RUHR-UNIVERSITÄT BOCHUM

RUB

RUBIN

WISSENSCHAFTSMAGAZIN

SONDERAUSGABE

IT-SICHERHEIT

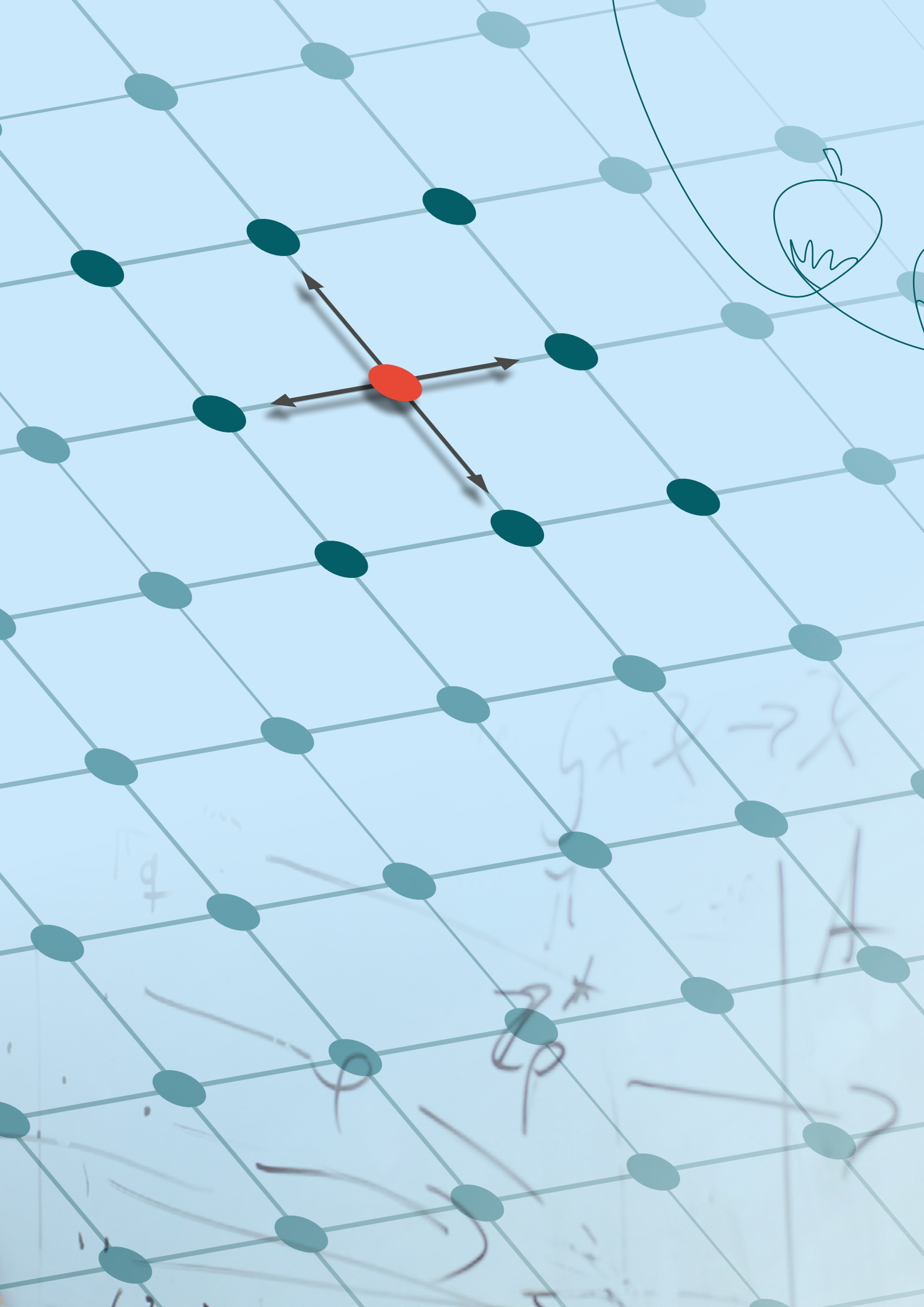
Wie sich künstlich erzeugte Bilder verraten

Drei harte Nüsse für Quantencomputer

Start-up: Fit für die neue Mobilfunkgeneration

#33 Jahrgang

Sonderausgabe 2023



DREI HARTE NÜSSE FÜR **QUANTENCOMPUTER**

Bochumer Algorithmen werden zum weltweiten Standard für die sichere Verschlüsselung im Zeitalter des Quantencomputings. Sie kommen gerade noch rechtzeitig.

i QUANTENCOMPUTER

Herkömmliche Computer codieren Informationen in Form von Bits, die die Werte 0 und 1 annehmen können. Quantencomputer hingegen arbeiten mit Quantenbits. Sie können gleichzeitig die Zustände 0 und 1 besitzen. Das erlaubt es ihnen, gewisse mathematische Aufgaben wesentlich effizienter zu lösen als herkömmliche Rechner. Fachleute sprechen bei diesem Rechenvorteil von der Quantenüberlegenheit. Für derzeit existierende Computer, die Quantentechnik einsetzen, ist diese Überlegenheit jedoch noch nicht zweifelsfrei bewiesen worden. Die Geräte können die derzeit gängigen Verschlüsselungsverfahren noch nicht knacken.

Das Gitterproblem als Basis neuer Algorithmen: Welcher der blauen Punkte liegt am nächsten an dem rot markierten Nullpunkt des Gitters? Bei einem 500-dimensionalen Gitter ist dieses Problem nicht mehr effizient zu lösen.

Es ist noch früh am Morgen und bitterkalt. Gleich geht es los zur Arbeit. Zum Glück lässt sich das Auto über die Handysteuerung vorheizen. Auch vereiste Türschlösser gehören der Vergangenheit an. Öffnen kann man den Wagen mühelos über den Fingerabdruckscanner. Dann genügt ein kurzer Sprachbefehl, schon geht das Radio an. Der Motor startet, das Head-up-Display leuchtet auf. Los geht die Fahrt, die sich auch im etwas müden Zustand dank Spurhaltesystem sicher anfühlt.

Ein modernes Auto ist eigentlich eine Art Computer. Und wie bei allen anderen Computern können Angreifer sich potenziell Kontrolle über die Bordsysteme verschaffen. Daher sollte die Elektronik in smarten Autos vor Cyberattacken geschützt sein. Und zwar nicht nur vor den Angriffen, die jetzt schon möglich sind, sondern auch vor denen von morgen. Denn ein Auto hat eine lange Lebensdauer. Fahrzeuge, die heute vom Band rollen, werden eventuell lange genug halten, um das Zeitalter der Quantencomputer mitzuerleben.

„Quantencomputer werden einige der gängigen Verschlüsselungstechniken problemlos brechen können“, weiß Prof. Dr. Eike Kiltz. Er leitet den Lehrstuhl für Kryptografie und ist einer der Sprecher des Exzellenzclusters CASA (Cyber Security in the Age of Large-Scale Adversaries) am Horst-Görtz-Insitut für IT-Sicherheit. Damit die Technik von heute auch in Zukunft sicher ist, hat Kiltz zusammen mit Kolleginnen und Kollegen neue Verfahren entwickelt, die Daten vor Angriffen mit Quantencomputern schützen. Maßgeblich beteiligt waren die CASA-Mitglieder Prof. Dr. Tanja Lange, Prof. Dr. Peter Schwabe und Prof. Dr. Daniel Bernstein.

Das Team setzte sich in einem hochkompetitiven Wettbewerb durch, den das US-amerikanische National Institute of Standards and Technology, kurz NIST, 2016 ausgerufen hatte. NIST-Wettbewerbe gab es bereits zu verschiedenen Themen, mit dem Ziel, bestmögliche Lösungen für drängende Probleme der IT-Sicherheit zu finden. Forschungsgruppen weltweit können ihre Lösungsvorschläge einreichen; in einem mehrere Jahre dauernden, schrittweisen Verfahren werden dann die besten Ansätze herausgefiltert. Im Rahmen des 2016er Wettbewerbs zu sicheren Algorithmen gegen Quantencom- ▸

puter-Angriffe wurden 82 Vorschläge eingereicht. Vier davon sollen nun standardisiert werden, wie das NIST 2022 verkündete. Von diesen vier Gewinnerverfahren stammen drei aus dem Exzellenzcluster CASA.

Verfahren, die beim NIST-Wettbewerb gewonnen haben, haben sich in der Vergangenheit stets weltweit durchgesetzt. Es ist also davon auszugehen, dass die quantencomputersicheren CASA-Algorithmen künftig auf dem ganzen Globus zum Verschlüsseln und digitalen Signieren genutzt werden. Die NSA, der größte Auslandsgeheimdienst der Vereinigten Staaten, empfiehlt der US-Regierung bereits jetzt die Verfahren Crystals-Kyber und Crystals-Dilithium zu verwenden, an denen Eike Kiltz und Peter Schwabe beteiligt waren.

Crystals-Kyber dient der Verschlüsselung – etwa von Daten, die per E-Mail verschickt werden oder von Kreditkarteninformationen, die fürs Onlineshopping hinterlegt werden. Crystals-Dilithium ist zur Absicherung von Authentifizierungsprozessen gedacht, kommt also dann zum Einsatz, wenn ein Mensch oder ein Objekt seine Identität beweisen muss. So muss beispielsweise bei einem Update des Betriebssystems die Software beweisen, dass sie ein offizielles Produkt des Herstellers ist und nicht von einem Hacker stammt.

Mit Crystals-Kyber und Crystals-Dilithium – Fans von Star Wars und Star Trek werden erkennen, dass die Namen eine Hommage an die Filme sind – ist Eike Kiltz' Forschung direkt in die Anwendung gemündet. Eine ungewöhnliche Erfahrung für ihn. Denn üblicherweise spielt sich die Arbeit des Informatikers am äußersten Rand der Theorie ab. Nun werden die Algorithmen des CASA-Teams in der ganzen Welt zum Einsatz kommen. „Wir tragen eine große Verantwortung", ist Kiltz sich bewusst und freut sich zugleich: „Endlich kann ich mal erklären, wofür meine Forschung gut ist."

Dabei geht es im Kern seiner Arbeit um sehr abstrakte Fragen, sogenannte schwere mathematische Probleme. „Das sind Probleme, mit denen sich viele schlaue Köpfe in den vergangenen Jahrzehnten beschäftigt haben, ohne eine Lösung zu finden", erklärt er. Eines davon ist das Gitterproblem, das Crystals-Kyber und Crystals-Dilithium zugrunde liegt.

Um sich das Problem zu verdeutlichen, stellt man sich zunächst ein zweidimensionales Gitter vor, das an einer Stelle einen Nullpunkt besitzt. Überall dort, wo sich Linien kreuzen, befinden sich sogenannte Kreuzungspunkte. Die Frage lautet: Welcher Kreuzungspunkt liegt am nächsten beim Nullpunkt? Sie ist für ein zweidimensionales Gitter einfach zu beantworten. Je mehr Dimensionen man hinzunimmt, desto schwieriger wird es. Ab etwa 500 Dimensionen gibt es keine effiziente Lösung mehr für das Problem.

Die CASA-Algorithmen beruhen auf dem Gitterproblem in einer leicht vereinfachten Form: Gesucht wird nicht der nächstgelegene Kreuzungspunkt, sondern ein beliebiger Kreuzungspunkt, der sich in einem bestimmten Radius um den Nullpunkt befindet. Wenn ein Softwareupdate dem Betriebssystem beispielsweise beweisen möchte, dass es von einem offiziellen Softwarehersteller stammt, muss es nachweisen, dass es ein Geheimnis kennt – nämlich einen dieser Kreuzungspunkte in der Nähe des Nullpunkts.

Moderne Autos mit ihrer ganzen Elektronik sind Computer – und somit anfällig für Cyberattacken. Die Quantencomputer von morgen könnten in der Lage sein, heute gängige Verschlüsselungstechniken auszuhebeln. Daher ist es entscheidend, langlebige Technik wie Autos durch Algorithmen zu sichern, die den Attacken von morgen gewachsen sind.

Weil das Gitterproblem mathematisch andersartig ist als die Technik, auf der gängige Verschlüsselungen beruhen, werden Quantencomputer es genauso wenig lösen können wie herkömmliche Rechner. „Quantencomputer haben nur bei sehr bestimmten Aufgaben einen Vorteil", erklärt Eike Kiltz. Das ist zum Beispiel immer dann der Fall, wenn man eine Aufgabe als Periodenfinde-Aufgabe ausdrücken kann. Als Periode bezeichnet man den Abstand zwischen dem Auftreten gleicher Werte in einer Funktion. Stellt man sich eine Sinuskurve vor, so umfasst die Periode einen Berg und ein Tal der Kurve. Gäbe es einen leistungsfähigen Quantencomputer, dann könnte er die Periode einer beliebigen Funktion sehr schnell ermitteln.

Das wäre ein Problem für das gängige Verschlüsselungsverfahren namens RSA, das auf dem Problem der Primfaktorzerlegung basiert. Aufgabe bei dieser mathematischen Übung ist es, für eine Zahl mit mehreren hundert Stellen herauszufinden, welche zwei Primzahlen man miteinander multiplizieren müsste, um die Zahl zu erhalten. Mit herkömmlichen Rechnern ist diese Frage nicht effizient lösbar. Quantencomputer könnten das aber mühelos, weil man die Primfaktorzerlegung als Periodenfinde-Aufgabe beschreiben kann. Mit dem Gitterproblem geht das nicht. Daher ist es vor Quantencomputerangriffen sicher.

Ihre Verfahren Crystals-Kyber und Crystals-Dilithium haben die Bochumer Forschenden mittlerweile so weit opti-

„DIE ENTWICKLUNG KOMMT GERADE NOCH RECHTZEITIG.“

Eike Kiltz

Gemeinsam mit Kolleginnen und Kollegen hat Eike Kiltz neue quantencomputersichere Algorithmen entwickelt und damit einen mehrjährigen Wettbewerb gewonnen.

miert, dass sie in punkto Effizienz mit dem heute üblichen RSA-Verfahren mithalten können. Die neuen Verfahren sind sogar zwei- bis dreimal schneller als RSA, dafür brauchen sie 20- bis 30-mal so lange Chiffren. „Man braucht also etwas mehr Speicherplatz, dafür kann man einen kleineren Prozessor verwenden“, verdeutlicht Eike Kiltz.

Bis die Verfahren sich weltweit durchgesetzt haben, wird es aber noch ein wenig dauern. Zwei Jahre wird es brauchen, bis Crystals-Kyber und Crystals-Dilithium standardisiert sind. Die Implementierung, so schätzt Eike Kiltz, wird dann noch einmal fünf bis zehn Jahre erfordern. „Die Entwicklung kommt also gerade noch rechtzeitig“, sagt der Bochumer Forscher. Er geht davon aus, dass es in 10 bis 20 Jahren Quantencomputer geben könnte, die gängige Verschlüsselungsverfahren brechen können. Das klingt noch lange hin. „Aber man muss bedenken, dass zum Beispiel Geheimdienste verschlüsselte Daten speichern, die auch in Zukunft noch interessant sein können – und in Zukunft können sie sie vielleicht mithilfe von Quantencomputern entschlüsseln“, gibt Kiltz ein Beispiel. Und auch die eingangs erwähnten Autos, die mit allerhand Elektronik bestückt in den kommenden Jahren auf die Straßen entlassen werden, werden vielleicht immer noch herumfahren, wenn Quantencomputer längst Wirklichkeit geworden sind.

Text: jwe, Fotos: ms

i DRITTES GEWINNERVERFAHREN

Nicht nur mit Crystals-Kyber und Crystals-Dilithium, sondern auch mit dem Algorithmus Sphincs+ hat sich das CASA-Team im NIST-Wettbwerb um quantensichere Verfahren durchgesetzt. Sphincs+ kann zum sicheren Erstellen von digitalen Signaturen genutzt werden. Es basiert auf Hash-Funktionen. Hash-Funktionen erzeugen aus einem beliebigen Input, etwa einer Datei, einen völlig anders aussehenden Output. Würde man eine Kleinigkeit an der Eingangsdatei verändern, würde die resultierende Ausgabe trotzdem ganz anders aussehen. So verschleiern die Hash-Funktionen die Struktur der Daten. Das Verfahren wurde maßgeblich von CASA-Mitglied Peter Schwabe entwickelt, der am Bochumer Max-Planck-Institut für Sicherheit und Privatsphäre forscht.

REDAKTIONSSCHLUSS

Die Hasen im CASA Universe sind aufgeschreckt: Der scheinbar gut gesicherte Zugang zum Karottenvorrat von Hase Mark wurde gehackt und alle Wintervorräte geraubt. Die mutige Häsin Betty macht sich daraufhin auf die Suche nach Unterstützung im nahegelegenen CASA Hub C – einem geheimnisvollen Ort, der Lösungen für digitale Sicherheit bereithalten soll. So beginnt das Abenteuer von Häsin Betty, der Protagonistin des ersten Wissenschaftscomics des Exzellenzclusters CASA. Gemeinsam mit Betty lernen die Leserinnen und Leser bei ihrem Streifzug durch den Research Hub die Forschungsschwerpunkte und Herausforderungen kennen, mit denen sich die Wissenschaftlerinnen und Wissenschaftler im Forschungsbereich Hub C „Sichere Systeme" tagtäglich beschäftigen. Wie Sie alle Comics der Reihe kostenlos lesen können, erfahren Sie unter:

↗ *casa.rub.de/outreach/wissenschaftscomics*

Auflösung
DEEPFAKE-QUIZ
Folgende Gesichter sind echt:
1a, 2a, 3b, 4a, 5b, 6a

IMPRESSUM

HERAUSGEBER: Exzellenzcluster CASA und Horst-Görtz-Institut für IT-Sicherheit der Ruhr-Universität Bochum in Verbindung mit dem Dezernat Hochschulkommunikation der Ruhr-Universität Bochum (Hubert Hundt, v.i.S.d.P.)

REDAKTIONSANSCHRIFT: Dezernat Hochschulkommunikation, Redaktion Rubin, Ruhr-Universität Bochum, 44780 Bochum, Tel.: 0234/32-25228, rubin@rub.de, news.rub.de/rubin

REDAKTION: Dr. Julia Weiler (jwe, Redaktionsleitung); Meike Drießen (md); Lisa Bischoff (lb)

FOTOGRAFIE: Michael Schwettmann (ms), Dammstr. 6, 44892 Bochum, Tel.: 0177/3443543, info@michaelschwettmann.de, www.michaelschwettmann.de

COVER: Sashkin – stock.adobe.com

BILDNACHWEISE INHALTSVERZEICHNIS: Michael Schwettmann

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

DRUCK: LD Medienhaus GmbH & Co. KG, Van-Delden-Str. 6-8, 48683 Ahaus, Tel.: 0231/90592000, info@ld-medienhaus.de, www.ld-medienhaus.de

AUFLAGE: 4.700

BEZUG: Die reguläre Ausgabe von Rubin erscheint zweimal jährlich und ist erhältlich im Dezernat Hochschulkommunikation der Ruhr-Universität Bochum. Das Heft kann kostenlos abonniert werden unter news.rub.de/rubin. Das Abonnement kann per E-Mail an rubin@rub.de gekündigt werden. Die Sonderausgabe 2023 ist erhältlich beim Horst-Görtz-Institut für IT-Sicherheit. Interessierte können sich per E-Mail an hgi-presse@rub.de melden.

ISSN: 0942-6639