Office Rubin, Ruhr-Universität Bochum, 44780 Bochum, Germany, phone: +49 234 32 25228, rubin@rub.de, news.rub.de/rubin

EDITORIAL BOARD: Dr. Julia Weiler (jwe, editor-in-chief); Meike Drießen (md); Lisa Bischoff (lb)

PHOTOGRAPHER: Michael Schwettmann (ms), Dammstr. 6, 44892 Bochum, Tel.: +49 177 3443543, info@michaelschwettmann.de, www.michaelschwettmann.de

COVER: Sashkin – stock.adobe.com

PHOTOGRAPHS FOR TABLE OF CONTENTS: Michael Schwettmann

GRAPHIC DESIGN, ILLUSTRATION, LAYOUT:
Agentur für Markenkommunikation, Ruhr-Universität Bochum,
www.einrichtungen.rub.de/de/agentur-fuer-markenkommunikation

PRINTED BY: LD Medienhaus GmbH & Co. KG, Van-Delden-Str. 6-8, 48683 Ahaus, Germany, Tel.: +49 231 90592000, info@ld-medienhaus.de, www.ld-medienhaus.de

EDITION: 800

DISTRIBUTION: Rubin is published twice a year in German language; the regular issues are available from the Corporate Communications Department at Ruhr-Universität Bochum. The magazine can be subscribed to free of charge at news.rub.de/rubin/abo. The subscription can be cancelled by email to rubin@rub.de. The special issue 2021 is available from the Horst Görtz Institute for IT Security. In case of interest, please contact hgi-presse@rub.de.

ISSN: 0942-6639

Reprinting with reference to source and submission of proof copies