

Assignment #8: Kryptographie

Lecture: D3.2: Information Security and Privacy

Abgabe: 16.12.2022 - 12:00 - per Moodle

1. Sie finden auf Seite zwei, drei und vier einen wissenschaftlichen Text über den, in der ersten Vorlesung anmoderierten, Quantencomputer. Lesen Sie sich in das Dokument ein, welches Ihnen einen ersten Eindruck über wissenschaftliche Publikationen vermittelt. Beantworten Sie in einer kurzen Dokumentation die folgenden Fragen. Sie finden die Antworten im Text.
 - (a) (2p.) Was ist die Main Botschaft des Artikels?
 - (b) (4p.) An welchen Punkten des bereits behandelten Materials, in der Vorlesung, können die Ergebnisse aus (a) angewendet werden? Begründen Sie Ihre Antwort.
 - (c) (4p.) Geben Sie Ihre Ideen an, was die Bedeutung des Apfels, der Möhre und der Zitrone sein kann.

QUANTENSICHER

TEXT: PETER HERGERSBERG

Für die Onlinekommunikation ist es ein bedrohliches Szenario: Sobald es leistungsfähige Quantencomputer gibt, sind die heutigen Verschlüsselungstechniken schlagartig unsicher. Peter Schwabe, Forschungsgruppenleiter am Max-Planck-Institut für Sicherheit und Privatsphäre, entwickelt daher mit internationalen Partnern Methoden der Post-Quanten-Kryptografie. Vier solcher Verfahren standardisiert nun das National Institute for Standards and Technology in den USA – an dreien davon war Peter Schwabe beteiligt.

Der Quantencomputer ist für viele eine Verheißung – ganz bestimmt für die Geheimdienste dieser Welt. Online-dienste, die auf einen sicheren Datenaustausch angewiesen sind, sehen darin dagegen auch eine Bedrohung. Es ist noch nicht abzusehen, wann die ersten leistungsfähigen Rechner dieser Art ihre Arbeit aufnehmen werden. Klar ist aber: „Die kryptografischen Protokolle, die heute quasi den gesamten Datenverkehr schützen, sind wertlos, sobald es die ersten Quantencomputer gibt“, sagt Peter Schwabe, Forschungsgruppenleiter am Max-Planck-Institut für Sicherheit und Privatsphäre und Professor an der Radboud-Universität in Nijmegen.

„Denn sie können die beiden mathematischen Probleme lösen, auf denen heutige kryptografische Methoden beruhen.“ So können sie eine große Zahl im Handumdrehen in zwei Primzahlfaktoren zerlegen. Da herkömmliche Computer dafür Zehntausende Jahre benötigen würden und dabei auch noch so viel Energie verschlängen, wie die Sonne in diesem Zeitraum zur Erde schickt, bildet die Primzahlfaktorisation den Kern einer weitverbreiteten Verschlüsselung.

Um den Datenverkehr künftig auch gegen Angriffe mit Quantencomputern zu schützen, haben 69 Teams beim National Institute for Standards and Technology (NIST) Vorschläge für neue kryptografische Methoden eingereicht; sie sprechen von Post-Quanten-Kryptografie. Nach einigen Runden hat das NIST entschieden, vier dieser Verfahren zu standardisieren. „Sie stellen einen besseren Schutz für die digitale Kommunikation dar – gerade weil Quantencomputer die bisherigen Verschlüsselungsmethoden und Signatursysteme aushebeln würden“, sagt Eike Kiltz, der als Professor an

der Ruhr-Universität Bochum forscht und lehrt und mit Peter Schwabe und zahlreichen Partnern an solchen neuen Verschlüsselungstechniken arbeitet.

Drei der ausgewählten Methoden dienen der Authentifizierung, darunter die Verfahren Sphincs+ und Crystals-Dilithium, an deren Entwicklung Peter Schwabe beteiligt war: „Bei der Authentifizierung stellt eine digitale Signatur sicher, dass etwa ein Server auch tatsächlich der ist, der er vorgibt zu sein.“ Schwabe koordinierte zudem das internationale Team, das Crystals-Kyber konzipiert und zur Anwendungsreife gebracht hat. Mit diesem Verfahren werden auf sichere Weise Schlüssel für die weitere Kommunikation übertragen.

Am Beispiel des Schlüsselaustauschs lassen sich einige Aspekte der Kryptografie gut erklären: In vielen Anwendungen, sei es ein Messengerdienst oder ein Onlineeinkauf, werden Daten mit asymmetrischen Verfahren verschlüsselt. Das heißt, der Schlüssel zum Verschlüsseln einer Nachricht ist öffentlich. Nur der Code zum Ent-

61



schlüsseln der Botschaft ist geheim. Im Gegensatz zu symmetrischen Kryptografiertechniken, die mit nur einem geheimen Schlüssel arbeiten, können die öffentlichen Schlüssel asymmetrischer Verfahren über nicht sichere Kanäle ausgetauscht werden. Denn was ist schon ein sicherer Kanal? Nicht von ungefähr erhalten wir eine Geheimzahl der Bank als aufwendig verpackten Rubbelcode. So einen Geheimbrief an jeden E-Mail-Kontakt zu schicken, dürfte wohl die Freude an der Onlinekommunikation rasch verderben. Zu den asymmetrischen Methoden der Kryptografie gehört auch das weitverbreitete RSA-Verfahren, das letztlich auf der Primzahlfaktorisation beruht, aber durch Quantencomputer ausgehebelt werden kann.

Einfache, effiziente und sichere Verfahren

62 Techniken der Post-Quanten-Kryptografie wie etwa Crystals-Kyber arbeiten daher mit mathematischen Problemen, die für Quantencomputer nach heutigem Wissensstand fast so knifflig sind wie für herkömmliche Rechner. Dabei sind die eigentlichen Rechenoperationen bei Crystals-Kyber denkbar einfach – es geht nur um Multiplizieren und Addieren: Ein Wert, genauer gesagt ein Polynom, wird mit einem anderen Wert multipliziert, der der geheime Schlüssel ist. Zu dem Produkt wird ein weiterer Wert addiert, der das Ganze kompliziert macht. Der geheime Schlüssel und der addierte Wert – auch dabei handelt es sich um Polynome – sind klein. Trotzdem ist es in dieser Konstellation beliebig schwierig, den geheimen Schlüssel zu ermitteln, selbst wenn man das Ergebnis dieser Operation und das Ausgangspolynom kennt, die gemeinsam als öffentlicher Schlüssel dienen.

„Auf diesem Prinzip beruhen einige der Vorschläge für die Post-Quanten-Kryptografie“, erklärt Peter Schwabe. Aber es kommt nicht nur auf das mathematische Problem hinter einem

Verfahren an, sondern auch darauf, wie die Rechenvorschrift in Softwarecode formuliert wird. Genau das beherrscht Peter Schwabe besonders gut. „Bei der Implementierung müssen wir zahlreiche Faktoren gegeneinander abwägen, weil ein Gewinn bei dem einen immer auf Kosten eines anderen geht. Mein Beitrag bestand darin, viele Entscheidungen so zu treffen, dass das Verfahren letztlich einfach, effizient und vor allem sicher ist.“ Genau das waren die Kriterien, nach denen das NIST seine Auswahl getroffen hat. Jetzt wird es zu den ausgewählten Verfahren Standards schreiben. Das heißt, es wird die kryptografischen Techniken erläutern und auch Hinweise formulieren, damit beispielsweise Onlinedienste sie vergleichsweise einfach in ihre Anwendungen einbinden können – und vor allem, ohne dabei Löcher in die Sicherungsvorkehrungen zu reißen.

Gegen die Arbeit des NIST gibt es auch Vorbehalte. Manche Kritiker fürchten, die Behörde könnte auf Geheiß der NSA Verschlüsselungsmethoden standardisieren, welche dem US-Geheimdienst Hintertüren offen lassen. „Es ist ziemlich sicher, dass dies in der Vergangenheit in einem Fall geschehen ist“, erzählt Peter Schwabe. Das habe die Behörde aber vermutlich nicht wissentlich getan und inzwischen selbst auch als großen Fehler eingeräumt. „Das Verfahren mit der Hintertür kam – anders als die Methoden, die jetzt zur Auswahl standen – nicht aus der Wissenschaft. Heute ist die Kryptocommunity an der Auswahl auch stärker beteiligt.“ So klopfen jetzt nicht mehr nur das NIST die zur Wahl stehenden Methoden auf mögliche Sicherheitslücken ab, sondern auch nahezu die gesamte Kryptografiegemeinde der Welt. „NIST hat die Auswahl neuer Kryptografiestandards bereits zweimal so gestaltet wie bei der Post-Quanten-Kryptografie“, sagt Peter Schwabe. „Und die Verfahren, die dabei herausgekommen sind, haben sich als sehr sicher erwiesen – und sie werden heute auf der ganzen Welt genutzt.“

Es ist daher gut möglich, dass das NIST mit seiner Entscheidung zumindest für die USA und Europa Standards setzt. Das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt in einer technischen Richtlinie allerdings schon seit 2020 zwei andere Methoden für den Schlüsselaustausch im Zeitalter des Quantencomputers. „Diese Verfahren halten wir für besonders sicher“, sagt Stephan Ehlen, der als Mathematiker beim BSI quantensichere Verschlüsselung untersucht. Sie beruhen auf einem mathematischen Problem, das mit dem Prinzip von Crystals-Kyber verwandt ist. Allerdings seien diese Verfahren nicht so effizient wie jene, die das NIST nun standardisiert, sagt Ehlen. Für das

AUF DEN PUNKT GEBRACHT

Sobald es leistungsfähige Quantencomputer gibt, sind heutige Verschlüsselungstechniken schlagartig unsicher.

Das National Institute for Standards and Technology wird nun vier von 69 vorgeschlagenen Methoden der Post-Quanten-Kryptografie standardisieren.

Peter Schwabe hat drei der ausgewählten Verfahren maßgeblich mitentwickelt, zwei dienen der Authentifizierung, ein weiteres dem sicheren Austausch von kryptografischen Schlüsseln.

NIST sei Effizienz aber ein wichtiges Kriterium, damit sich die Verfahren auch gut für die breite Anwendung in der alltäglichen Internetnutzung eignen. „Es ist durchaus möglich, dass wir bei einer Aktualisierung der Richtlinien weitere Verfahren aufnehmen, auch solche, die jetzt vom NIST ausgewählt wurden“, so Ehlen. Das würde nicht zuletzt die sichere

Kommunikation von Bundesbehörden, die den BSI-Empfehlungen folgen, beispielsweise mit Unternehmen erleichtern, die den NIST-Standard anwenden. Für die digitalen Signaturen wird das BSI erst noch Verfahren auswählen. „Das war bislang nicht so dringlich, weil es da nicht das Problem gibt, dass verschlüsselte Kommunikation möglicherweise heute schon abgefangen und gespeichert, aber erst später entschlüsselt wird.“

Die Standardisierung könnte Ende 2023 abgeschlossen sein, vermutet der Informatiker. Doch schon jetzt nutzen zum Beispiel Google, Amazon und Cloudflare, ein Dienstleister für IT-Sicherheit, testweise Methoden der Post-Quanten-Kryptografie – gemeinsam mit den heutigen Standard-

verfahren, welche für Angriffe mit Quantencomputern verletzlich sind. Und auch Automobilhersteller beschäftigen sich bereits mit der Post-Quanten-Kryptografie, um sicherzustellen, dass sie die Software ihrer heute gebauten Fahrzeuge auch in fünfzehn oder zwanzig Jahren noch ohne großen Aufwand sicher aktualisieren können. „Wir gehen davon aus, dass nach der Standardisierung immer mehr Dienste die neuen Verfahren einsetzen werden“, erläutert Peter Schwabe. Dann werden die Verschlüsselungsmethoden, welche die Bochumer Forschenden mitentwickelt haben, den Besuch einer Webseite, den E-Mail-Verkehr oder Bankgeschäfte hoffentlich schon sichern, bevor es den ersten leistungsfähigen Quantencomputer gibt.




GLOSSAR




AUTHENTIFIZIERUNG
stellt in der Onlinekommunikation sicher, dass ein Computer oder Server auch der ist, der zu sein er vorgibt, also etwa der Server eines E-Mail-Dienstes.

POST-QUANTEN-KRYPTOGRAPHIE
bezeichnet Verschlüsselungsmethoden, die auch Quantencomputer nicht knacken können.

SCHLÜSSELAUSTAUSCH
ist ein kryptografisches Verfahren, das es zwei Parteien erlaubt, über einen unsicheren Kanal einen gemeinsamen geheimen Schlüssel auszutauschen.

STANDARDISIERUNG DURCH DAS NIST
umfasst Erläuterungen der Verschlüsselungsmethoden sowie Hinweise, wie die Verfahren sicher und möglichst einfach in Programme für digitale Dienste integriert werden können.

öffentlich  : (A, t) v = t  +  + m

geheim  : s u = A  + 

} Chiffretext

Entferne den öffentlichen Schlüssel

$$d = v - su = t \text{ (carrot)} + \text{apple} + m - s (A \text{ (carrot)} + \text{lemon})$$

$$d = \text{broccoli} \text{ (carrot)} + \text{apple} + m + s \text{ (lemon)} \quad (\text{weil: } A s + \text{broccoli} = t)$$

Entferne das Rauschen durch Runden

$$d = \underbrace{m}_{\text{groß}} + \underbrace{\text{broccoli (carrot)} + \text{apple} - s \text{ (lemon)}}_{\text{klein}}$$

Verschlüsselung als Buchstabensalat: Beim Schlüsselaustausch mit Crystals-Kyber erhält der Absender einer Nachricht vom Empfänger die öffentlichen Schlüssel A und t, mit denen er seine Nachricht m verschlüsselt. Nur mit dem geheimen Schlüssel s kann der Empfänger die Nachricht entschlüsseln. Die Icons stehen für kleine Werte, die die entscheidenden Komponenten leicht verzerren und die Entschlüsselung für Angreifer noch komplizierter machen. Sie werden im letzten Schritt entfernt, indem auf die Null oder Eins eines Bits gerundet wird.