RUHR-UNIVERSITÄT BOCHUM

RUB

RUBIN

SCIENCEMAGAZINE

SPECIAL ISSUE

IT SECURITY

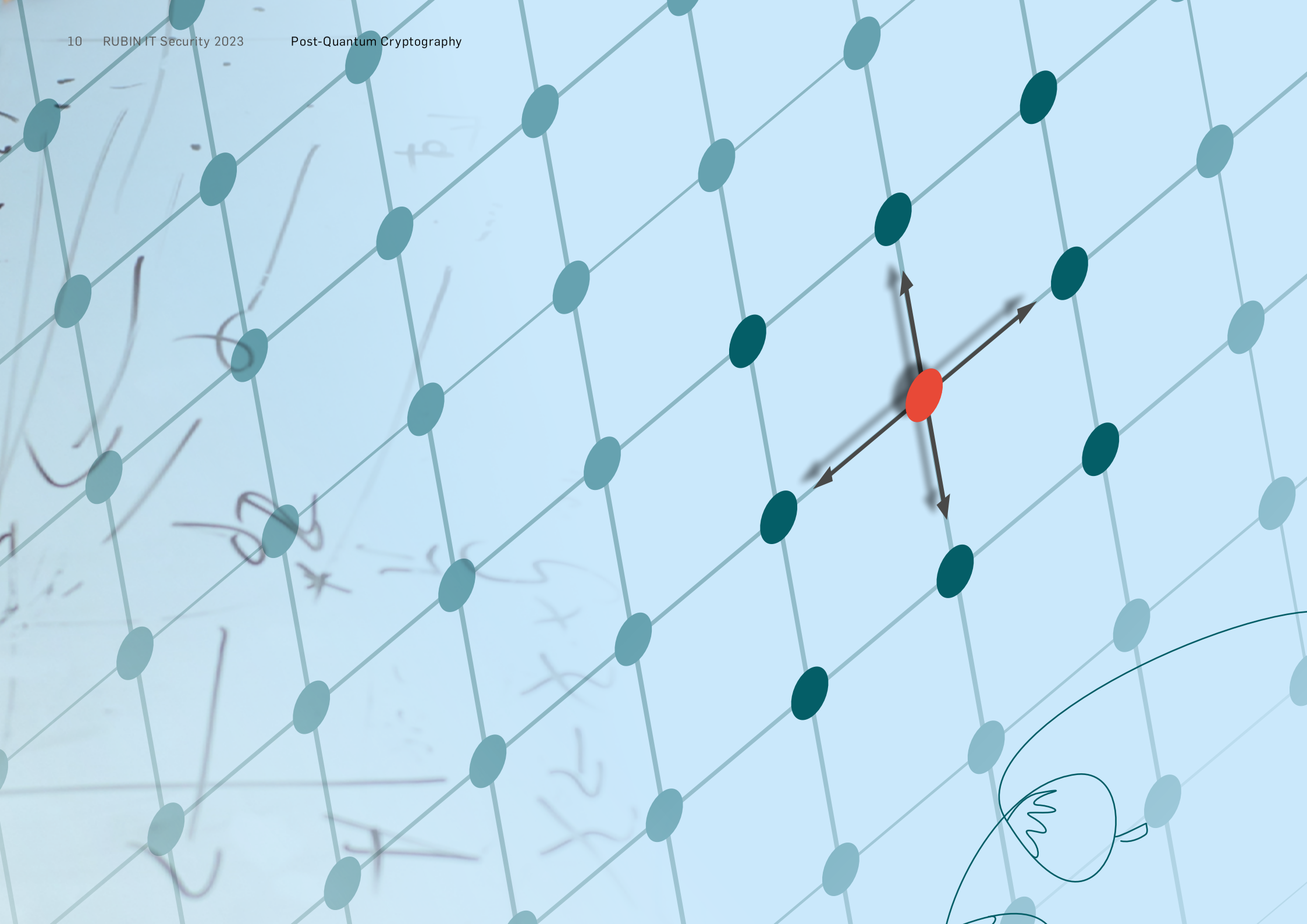
Three tough nuts for quantum computers to crack

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



THREE TOUGH NUTS FOR **QUANTUM COMPUTERS** TO CRACK

Algorithms made in Bochum are becoming the global standard for secure encryption in the age of quantum computing. They've arrived just in time.

i QUANTUM COMPUTERS

Conventional computers encode information in the form of bits that can assume the values 0 and 1. Quantum computers, on the other hand, operate with quantum bits. They can have the states 0 and 1 at the same time. This allows them to solve certain mathematical tasks much more efficiently than conventional computers. Experts refer to this computing advantage as quantum superiority. For currently existing computers that use quantum technology, however, this superiority has not yet been proven beyond doubt. The devices are not yet able to crack the encryption methods currently in use.

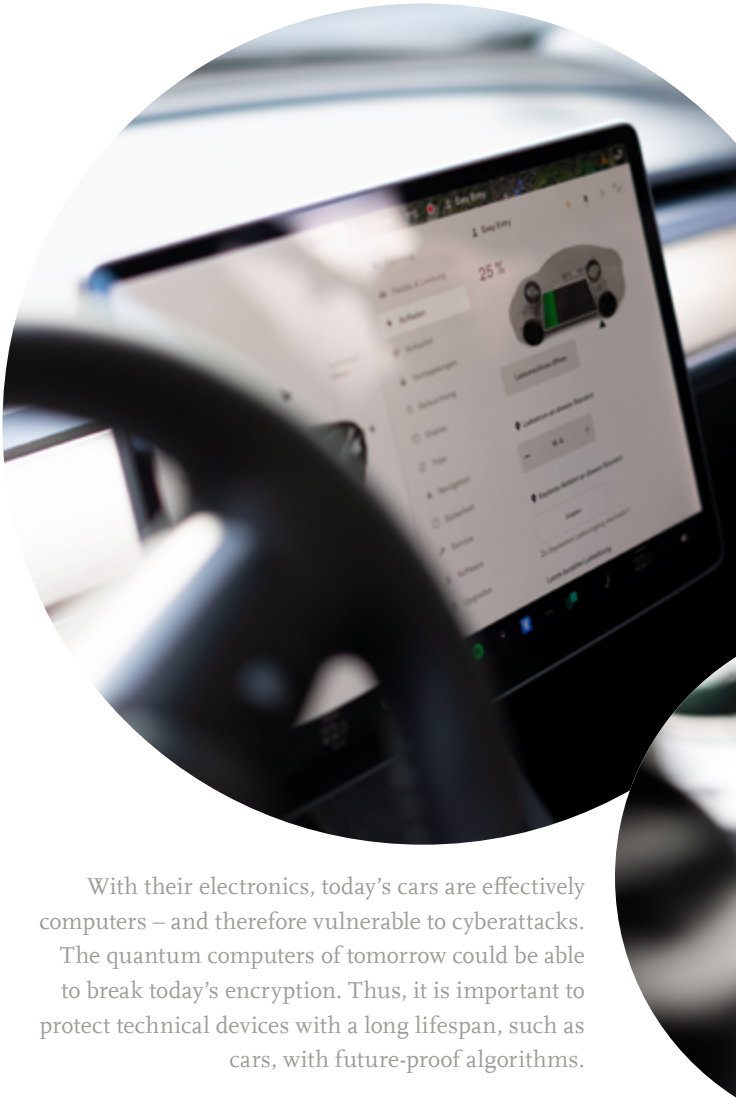
The lattice problem: which blue point is closest to the zero point marked red in the lattice? In a 500-dimensional lattice, this problem can no longer be efficiently solved.

It's still early in the morning and a bitterly cold day. You're about to leave for work. Fortunately, the car can be preheated remotely from your smartphone. Frozen door locks are also a thing of the past. The car can be opened effortlessly with the fingerprint scanner. Then, a brief voice command turns on the radio. The engine starts and the head-up display lights up. Off you go on a journey that feels safe even when you're a little tired, thanks to the lane keeping assist system.

A modern car is more or less a computer. And like with all other computers, attackers can potentially gain control over the on-board systems. Therefore, the electronics in smart cars must be protected against cyberattacks. This includes not only the attacks that are possible today, but also those of tomorrow – because a car has a long lifespan. Vehicles that roll off the assembly line today may be around long enough to experience the age of quantum computers.

"Quantum computers will be able to crack some of the current encryption technologies without any problems," points out Professor Eike Kiltz. He heads the Chair for Cryptography and is one of the spokespersons for the Cluster of Excellence CASA – Cyber Security in the Age of Large-Scale Adversaries at the Horst Görtz Institute for IT Security. To ensure that today's technology will still be secure in the future, Eike Kiltz and his colleagues have developed new methods to protect data from attacks with quantum computers. CASA members Professor Tanja Lange, Professor Peter Schwabe and Professor Daniel Bernstein were instrumental in this work.

The team won a highly prestigious competition organised by the US National Institute of Standards and Technology (NIST) in 2016. NIST competitions have already taken place on a range of topics, with the aim of finding the best possible solutions to the most pressing problems in IT security. Research groups worldwide can submit their proposed solutions; the best approaches are then filtered out in a step-by-step process lasting several years. In the 2016 competition on secure ▸



With their electronics, today's cars are effectively computers – and therefore vulnerable to cyberattacks. The quantum computers of tomorrow could be able to break today's encryption. Thus, it is important to protect technical devices with a long lifespan, such as cars, with future-proof algorithms.

algorithms against quantum computer attacks, 82 proposals were submitted. Four of them are now to be standardised, as NIST 2022 announced. Of these four winning methods, three come from the CASA Cluster of Excellence.

In the past, methods that have won the NIST competition have caught on at a worldwide scale. It can therefore be assumed that the quantum-safe CASA algorithms will be used for encryption and digital signatures all over the world in the future. The NSA, the largest foreign intelligence service in the United States, is already recommending that the US government use the Crystals-Kyber and Crystals-Dilithium methods, in the development of which Eike Kiltz and Peter Schwabe were involved.

Crystals-Kyber is used for encryption – for example, of data sent by e-mail or of credit card information submitted for online shopping. Crystals-Dilithium is designed to secure authentication processes, i.e. it's used when a person or an object has to prove their identity. For example, when an operating system is being updated, the software must prove that it is an official product of the manufacturer and doesn't come from a hacker.

With Crystals-Kyber and Crystals-Dilithium – fans of Star Wars and Star Trek will recognise that the names are an homage to the films – Eike Kiltz' research has been directly translated into application. For him, an unusual experience. This is because the computer scientist usually operates at the very edge of theory. Now, the CASA team's algorithms will be implemented all over the world. "We bear a great responsibility," says Kiltz, aware of this fact and at the same time pleased. "Finally, I can explain what my research is good for."

At the core of his research are highly abstract questions, so-called hard mathematical problems. "These are problems that many brilliant minds have grappled with over the past decades without ever finding a solution," he explains. One of them is the lattice problem that constitutes the backbone of Crystals-Kyber and Crystals-Dilithium. To visualise the problem, imagine a two-dimensional lattice that has a zero point somewhere. Everywhere where lines cross, there are so-called intersection points. The question is: which intersection point is closest to the zero point? This is easy to answer for a two-dimensional lattice. The more dimensions you add, the more difficult it becomes. Above about 500 dimensions, there is no efficient solution to the problem.

The CASA algorithms are based on the lattice problem in a slightly simplified form: the search is not for the nearest intersection point, but for any intersection point that lies within a certain radius around the zero point. If, for example, a software update wants to prove to the operating system that it comes from an official software manufacturer, it must prove that it knows a secret – namely one of these intersection points near the zero point.

Since the lattice problem is mathematically different from the method on which standard encryption is based, quantum computers won't be able to solve it any more than conventional computers. "Quantum computers only have an advantage when it comes to highly specific tasks," says Eike Kiltz. This is always the case, for example, when you can express a task as a period-finding task. A period is the distance between the repetition of values in a function. If you imagine a sine curve, the period comprises a mountain and a valley of the curve. If a powerful quantum computer did exist, it could determine the period of any function very quickly.

This would be a problem for the commonly used encryption method RSA, which is based on the problem of prime factorisation. This mathematical exercise involves finding out, for a number with several hundred digits, which two prime numbers you'd have to multiply to get this number. This question can't be efficiently solved with conventional computers. Quantum computers, however, could do this easily, because prime factorisation can be described as a period-finding task. The same doesn't apply to the lattice problem. It is therefore safe from quantum computer attacks.

The Bochum-based researchers have now optimised their Crystals-Kyber and Crystals-Dilithium methods to such an extent that they can keep up with today's standard RSA method in terms of efficiency. The new methods are even two to three times faster than RSA, but they require ciphers that are 20

> FINALLY, I CAN EXPLAIN WHAT MY RESEARCH IS GOOD FOR.
>
> Eike Kiltz

Together with colleagues, Eike Kiltz has developed new algorithms that are effective against quantum computer attacks. With these algorithms, the researchers won a multi-year competition.

to 30 times longer. “This means that you need a little more storage space, but you can use a smaller processor,” points out Eike Kiltz.

Still, it will take quite some time before the processes gain traction worldwide. Crystals-Kyber and Crystals-Dilithium are expected to be standardised in two years. According to Eike Kiltz’ estimates, implementation will then take another five to ten years. “The development process will be completed just in time,” says the Bochum-based researcher. He assumes that in 10 to 20 years quantum computers might exist that will be able to break conventional encryption methods. This still sounds a long way off. “But you have to consider that intelligence services, for example, store encrypted data that may still be relevant in the future – and in the future they may be able to decrypt it with the help of quantum computers,” illustrates Kiltz. Plus, there are the cars mentioned above, which will hit the roads in the coming years equipped with all kinds of electronics; they may still be driving around when quantum computers have long since become a reality.

text: jwe, photos: ms

THIRD AWARD-WINNING METHOD

It wasn't only Crystals-Kyber and Crystals-Dilithium that secured the CASA team its success in the NIST competition for quantum-safe methods, but also the Sphincs+ algorithm. Sphincs+ can be used to create secure digital signatures. It is based on hash functions. Hash functions create an output from any input, such as a file, that looks completely different from the input. If a minor change were made to the input file, the resulting output would look completely different. This is how the hash functions disguise the structure of the data. The method was for the most part developed by CASA member Peter Schwabe, a researcher working at the Max Planck Institute for Security and Privacy in Bochum.

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