Sichere DATEN – auch in der Zukunft

Informationen haben sich zu einem wichtigen Wirtschaftsgut entwickelt – der Schutz dieser Daten ist eine zentrale Herausforderung des 21. Jahrhunderts. Prof. Antonia Wachter-Zeh will mit mathematischen Codes neue Verschlüsselungsmethoden entwickeln, die selbst leistungsfähigsten Quantencomputern standhalten. Ihre Verfahren sollen gleichzeitig helfen, Daten langfristig in DNA zu speichern.

Link
www.ei.tum.de/en/lnt

Full Article (PDF, EN): www.tum.de/faszination-forschung-27

Data Security – Now and in the Future

E

To prevent outsiders from eavesdropping on and misusing sensitive information, data is encrypted. The advent of quantum computers means that the security of some common encryption techniques is now under threat. Harnessing quantum physics, quantum computers are able to crack existing cryptographic systems – a major headache for secure IT communications. Although powerful quantum computers are only at the prototype stage, time is running out if we are to solve this problem. Antonia Wachter-Zeh, TUM Professor of Coding and Cryptography, is using algebraic codes to develop new encryption schemes able to withstand attack from quantum computers. Wachter-Zeh is also applying the concept of algebraic codes to DNA storage. This new storage technique involves writing data directly to DNA strands. Prof. Wachter-Zeh is aiming to use algebraic codes to correct read and write errors in DNA storage. □

Grafiken: ediundsepp (Quelle: TUM)

In einer zunehmend digitalisierten Welt ist es enorm wichtig, Daten zu schützen. Egal ob beim Home-Banking, beim Online-Shopping oder beim Austausch von Geschäftsdokumenten – um die Sicherheit der Daten und der Datenübertragung zu gewährleisten, werden diese verschlüsselt. Dafür stehen verschiedene Verschlüsselungsverfahren bereit, die je nach Einsatzzweck verwendet werden.

Weit verbreitet sind sogenannte asymmetrische Kryptosysteme. Diese Verschlüsselungsalgorithmen nutzen einen öffentlichen (public) und einen geheimen (private) Schlüssel und bilden die Basis vieler Krypto-Verfahren in der IT. Public-Key-Systeme werden im E-Mail-Verkehr ebenso verwendet wie beim Internet-Banking und bei der Kommunikation mit Web-Servern. Mathematisch beruht die Sicherheit der Public-Key-Verschlüsselung darauf, dass die Berechnung des geheimen Schlüssels aus dem öffentlichen Schlüssel äußerst schwierig ist – und selbst von den aktuell leistungsfähigsten Supercomputern nicht durchgeführt werden kann.

Damit könnte jedoch in den nächsten Jahren Schluss sein. Mit dem Bau von Quantencomputern sind die in der Praxis eingesetzten Public-Key-Verfahren wie RSA und Elliptic Curve Cryptography nicht mehr sicher. Wann es einen derart leistungsfähigen Quantencomputer geben wird, steht zwar noch nicht fest, doch dass er kommt, ist gewiss. Google, IBM und andere IT-Unternehmen haben bereits erste Prototypen entwickelt. Das Bundesamt für Sicherheit in der Informationstechnik geht davon aus, dass es Anfang der 30er Jahre eine Maschine geben wird, die ein kryptografisch relevantes Level erreicht und Public-Key-Verschlüsselungen brechen kann.

Gefahr Quantencomputer

Antonia Wachter-Zeh, Professorin für Coding and Cryptography an der TUM, ist sich der Tragweite dieser Gefahr bewusst. „Sobald es einen fähigen Quantencomputer gibt, der mit genügend Qubits rechnen kann, haben wir ein Problem bei den verbreiteten Public-Key-Kryptosystemen“, sagt sie. Die mit dem Heinz Maier-Leibnitz-Preis der Deutschen Forschungsgemeinschaft (DFG) ausgezeichnete Professorin will mit ihrer Forschungsgruppe im Rahmen des mit einem Starting Grant des European Research Council (ERC) geförderten Projekts inCREASE neue Verschlüsselungsmethoden entwickeln, die auch Quantencomputern standhalten.

Grundsätzlich bedrohen Quantencomputer nicht alle Verschlüsselungssysteme. Für die sehr effizienten symmetrischen Verschlüsselungsverfahren, wie beispielsweise AES, sind Quantencomputer eine relativ kleine Gefahr. Hier kann man der gestiegenen Rechenleistung mit längeren Schlüsseln entgegenwirken. Das Problem ist jedoch, dass beide Parteien den gleichen Schlüssel benötigen. Und für den Austausch dieses Schlüssels brauchen sie Public-Key-Verfahren. Somit sind Public-Key-Methoden zwar in der Praxis meist „nur“ für den Schlüsselaustausch des symmetrischen Verfahrens zuständig. Aber genau dieser Schlüsselaustausch ist essenziell. Und weil die für den Austausch notwendigen Verfahren komplett gebrochen sind, können sie in absehbarer Zeit nicht mehr verwendet werden.

Die Zeit für die Lösung des Problems ist schon heute kritisch. Vor allem die Hersteller langlebiger Produkte – wie

Autos, Flugzeuge oder Satelliten mit einem Lebenszyklus von weit über zehn Jahren – sind davon betroffen. „Wir wollen für die Daten, die wir heute kommunizieren, Langzeitsicherheit haben und unsere Systeme werden ja auch über sehr lange Zeit genutzt“, sagt Wachter-Zeh. „Satelliten im Orbit kann man beispielsweise schlecht updaten. Wir möchten aber, dass die Daten, die darüber kommuniziert werden, auch in 20 Jahren noch sicher sind.“
Ein weiterer Grund, sich bereits jetzt mit dem Problem zu beschäftigen, ist für Wachter-Zeh, dass die Kommunikation, die wir heute betreiben, oft gespeichert wird: „Auch in zehn oder 20 Jahren soll niemand in der Lage sein, das zu entschlüsseln, was wir heute kommunizieren.“

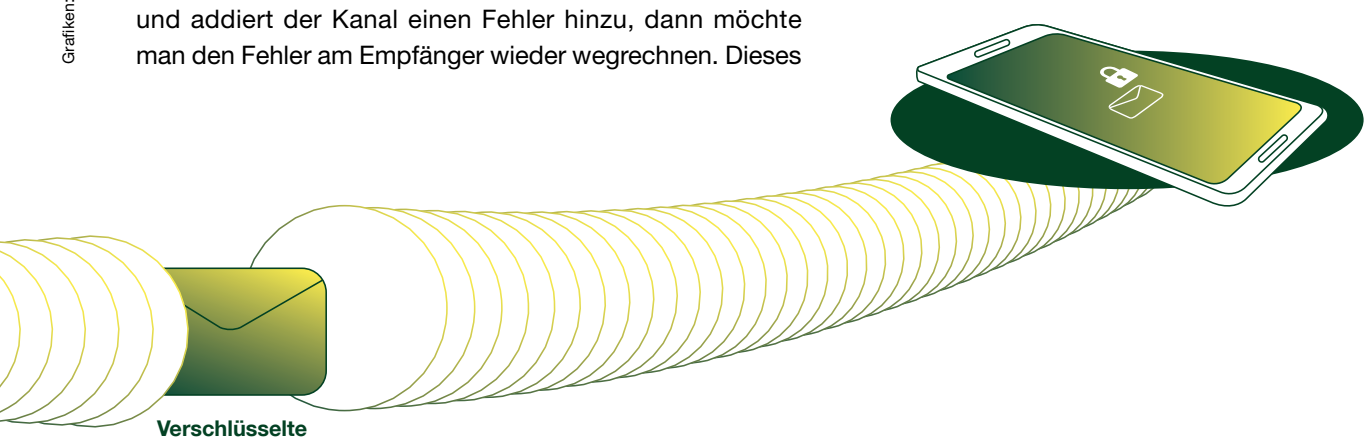
Post-Quantum-sichere Kryptografie

Es ist also höchste Zeit, auf Quantencomputer--sichere Verschlüsselungsverfahren umzustellen. Aus diesen Gründen hat das US-amerikanische National Institute of Standards and Technology (NIST) einen kryptografischen Wettbewerb ausgerufen, der sich aktuell in der finalen Runde befindet. Das Ziel ist die Etablierung einer sogenannten „Post-Quantum-Kryptografie“: die Standardisierung von Verschlüsselungssystemen, die selbst von Quantencomputern nicht zu entschlüsseln sind.
Im Kern geht es bei der Entwicklung Post-Quantum-sicherer Kryptografie um mathematische Konzepte, die sich in mehrere Gruppen einteilen lassen. Wachter-Zehs Gruppe erforscht solche sicheren Verschlüsselungsverfahren und nutzt dafür sogenannte fehlerkorrigierende Codes. Dieser vielversprechende Ansatz beruht auf der Korrektur von Fehlern, die bei der Übertragung oder Speicherung von Daten auftreten können. Er erlaubt es, Daten so zu codieren, dass eine bestimmte Anzahl an Fehlern ausgeglichen werden kann.
„Solche Codes werden in der klassischen Kommunikationstechnik verwendet und hängen im einfachsten Fall Redundanz an eine Nachricht an“, erklärt Wachter-Zeh. „Überträgt man in der Nachrichtentechnik ein Codewort und addiert der Kanal einen Fehler hinzu, dann möchte man den Fehler am Empfänger wieder wegrechnen. Dieses Grundprinzip lässt sich zum Verschlüsseln nutzen: Man wählt wissentlich einen gewissen Fehler, sodass dieser nicht von jemand anderem entschlüsselt werden kann.“
Wachter-Zeh ist Expertin für sogenannte Rank Metric Codes, einer bestimmten Klasse von fehlerkorrigierenden Codes. Die NIST stuft Rank-Metric-basierte Verfahren als extrem vielversprechend ein, sieht jedoch noch erheblichen Forschungsbedarf. Wachter-Zeh und ihre Gruppe haben einige der weltweit effizientesten Decodierverfahren für die Rank Metric entwickelt und ein neues Public-Key-System basierend auf Rank Metric Codes vorgeschlagen (LIGA).

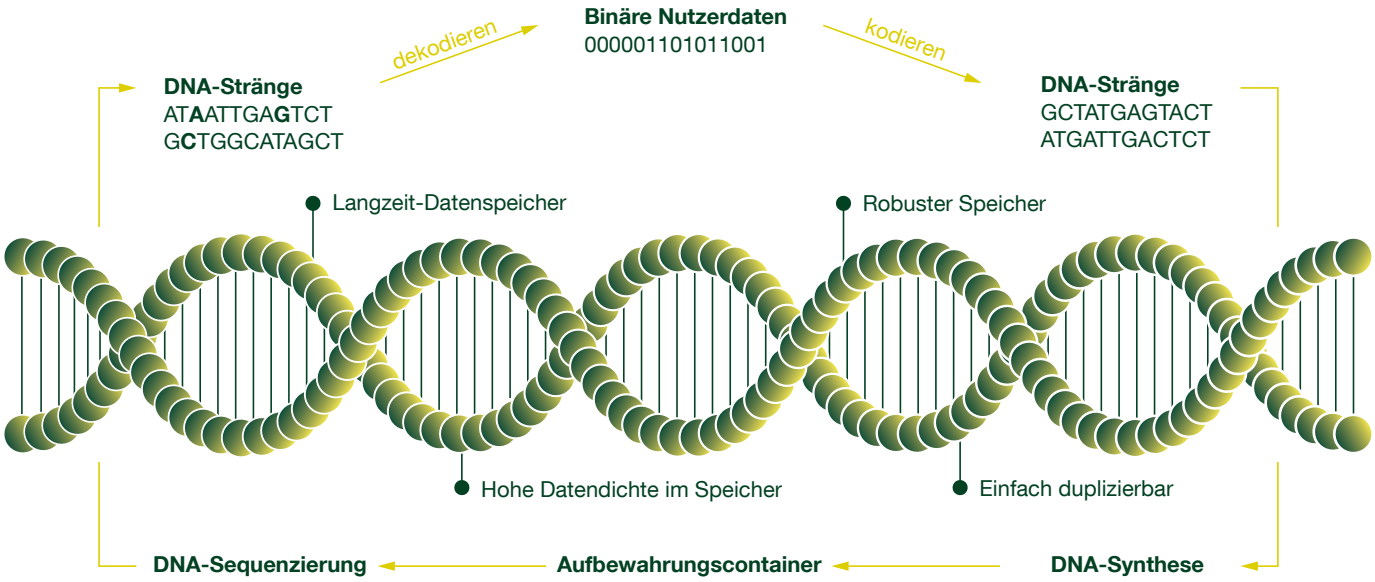
DNA-basierter Speicher

Von diesen fehlerkorrigierenden Codes verspricht sich Wachter-Zeh auch Lösungen für ein ebenso virulentes Thema: die Datenspeicherung in DNA. Bei dieser neuen Speichermethode werden Daten direkt in DNA-Strängen abgelegt. Die Nullen und Einsen der digitalen Daten werden dabei in die Basen transformiert, aus denen DNA besteht: Adenin (A), Cytosin (C), Guanin (G) und Thymin (T). Im einfachsten Fall fasst man immer zwei Bit zu einem DNA-Symbol zusammen.
Die Speicherung von Daten in DNA-Strängen hat das Potenzial, ein immer dringlicheres Problem zu lösen: Klassische Speichermedien wie DVDs oder Festplatten halten nur eine sehr begrenzte Zeit. Sollen Daten länger gehalten werden – etwa über Jahrzehnte –, so ist das Risiko eines Datenverlustes hoch.
Bei DNA-Storage ist die Haltbarkeit der Daten wesentlich höher. Bestes Beispiel sind uralte Mammutknochen, aus denen heute DNA wiederhergestellt werden kann. „Die DNA-Speicherfähigkeit von Fossilien kann für die Archivdatenspeicherung nachgeahmt werden. Wenn wir über Generationen Daten speichern wollen, dann eignet sich DNA-based Storage dafür gut.“

Grafiken: ediundsepp (Quelle: TUM)



Verschlüsselte Nachricht



Beim Speichern von Daten in DNA werden die Nullen und Einsen der binären Ausgangsdaten in eine bestimmte Abfolge der vier DNA-Basen A, C, G und T überführt. Das Speichern von Daten in DNA könnte mehrere Probleme lösen, darunter die Lebensdauer und die Kapazität konventioneller Datenspeicher.

Prof. Antonia Wachter-Zeh

ist Professorin an der Fakultät für Elektro- und Informationstechnik. Sie erlangte im Jahr 2009 an der Universität Ulm den Master of Science in Kommunikationstechnik. Dort und an der Université de Rennes in Frankreich erwarb sie 2013 ihren Doktortitel. Von 2013 bis 2016 war sie Postdoktorandin am Technion – Israel Institute of Technology in Haifa, Israel, und von 2016 bis 2020 Tenure Track Assistant Professor an der TUM. Wachter-Zeh wurde mit dem Heinz Maier-Leibnitz-Preis der DFG ausgezeichnet und wird mit einem ERC Starting Grant gefördert. Ihre Forschungsinteressen sind Codierungstheorie, Kryptografie und Informationstheorie sowie deren Anwendung auf Speicherung, Kommunikation, Privacy und Sicherheit.

Ein weiterer Vorteil von DNA-Speichern ist, dass die Gen-Sequenzen sehr dicht sind und man auf sehr wenig Platz sehr viele Daten unterbringen kann. „Während von den aktuellen Archivspeichermedien das Band mit maximal 100 GB pro Kubikmillimeter die höchste Datendichte aufweist, bringt man in DNA zehn hoch neun GB pro Kubikmillimeter unter“, sagt Wachter-Zeh.

Fehler eliminieren

Bis DNA-basierte Storage praktisch verwendbar ist, müssen allerdings noch eine ganze Reihe von Hindernissen beseitigt werden. Dies betrifft vor allem das Schreiben und Lesen der Daten. Das Schreiben der Daten in die DNA, die sogenannte DNA-Synthese, ist derzeit der kostspieligste Teil der Speichersysteme. Wachter-Zehs Gruppe versucht, dies effizienter zu machen. „Wir möchten mehrere Sequenzen gleichzeitig und möglichst schnell schreiben“, sagt die TUM Professorin. „Wenn das eine Maschine parallel machen kann, stellt sich die Frage, wie das aus theoretischer Sicht am besten zu bewerkstelligen ist.“ Dazu betrachtet sie Syntheseverfahren, bei denen viele Stränge parallel und schrittweise unter Verwendung einer festen Supersequenz aufgebaut werden.

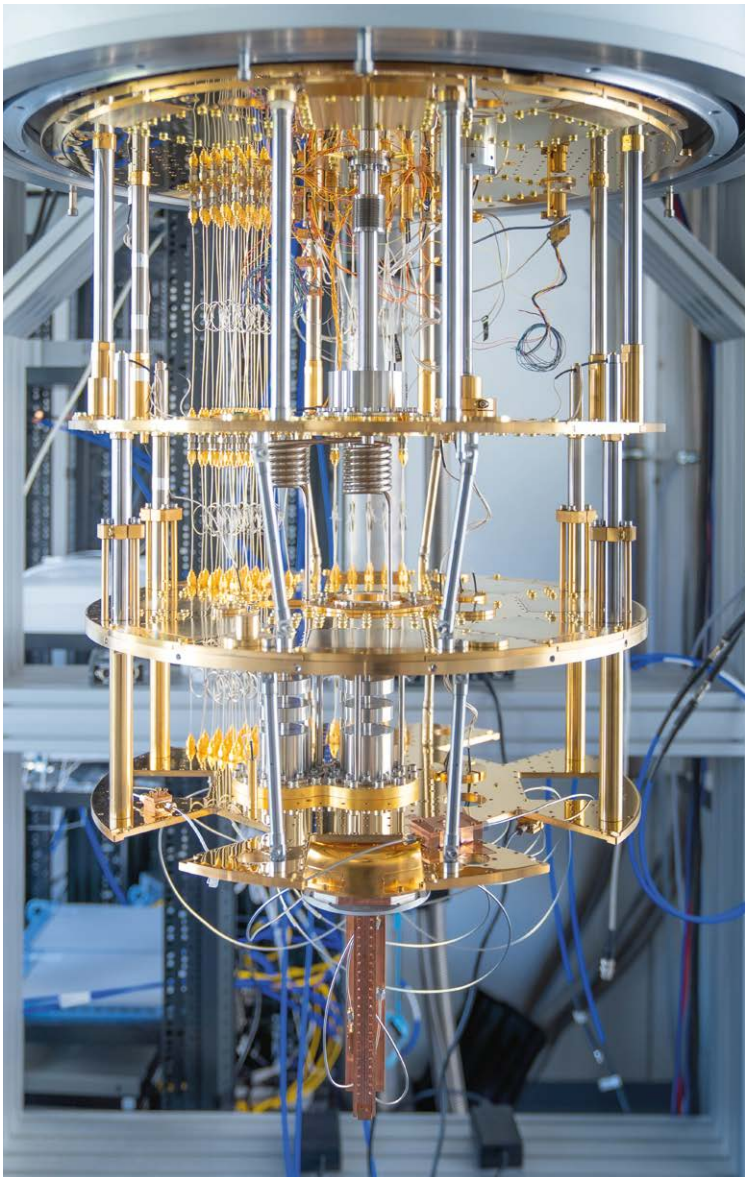
Der zweite Schwerpunkt, mit dem sich die Forschungsgruppe beschäftigt, ist das Lesen der Daten. Dies stellt aktuell mit die größte Herausforderung bei DNA-basierten Speichersystemen dar. Grundsätzlich erfolgt das Auslesen der Daten mit DNA-Sequenzierung. Weil jeder Strang sehr oft vervielfältigt wird, liegen die gelesenen Sequenzen immer in einer Art Cluster um die geschriebenen herum. Man bekommt dabei eine Menge von Strängen zurück und muss diese irgendwie sortieren.

Zusätzlich treten unterschiedliche Fehler auf. So können Sequenzen verloren gehen, weil sie nicht ausgelesen werden. Auch die Ordnung der Sequenzen kann verloren gehen und es können Symbole innerhalb von Sequenzen eingefügt, gelöscht oder dupliziert werden.

Beim Lesen der Daten müssen diese Fehler korrigiert werden. „In der Vergangenheit zeigte sich, dass DNA-Systeme ohne Fehlerkorrektur kaum Daten wiederherstellen konnten“, erklärt Wachter-Zeh. „Es traten einfach zu viele Fehler auf. Eine Fehlerkorrektur ist deshalb essenziell – und dazu kann man bekannte Verfahren aus der Nachrichtentechnik verwenden.“

Auch hier nutzt Wachter-Zeh fehlerkorrigierende Codes. Da Fehler wie Löschungen von Symbolen auftreten, müssen allerdings ganz neue Verfahren entwickelt werden. Ihre Forschungsgruppe kann dabei von ihrer Expertise in der Methodologie profitieren. So hat ihre Gruppe ein allgemeines Prinzip entwickelt, um Codierung über ungeordnete Sequenzen zu ermöglichen. Wachter-Zeh ist außerdem weltweit führend in der Entwicklung von Codes, die Insertions und Deletions – also das fehlerhafte Einfügen oder Löschen von Symbolen – korrigieren können.

■ *Klaus Manhart*



Kryogene Infrastruktur zum Betrieb eines supraleitenden Quantencomputers am Walther-Meißner-Institut, gefördert durch das Münchner Exzellenzcluster MCQST. Viele Oberflächen und elektrische Kontakte sind vergoldet, um einen minimalen elektrischen Widerstand und eine maximale thermische Leitung zu erhalten.

Bildquellen: Astrid Eckert/TUM, C. Hohmann/MCQST; Grafiken: ediundsepp (Quelle: TUM)