BSI
19. Deutscher
IT-Sicherheitskongress
10.-11. Mai 2023

Post-Quanten-Kryptografie und neue Algorithmen

Standardisierungsprozesse und stärkere Hardware

(BS/Alexander Wagner) Im Jahr 1994 veröffentlichte Peter Shor seine Arbeiten zur Berechnung von diskreten Logarithmen und Faktorisierung. Was zunächst sehr abstrakt klingt, könnte in der nahen Zukunft konkret beeinflussen, wie wir über das Internet kommunizieren.

Chipkarten wie diese enthalten einen kleinen Arbeitsspeicher, über den die Verschlüsselungssignatur läuft. Für post-quantensichere Verschlüsselungen müssten diese Arbeitsspeicher größer werden. Foto: BS/PublicDomainPictures, pixabay.com

Alexander Wagner forscht bei Fraunhofer AISEC zu Post-Quanten-Kryptografie und Hardware-Sicherheit.
Foto: BS/Ulrike Jehle

Denn Kryptosysteme auf Basis von RSA und elliptischen Kurven, wie sie heutzutage verwendet werden, um sicher Daten auszutauschen, funktionieren aufgrund der Komplexität dieser Probleme. Nach unserem aktuellen Kenntnisstand können Dritte mit klassischen Computern die Verschlüsselung auch dann nicht aufbrechen, wenn sie bis zum voraussichtlichen Ende des Universums rechnen. Für Quantencomputer gilt diese Annahme seit der wegweisenden Arbeit von *Peter Shor* nicht mehr.

Noch ist eine Anwendung des Shor-Algorithmus auf existierende kryptografische Verfahren nicht möglich, da heutigen Quantencomputern dafür die Rechenleistung fehlt. Mit dem Begriff Post-Quanten-Kryptografie werden verschiedene Verfahren bezeichnet, die eine sichere Verschlüsselung auch gegen Angriffe von Quantencomputern versprechen. Eine allgemeine Umstellung auf solche Verfahren bringt jedoch verschiedene Herausforderungen mit sich und ist noch nicht absehbar.

Wann brauchen wir Alternativen?

Die Entwicklung von leistungsfähigen Quantencomputern ist zeitlich schwer abschätzbar. Dennoch betreffen uns die zukünftigen Auswirkungen schon heute. Nach heutigem Stand der Technik können sichere Datenübertragungen mit rechenstarken Quantencomputern in der Zukunft gebrochen werden. Es ist also realistisch, dass verschlüsselte Datenübertragungen heute aufgezeichnet und nachträglich mithilfe von Quantencomputern entschlüsselt werden. Damit wären vertrauliche Daten, die heute übertragen werden, in Zukunft für Dritte lesbar.

Des Weiteren beginnt die Sicherheit unserer heutigen IT-Systeme häufig in Hardware-Bausteinen, sogenannten Roots of Trust. Diese sind für die Umsetzung fundamentaler Sicherheitsfunktionen verantwortlich, die die Grundlage für Sicherheitsmechanismen auf höheren Systemschichten bilden. Dafür genutzte kryptografische Verfahren sind oft direkt in Hardware implementiert, eine Änderung des zugrunde liegenden Verfahrens ist daher schwer bis unmöglich. Um neue Post-Quanten-Kryptografie-Verfahren zu adaptieren, müssen also neue Generationen von Roots of Trust entwickelt und in IT-Systeme eingebaut werden.

Damit unsere Kommunikation und unsere IT-Systeme auch in Zukunft sicher sind, benötigen wir schon heute Post-Quanten-Kryptografie und sichere Implementierungen.

Status quo der Sicherheitsforschung

Post-Quanten-Kryptografie ist ein aktuelles Forschungsthema mit vergleichsweiser kurzer Historie. Neben den Verfahren selbst ist auch die Sicherheit und die Effizienz der Implementierungen im Fokus. Dafür müssen Post-Quanten-Algorithmen auch im Kontext von Seitenkanalanalysen und Fehlerangriffen analysiert werden. In diesem Forschungsfeld sind wir, das Fraunhofer AISEC, aktiv. In der Hardware-Security-Abteilung des Fraunhofer AISEC analysieren wir Algorithmen und Implementierungen auf ihre Resilienz gegenüber Schwachstellen und auf ihr Optimierungspotenzial. Dieses Verständnis ermöglicht uns die Entwicklung gehärteter und effizienter Implementierungen. Der Übergang zu post-quantensicheren IT-Systemen ist ein dynamischer Prozess, welcher uns in den nächsten Jahren fortlaufend begleiten wird.

Zum einen schreitet die Standardisierung von Post-Quanten-Kryptografie stetig voran. Beispielsweise wurden durch die Internet Engineering Task Force erste Signaturverfahren standardisiert (LMS und XMSS), welche sowohl vom US-amerikanischen National Institute of Standards and Technology (NIST) als auch vom Bundesamt für Sicherheit in der Informationstechnik (BSI) als sicher angesehen werden. Daneben hat das Auswahlverfahren des NIST weitere Post-Quanten-Algorithmen hervorgebracht. Für die Durchführung eines Schlüsselaustauschs ist dies der Algorithmus CRYSTALS-Kyber und für die Erstellung und Überprüfung digitaler Signaturen sind das die Algorithmen CRYSTALS-Dilithium, FALCON, und SPHINCS+.

Zusätzlich läuft dieses Jahr noch ein Auswahlverfahren des NIST an, um weitere Post-Quanten-Signaturalgorithmen zu finden. Zum anderen ist eine sofortige Umstellung auf Post-Quanten-Kryptografie (noch) nicht ohne Eingriffe in heutige IT-Infrastruktur möglich. Bis dato bekannte Verfahren der Post-Quanten-Kryptografie benötigen zum Beispiel größere Datenspeicher oder längere Laufzeiten zur Berechnung. Diese Herausforderungen müssen vor einer allgemeinen Umstellung auf Post-Quanten-Kryptografie noch gelöst werden.