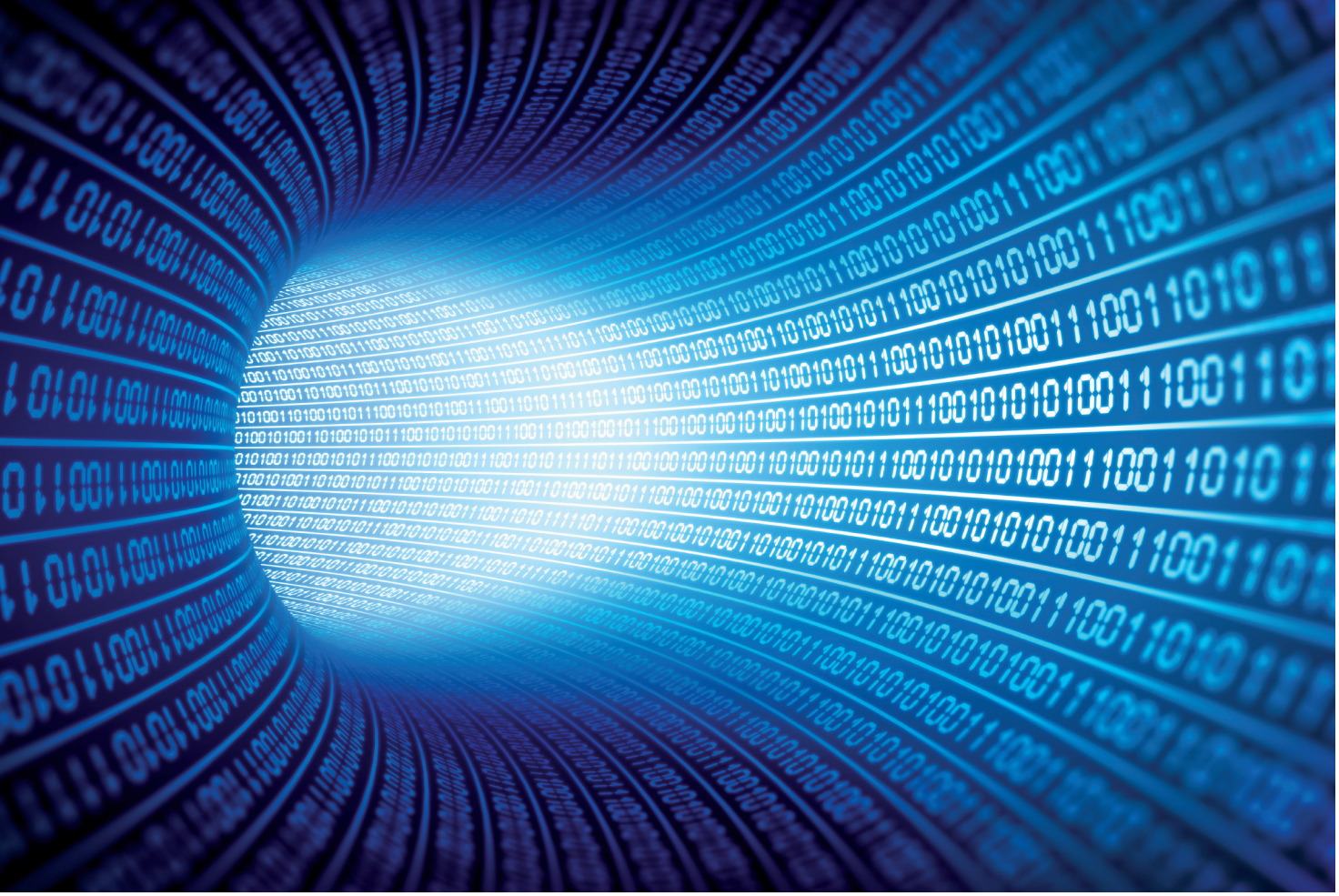


Nachricht in der Schatulle

Ihr Einsatz garantiert zwar nicht absolute Sicherheit der Kommunikation, die Hürden für Schnüffelprogramme liegen aber sehr hoch: die Rede ist von der Kryptographie. Die Oldenburger Mathematiker Florian Heß und Andreas Stein über ein Forschungsgebiet, das nicht erst seit den Enthüllungen des Whistleblowers Edward Snowden hoch im Kurs steht.

Florian Heß, Andreas Stein

Schreiben Sie E-Mails? Speichern Sie Ihre Daten in der Cloud? Laden Sie Softwareupdates oder Apps aus dem Internet? Angesichts der öffentlichen Diskussion um Geheimdienste und Spionageprogramme haben Sie sich sicher gefragt, wie sich das Ausspähen von Daten oder das Installieren von zu Schnüffelzwecken verfälschter Software verhindern oder zumindest erschweren lässt. Lösungen für diese und viele andere sicherheitsbezogene Probleme der digitalen Welt liefert die Kryptographie.

Verschlüsselung ist die offensichtliche Aufgabe der Kryptographie. Sie soll eine Nachricht, zum Beispiel eine Datei, vor ihrer Übertragung unkenntlich machen, so dass lediglich der Empfänger sie rekonstruieren und lesen kann. Weniger offensichtlich, aber ebenso wichtig sind Datenintegrität und –authentizität. Für sie sorgt häufig eine digitale Signatur. Sie soll sicherstellen, dass die Nachricht auf dem Weg vom Sender zum Empfänger nicht verfälscht wird und dass die Nachricht tatsächlich vom Sender und nicht aus einer sinisteren Quelle stammt. Die Anwendungsgebiete der Kryptographie sind vielfältig und erstrecken sich über elektronische Wahlen bis hin zu elektronischem Geld. Bei E-Commerce oder E-Government ist sie unentbehrlich für die Informationssicherheit von Unternehmen und Staaten.

Aussagen des NSA-Whistleblowers Edward Snowdon, dessen Enthüllungen Einblicke in das Ausmaß und die Praktiken von Geheimdiensten gaben, bestätigen den Nutzen der Kryptographie. Wie aktuelle Presseberichte zeigen, zielen die Schnüffelangriffe primär auf die Endpunkte kryptographischer Kommunikation und auf den Einbau von Hintertüren. Solche Attacken sind mit hohen Hürden und Risiken für die Angreifer verbunden. Der Einsatz von Kryptographie bedeutet daher in der Praxis zwar nicht absolute, aber doch allgemeine Kommunikationssicherheit in hohem Maße.

Die mathematischen und algorithmischen Grundlagen der Kryptographie zählen zu den Forschungsschwerpunkten des Instituts für Mathematik der Universität Oldenburg. Hier spielen

Message in the Strongbox

Cryptography may not guarantee absolute security for communications but it creates very high hurdles for spying programmes. Oldenburg mathematicians Florian Heß and Andreas Stein discuss a field of research that has that is in high demand - and not just since the revelations of whistleblower Edward Snowden.

Do you write emails? Do you save data to the Cloud? Do you download software updates or apps from the Internet? In view of the public debate about the secret services and their spying programmes you will no doubt have wondered how data espionage or the installation of fake software that is actually used for spying purposes can be prevented or at least impeded. Cryptography provides solutions to this and many other security-related problems in the digital world.

Cryptography's most obvious task is encryption. It can be used to render a message, a piece of data for example, indecipherable before sending, so that it can be reconstructed and read only by its intended recipient. Less obvious but equally important is data integrity and authenticity. This is often taken care of by a digital signature. Its aim is to ensure that the message is not corrupted on its way from sender to receiver and that it actually stems from the sender and not from some sinister source. Cyptography's field of application is broad and ranges from the use of electronic voting to electronic money. In e-commerce and e-government it is indispensable for the data security of businesses and states.

The statements made by NSA whistleblower Edward Snowden, whose revelations shed light on the scale of the operations and practices of the secret services, have confirmed cryptography's importance. As current media reportage shows, the spying attacks are aimed primarily at the endpoints of cryptographic communication and the insertion of backdoors. These attacks pose major hurdles and risks for the attacker. Thus in practice, the use of cryptography may not guarantee absolute communication security, but generally speaking the level of security provided is high.

Cryptography's mathematical and algorithmic foundations are one of the key areas of research at the University of Oldenburg's Institute of Mathematics. Methods from number theory, arithmetic geometry and computer algebra all play an important role here.

Curve-Based Cryptography

Modern cryptographic algorithms require computational problems that are "easy" to set but "difficult" to solve. One example: among the nonnegative integers a prime number is a number larger than one which is divisible only by one and itself with no remainder, such as 2, 3, 5, 7, and so on. Using a computer it is possible to calculate two random prime numbers with 300 decimal digits as well as their product in a matter of seconds. The reverse calculation of the prime numbers starting from the product, on the other hand, would take several years at the current level of research. Computational problems for prime factor decomposition are therefore "easy" to set and "difficult" to solve. This allows encryptions and digital signatures to be quickly generated and categorized as secure for extended periods of time.

In Oldenburg the research focus on cryptography's mathematical and algorithmic foundations deals primarily with curve-based cryptography. As is the case with prime factor decomposition, computational problems from the field of number theory are also applied here, albeit for elliptic curves, and more generally for algebraic curves over finite fields. The emphasis here is on efficiency and security, potential applications, as well as related questions from number theory and arithmetic geometry. The relationship between efficiency and security in cryptographic algorithms is much more favourable using elliptic curves than in the example involving prime factor decomposition. And there are also new applications such as pairing-based cryptography. All these aspects make elliptic curves particularly interesting for cryptography. In Germany they are used, among other things, in passports and identity cards. Elliptic curves are much more structured, complex number theoretic objects than prime numbers. This makes them particularly interesting for mathematicians, but virtually unintelligible for non-mathematicians.

Key constituents of the underlying mathematical theory were developed in the 1930s and 40s by the German number theorists Helmut Hasse and Max Deuring as part of their research in pure mathematics, without a view to practical applications. Seventy years later their findings represent a central component of applied cryptography. Beyond cryptography, elliptic curves play an important role in number theory and arithmetic geometry. This can be seen, for instance, in Pierre de Fermat's Last Theorem and its proof, or in the Birch and Swinnerton-Dyer conjecture – one of the greatest unsolved mathematical problems and one of the so-called Millennium Prize Problems. Cryptography is therefore also an interesting field of activity for number theorists with an interest in algorithms outside the "ivory tower of pure mathematics".

Cryptography has a long history that stretches back to ancient times. It was not until the 20th century, however, that it gained scientific status. The increasingly technological nature of communication and the invention of computers, driven in part by the demands of cryptography itself, gave a considerable boost to the development by Alan Turing and Claude Shannon of information theory as the mathematical-computational basis of cryptography. These developments during and shortly after the end of World War II are intricately bound up with the

insbesondere Methoden aus Zahlentheorie, der arithmetischen Geometrie und der Computeralgebra eine wichtige Rolle. Für moderne kryptographische Verfahren sind Berechnungsprobleme erforderlich, die zwar „leicht" zu stellen, aber „schwer" zu lösen sind. Ein Beispiel: Unter den nicht-negativen ganzen Zahlen ist eine Primzahl eine Zahl größer als Eins, die nur durch Eins und sich selbst ohne Rest teilbar ist, wie beispielsweise 2, 3, 5, 7 und so weiter. Mit dem Computer lassen sich zwei zufällige Primzahlen mit 300 Dezimalstellen sowie ihr Produkt in wenigen Sekunden berechnen. Die umgekehrte Berechnung der Primzahlen aus dem Produkt hingegen nimmt nach gegenwärtigem Forschungsstand Jahre in Anspruch. Berechnungsprobleme zur Primfaktorzerlegung sind daher „leicht" zu stellen, aber „schwer" zu lösen. Entsprechend schnell können Verschlüsselungen oder digitale Signaturen erstellt werden, und entsprechend lange sind sie als sicher einzustufen.

Kurvenbasierte Kryptographie

Der Oldenburger Forschungsschwerpunkt zu den mathematischen und algorithmischen Grundlagen der Kryptographie befasst sich vor allem mit der kurvenbasierten Kryptographie. Hier kommen – ähnlich wie bei der Primfaktorzerlegung – zahlentheoretische Berechnungsprobleme zum Einsatz, nun allerdings für elliptische und allgemeiner für algebraische Kurven über endlichen Körpern. Dabei geht es um Effizienz und Sicherheit, um Verwendungsmöglichkeiten sowie um verwandte Fragen aus der Zahlentheorie und der arithmetischen Geometrie. Das Verhältnis von Effizienz und Sicherheit kryptographischer Verfahren ist bei elliptischen Kurven sehr viel günstiger als bei dem Beispiel zur Primfaktorzerlegung. Zudem gibt es darüber hinausgehende Verwendungsmöglichkeiten, etwa die paarungsbasierte Kryptographie. Diese Aspekte machen elliptische Kurven für die Kryptographie besonders interessant. In Deutschland verwendet man sie unter anderem in Pässen und Personalausweisen. Bei elliptischen Kurven handelt es sich zudem um deutlich strukturiertere, komplexere zahlentheoretische Objekte als Primzahlen. Das macht sie für Mathematiker besonders interessant, für Nichtmathematiker allerdings nur schwer verständlich.

Wichtige Teile der zugrunde liegenden mathematischen Theorie wurden in den 30er und 40er Jahren des 20. Jahrhunderts als Forschung zur reinen Mathematik ohne jeden Anwendungsbezug von den deutschen Zahlentheoretikern Helmut Hasse und Max Deuring erarbeitet. Siebzig Jahre später stellen diese Ergebnisse der Grundlagenforschung einen zentralen Bestandteil der angewandten Kryptographie dar. Über die Kryptographie hinaus nehmen elliptische Kurven eine bedeutende Rolle in Zahlentheorie und arithmetischer Geometrie ein. Dies kann zum Beispiel am großen Satz Pierre de Fermats und seinem Beweis oder an der Vermutung von Bryan Birch und Peter Swinnerton-Dyer gesehen werden – eins der größten offenen Probleme der Mathematik, das zu den so genannten Milleniumspreisproblemen zählt. Damit bietet die Kryptographie Zahlentheoretikern mit einem Interesse an Algorithmen ein interessantes Betätigungsfeld außerhalb des „Elfenbeinturms der reinen Mathematik".

Kryptographie als Wissenschaft

Die Kryptographie kann auf eine lange Entwicklung zurückblicken, die bis ins Altertum zurückreicht. Den Rang einer Wissenschaft erlangte sie erst im Lauf des 20. Jahrhunderts. Die Technologisierung der Kommunikation und die Erfindung von Rechenmaschinen, teilweise durch Anforderungen der Kryptographie selbst vorangetrieben, gaben wesentliche Impulse zur Entwicklung der Informationstheorie als mathematisch-informatischer Grundlage der Kryptographie durch Alan Turing und Claude Shannon. Diese Entwicklungen während und kurz nach dem Ende des Zweiten Weltkriegs sind eng mit der spannenden Geschichte der Chiffriermaschine Enigma verbunden, mit der das deutsche Militär seinen Nachrichtenverkehr verschlüsselte. Beststeller-Romane und Spionagefilme haben sie weltweit bekannt gemacht.

Mit ihrer Arbeit „New Directions in Cryptography" von 1976 begründeten Whitfield Diffie und Martin Hellman die Kryptographie mit öffentlichem Schlüssel, auf dem moderne, aktuelle kryptographische Verfahren zu wesentlichen Teilen beruhen.

Prof. Dr. Florian Heß

Florian Heß ist Professor für Mathematik und leitet die Arbeitsgruppe Computational Mathematics und diskrete Mathematik an der Universität Oldenburg. Nach der Promotion an der TU Berlin 1999 folgten Tätigkeiten als Postdoktorand in Sydney und Bristol sowie ab 2003 Professuren in Berlin und Mageburg. Seit 2010 forscht und lehrt Heß an der Universität Oldenburg. Seine Forschungsinteressen liegen in der Kryptographie sowie in der Zahlentheorie, algebraischen Geometrie und Computeralgebra.

Florian Hess is full professor for mathematics and is the head of the research group Computational and Discrete Mathematics at the University of Oldenburg. After his PhD in 1999 at TU Berlin he worked as a postdoc in Sydney and Bristol and as professor in Berlin and Magdeburg from 2003 on. Hess joined the University of Oldenburg in 2010. His research interests are in cryptography, number theory, algebraic geometry and computer algebra

Prof. Dr. Andreas Stein

Andreas Stein ist Professor für Mathematik und leitet die Arbeitsgruppe Algebra/Geometrie an der Universität Oldenburg. Nach der Promotion an der Universität des Saarlandes ging er 1997 als Postdoktorand nach Kanada an die Universitäten in Winnipeg und Waterloo. Bevor er 2008 nach Oldenburg kam, forschte und lehrte Stein in den USA an der University of Illinois at Urbana-Champaign und der University of Wyoming. Zu seinen Forschungsinteressen zählen unter anderem die algorithmische arithmetische Geometrie und die Kryptographie.

Andreas Stein is a full professor of Mathematics and is the head of the research group in Algebra/Geometry at the University of Oldenburg. After his Ph.D. in 1997 at the University of Saarland he worked as a post doctoral fellow in Canada at the universities in Winnipeg and Waterloo. Before he came to Oldenburg in 2008 he was a professor at the University of Illinois at Urbana-Champaign and at the University of Wyoming, both USA. His research interests include computational arithmetic geometry and cryptography.

Vernetzen die Oldenburger Kryptographie-Forschung und bauen sie aus: Andreas Stein (links), Florian Heß.

Andreas Stein (left) and Florian Heß are building up a cryptography research network at Oldenburg.

fascinating story of the Enigma encoding machine, which the German military used to encrypt its communications. Bestselling novels and spy films have made it famous the world over.

Cryptography as a Science

In their 1976 paper "New Directions in Cryptography", Whitfield Diffie and Martin Hellman layed the foundation of public-key cryptography, which forms an essential part of today's cryptographic technology. What was so groundbreaking about their work? If you imagine an encryption algorithm as a strongbox and the encryption process as encasing the message in the strongbox, up to that point in time sender and receiver needed the same secret key to lock and unlock the strongbox. This meant that the sender and the receiver had to have safely exchanged the key in advance. Diffie and Hellman introduced a new method with which sender and receiver – and only them – could calculate the secret key by exchanging publicly visible information. It was not long after this innovation that Ron Rivest, Adi Shamir and Leonard Adleman invented the RSA encryption algorithm that was named after them. It allowed the strongbox to be locked with a public key – but only opened again using a secret key. This brought enormous advantages for the exchange of keys and reduced the number of keys needed. The key innovation of both procedures was the introduction of computational problems from the field of number theory into cryptography. The RSA algorithm is based on the prime factor decomposition outlined above and is one of the most commonly applied encryption algorithms to date. As the opening of a secret archive at the end of the 1990s revealed, the British secret service had developed similar algorithms a number of years previously, without however making them public. In the mid-1980s Victor Miller and Neal Koblitz then introduced elliptic curves over finite fields into cryptography. Other relevant and contemporary number theoretical computational problems result from using lattices and linear codes. The security of public key cryptographic algorithms is based, as explained, on the fact that certain calculations are easy "forwards" and extremely difficult "backwards", with security increasing proportionally to difficulty. So far, however, high difficulty levels have remained unprovable. Such a proof would in fact solve another Millennium Prize Problem known as "P ≠ NP" at the same time. The security levels of cryptographic algorithms thus only reflect the current state of research as regards the estimated minimum effort required to solve the aforementioned calculations "backwards".

Of course calculations can be performed quicker by building better computers. The increase in computer performance has to date proven to be relatively easy to predict, making it possible to design computational problems that are sufficiently difficult and thus estimate security levels for a specific number of years. The spectre haunting applied cryptography, however, is the quantum computer. This is a theoretical computer model which would use quantum effects to perform certain calculations at a far faster rate than ordinary computers. A computer like this would render a large part of contemporary cryptography redundant, as Peter Shor demonstrated in the mid-1990s. It is however – fortunately

Private and Public Keys

Was war an dieser Arbeit so wegweisend? Stellt man sich ein Verschlüsselungsverfahren als Schatulle und den Verschlüsselungsprozess als Einschließen der Nachricht in der Schatulle vor, so mussten Sender und Empfänger bis dato den gleichen geheimen Schlüssel benutzen, um die Schatulle auf- und abzuschließen. Sender und Empfänger mussten also im Vorfeld den Schlüssel auf sichere Art und Weise austauschen. Diffie und Hellman führten nun eine Methode ein, mit der Sender und Empfänger – und nur diese – die geheimen Schlüssel durch Austausch öffentlich einsehbarer Informationen berechnen können. Kurz nach dieser Innovation erfanden Ron Rivest, Adi Shamir und Leonard Adleman das nach ihnen benannte RSA-Verschlüsselungsverfahren. Mit ihm lässt sich die Schatulle mit einem öffentlichen Schlüssel ab- und nur mit dem dazu passenden geheimen Schlüssel wieder aufschließen. Das bringt enorme Vorteile für den Schlüsselaustausch mit sich und reduziert die Anzahl benötigter Schlüssel. Die zentrale Neuerung beider Verfahren war die Einführung zahlentheoretischer Berechnungsprobleme in die Kryptographie. Das RSA-Verfahren basiert auf der oben dargelegten Primfaktorzerlegung und ist bis heute noch eines der meist eingesetzten Verschlüsselungsverfahren. Wie sich erst bei Öffnung geheimer Archive Ende der 90er Jahre zeigte, hatte der britische Geheimdienst schon einige Jahre früher ähnliche Verfahren entwickelt, aber nicht publik gemacht. Mitte der 80er Jahre haben dann Victor Miller und Neal Koblitz elliptische Kurven über endlichen Körper in die Kryptographie eingeführt. Weitere relevante und aktuelle zahlentheoretische Berechnungsprobleme ergeben sich aus Gittern und linearen Codes.

Private und öffentliche Schlüssel

Die Sicherheit kryptographischer Verfahren mit öffentlichem Schlüssel basiert, wie angedeutet, darauf, dass gewisse Berechnungen „vorwärts“ leicht und „rückwärts“ mit hohem Aufwand verbunden sind. Dabei gilt: Je höher der Aufwand, desto größer die Sicherheit. Hohe Aufwände konnten aber bisher in keinem Fall bewiesen werden. Ein solcher Beweis würde in der Tat ein weiteres Milleniumspreisproblem der Mathematik und Informatik namens „$P \neq NP$“ gleich mitlösen. Die Sicherheit kryptographischer Verfahren reflektiert daher nur den Forschungsstand bezüglich eines vermuteten Mindestaufwands besagter Berechnungen „rückwärts“.

Forschungslandschaft

Natürlich können Berechnungen auch dadurch schneller erledigt werden, dass man bessere Computer baut. Der Leistungszuwachs von Computern hat sich bisher als relativ gut vorhersehbar erwiesen, so dass man die Berechnungsprobleme ausreichend schwierig gestalten und die Sicherheit für eine konkrete Anzahl von Jahren abschätzen kann. Das Schreckgespenst der angewandten Kryptographie ist aber der Quantencomputer. Hierbei handelt es sich um ein theoretisches Modell eines Computers, der mittels Quanteneffekten gewisse Rechnungen extrem viel schneller als herkömmliche Computer lösen können sollte. Ein solcher Computer würde einen Großteil der aktuell benutzen Kryptographie unbrauchbar machen, wie Peter Shor Mitte der 90er Jahre gezeigt hat. Es ist allerdings, und vielleicht zum Glück, höchst fraglich, ob ein solcher Computer jemals gebaut werden kann. Für den Fall der Fälle gäbe es zumindest prinzipiell kryptographische Methoden, die einem Quantencomputer widerstehen können sollten.

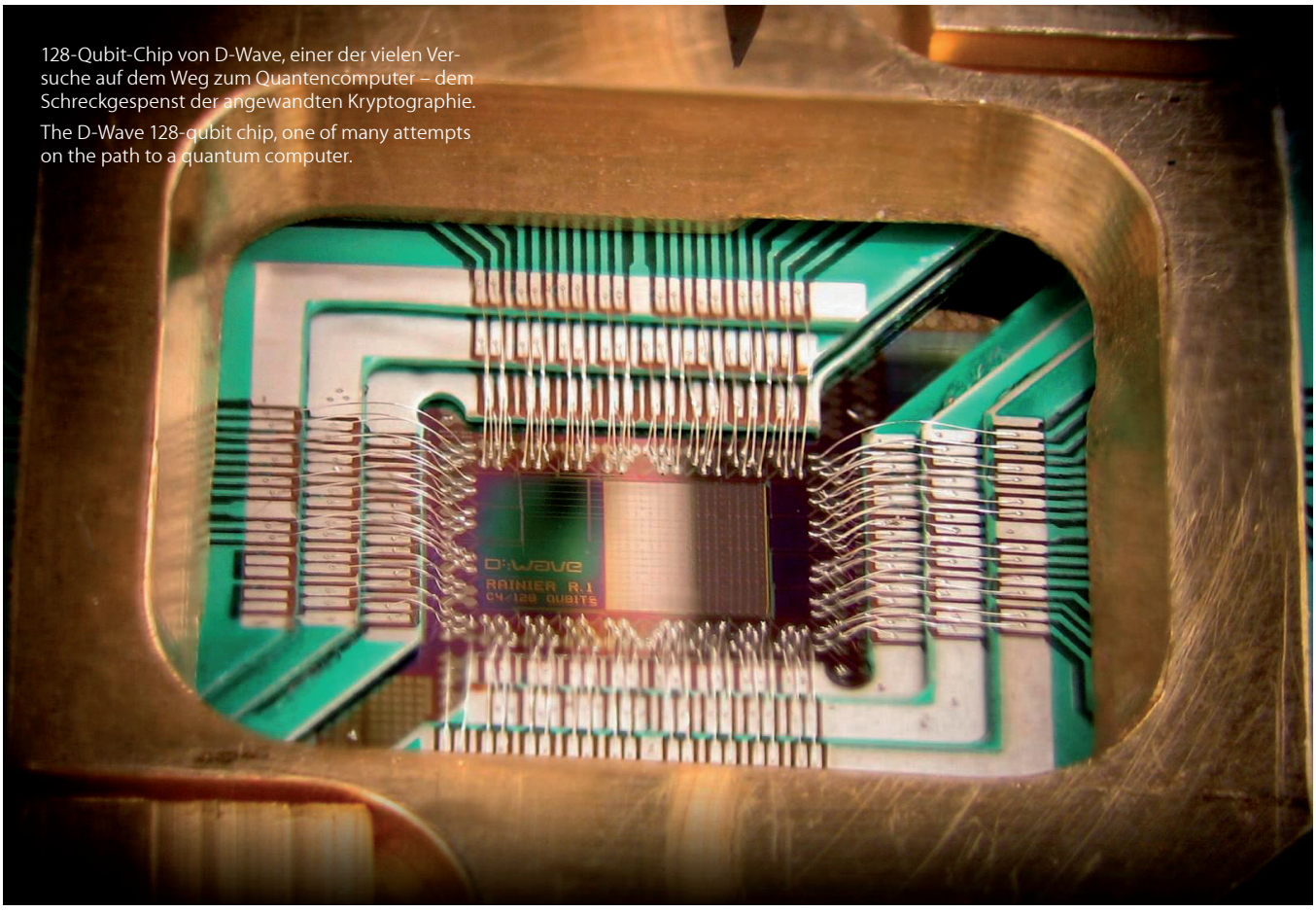
Die Kryptographie ist als Fachgebiet ausgesprochen interdisziplinär. Sie umfasst Bereiche der Mathematik, Informatik, Elektrotechnik und Physik. Wichtige mathematische Aspekte sind bereits angesprochen. Bei der Informatik dreht sich die Forschung insbesondere darum, wie die mathematischen Berechnungsprobleme konkret für spezielle kryptographische Aufgaben umgesetzt werden können und entwickelt entsprechende kryptographische Kommunikationsprotokolle. In der Elektrotechnik geht es um die Frage, wie kryptographische Berechnungen sich effizient in Hardware realisieren lassen und wie gespeicherte geheime Schlüssel wirklich geheim bleiben, auch wenn die Hardware allen möglichen physikalischen Untersuchungen unterworfen wird. Dies trifft zum Beispiel auf Chips in Bankkarten oder auf SIM-Karten in Mobiltelefonen zu. Der Oldenburger Forschungsschwerpunkt zu den mathematischen und algorithmischen Grundlagen der Kryptographie ist eingebettet in die regionale Forschungslandschaft zur sicherheitskritischen IT-Technologie, also Projekte, die vor allem am Department für Informatik der Universität und am Informatikinstitut OFFIS angesiedelt sind. Eine fachübergreifende Vernetzung kryptographiebezogener Forschung in Oldenburg und Emden mit einem breiten Spektrum an Themengebieten befindet sich gegenwärtig im Aufbau.

perhaps – highly questionable whether such a computer could ever be built. If this were the case, however, at least in principle cryptographic methods exist that would be capable of resisting even a quantum computer.

Research Landscape

Cryptography is a highly interdisciplinary field that spans areas of mathematics, computer science, electrical engineering and physics. The key mathematical aspects have already been outlined. As regards computer science, the research largely revolves around the application of mathematical computational problems to specific cryptographic tasks and the development of appropriate cryptographic communication protocols. In electrical engineering the issue is how to efficiently realize cryptographic calculations in computer hardware and guarantee that stored secret keys remain secret, even if the hardware is subjected to every possible physical scrutiny. This is relevant for chips in bank cards, for example, or SIM cards in mobile phones.

Oldenburg's research focus on the mathematical and algorithmic foundations of cryptography is embedded in the regional research landscape for safety-critical IT technology, that is in projects that are based primarily at the University's Department of Computer Science and the OFFIS Computer Science Institute. An interdisciplinary network of cryptography-related research in Oldenburg and Emden with a broad spectrum of research areas is currently under construction.



128-Qubit-Chip von D-Wave, einer der vielen Versuche auf dem Weg zum Quantencomputer – dem Schreckgespenst der angewandten Kryptographie.

The D-Wave 128-qubit chip, one of many attempts on the path to a quantum computer.