Medieninformation

TECHNISCHE UNIVERSITÄT DARMSTADT

Die nächste Generation sicherer Verschlüsselung

TU Darmstadt wappnet sich mit Partnern gegen Quantencomputer

Kommunikation und Medien
Corporate Communications

Karolinenplatz 5
64289 Darmstadt

Ihr Ansprechpartner:
Jörg Feuck
Tel. 06151 16 - 20018
Fax 06151 16 - 23750
feuck@pvw.tu-darmstadt.de

www.tu-darmstadt.de/presse
presse@tu-darmstadt.de

Darmstadt, 17. Januar 2017. Wissenschaftler der TU Darmstadt forschen mit dem Bundesamt für Sicherheit in der Informationstechnik und dem Chiphersteller Intel an Strategien für das Post-Quantum-Zeitalter.

An Quantencomputern wird weltweit intensiv geforscht. Experten schätzen, dass 2025 ein funktionierender Quanten-Computer gebaut werden könnte – dieser könnte bisher benutzte Public-Key-Verschlüsselungs- und Signaturverfahren brechen. Damit geschützte Daten wären offengelegt und entsprechende Signaturen wären fälschbar. Um sich auf das sogenannte Post-Quantum-Zeitalter vorzubereiten, forscht ein Team der TU Darmstadt um Professor Johannes Buchmann, Sprecher des Sonderforschungsbereichs CROSSING, mit Partnern aus der Industrie und Behörden an neuen kryptographischen Verfahren, die auch von einem Quantencomputer nicht gebrochen werden können. CROSSING-Wissenschaftler führen zu diesem Thema eine Studie für das BSI durch und kooperieren auch eng mit der Forschungsabteilung von Intel, den Intel Labs.

Klassische Public-Key-Verfahren vor dem Ende

Zusammen mit den Intel Labs entwickeln und testen die CROSSING-Wissenschaftler vielversprechende neue Verschlüsselungsverfahren, die die traditionellen Methoden im Post-Quantum-Zeitalter ablösen könnten. „Praktisch überall im Internet, ob geschäftlich oder privat, brauchen wir Verschlüsselung“, erklärt Professor Johannes Buchmann. Online-Banking sei das bekannteste Beispiel, aber auch das Versenden von E-Mails oder das Einkaufen im Internet werden im Hintergrund verschlüsselt geschützt. Sobald effiziente und im großen Stil nutzbare Quantencomputer existieren, können herkömmliche Verschlüsselungsmethoden allerdings durch die extrem schnellen und leistungsfähigen Quantenalgorithmen gebrochen werden. Dr. Rachid El Bansarkhani, Projektleiter der Forschungskollaboration an der TU Darmstadt, warnt: „Die klassischen Public-Key-Verfahren, beispielsweise RSA oder ECC, könnten bald unsicher werden. Deswegen müssen wir jetzt an neuen Verfahren arbeiten.“
Die Forschung zu Post-Quantum-Verschlüsselungstechniken ist essentiell, um auch in Zukunft Sicherheit und Privatsphäre zu gewährleisten und für die potenziellen Gefahren durch Quantencomputer gewappnet zu sein. Anand Rajan, Leiter der Forschungskollaboration bei den Intel Labs, bekräftigt: „Dass kryptographische Systeme auch zukünftigen

Sicherheitsanforderungen gewachsen sind, ist eine wesentliche Voraussetzung für Intel-Produkte. Um eine solche langfristige Sicherheit zu gewährleisten, erforscht Intel Labs die potenziellen Konsequenzen der Entwicklung großer Quantencomputer, die eines Tages die bisherigen Public-Key-Verschlüsselungsverfahren brechen könnten. Wir arbeiten mit dem auf diesem Gebiet führenden CROSSING-Projekt und der TU Darmstadt zusammen, um Alternativen zu untersuchen und umsetzbare, zukunftssichere kryptographische Systeme zu identifizieren."

Post-Quantum-Kryptographie in die Praxis bringen

Eine vielversprechende Verschlüsselungstechnologie für das Post-Quantum-Zeitalter ist die gitterbasierte Kryptographie – resistent gegen Angriffe von Quantencomputern sowie effizient und praktikabel umzusetzen. Für das Bundesamt für Sicherheit in der Informationstechnik (BSI) führen CROSSING-Wissenschaftler eine Bewertung gitterbasierter kryptographischer Verfahren durch. „Da das BSI regelmäßig Empfehlungen zu Themen der IT-Sicherheit ausspricht, können wir mit diesem Projekt dazu beitragen, dass die Gitter-Kryptographie schneller den Weg in die Praxis findet", erklärt Dr. Juliane Krämer, stellvertretende Projektleiterin.

Hintergrund:

Sonderforschungsbereich CROSSING

Mehr als 65 Wissenschaftler aus Kryptographie, Quantenphysik, Systemsicherheit und Softwaretechnik arbeiten an der TU Darmstadt in CROSSING zusammen und betreiben sowohl Grundlagen- als auch anwendungsorientierte Forschung. Das Ziel ist es, Kryptographie-basierte Sicherheitslösungen zu entwickeln, um auch in der Zukunft sichere und vertrauenswürdige Rechenumgebungen zu schaffen. Neben hohen Ansprüchen an die Effizienz und Sicherheit der entwickelten Lösungen, spielt auch die Benutzbarkeit eine große Rolle: Software-Entwickler, Administratoren und sogar Endanwender sollen in der Lage sein, die Lösungen zu verwenden, auch wenn sie keine Kryptographie-Experten sind.

CROSSING wird seit Oktober 2014 als Sonderforschungsbereich der Deutschen Forschungsgemeinschaft (DFG) mit 8 Millionen Euro gefördert. Das Programm ist auf bis zu zwölf Jahre ausgelegt.

Public-Key-Verschlüsselungsverfahren

Das RSA-Verschlüsselungsverfahren schützt im sogenannten TLS-Protokoll (Transport Layer Security) die Kommunikation im Internet, sei es beim Onlinebanking oder auf Shoppingwebseiten. Auch E-Mails werden mit dem RSA-Verfahren verschlüsselt.

TECHNISCHE UNIVERSITÄT DARMSTADT

RSA ist ein Public-Key-Verfahren: Jeder Kommunikationspartner hat einen privaten und einen öffentlichen kryptographischen Schlüssel. Das Schlüsselpaar ist über eine sogenannte Einwegfunktion miteinander verbunden, eine Berechnung, die in die eine Richtung einfach, in die andere aber schwierig bis unmöglich ist. Für das RSA-Verfahren werden hinreichend große Primzahlen benutzt: der private Schlüssel besteht aus Primzahlen, die miteinander multipliziert den öffentlichen Schlüssel ergeben – eine einfache Rechenoperation. Das Zerlegen zurück in die Primfaktoren hingegen ist sehr aufwendig, und mit der Rechenleistung heutiger Computer nicht zu bewerkstelligen. Der private Schlüssel ist sicher – solange kein Quantencomputer entwickelt ist, der mit seiner dramatisch höheren Rechenleistung die „schwere Richtung" der Einwegfunktion berechnen und die Verschlüsselung brechen kann.
ECC-Verschlüsselungsverfahren (Elliptic Curve Cryptography) funktionieren ebenfalls nach dem Prinzip der Public-Key-Verschlüsselung, statt Primzahlen wird aber das „diskrete-Logarithmus-Problem" als Einwegfunktion genutzt.

Internet:
www.crossing.tu-darmstadt.de

Ansprechpartner:
Sonderforschungsbereich CROSSING
Prof. Johannes Buchmann
Kontakt über: Ann-Kathrin Braun
Tel.: 06151 / 16-22662
E-Mail: akbraun@cysec.tu-darmstadt.de,

MI-Nr. 04/2017, Braun/feu