Deutscher Bundestag
Ausschuss Digitale Agenda

Ausschussdrucksache
19(23)017

Freie Universität Berlin

Fachbereich
Mathematik und Informatik
ID Management

Freie Universität Berlin, Fachbereich Mathematik und Informatik
Takustr. 9, 14195 Berlin

Prof. Dr. Marian Margraf
Takustr. 9
14195 Berlin

Telefon +49 30 838 75-245
Fax +49 30 838 75-194
E-Mail marian.margraf@fu-berlin.de

Deutscher Bundestag
Ausschuss Digitale Agenda
11011 Berlin

per E-Mail an: ada@bundestag.de

Berlin, 05.06.2018

Betr.: Fragenkatalog zur öffentlichen Anhörung „Quantencomputer“ des Ausschusses Digitale Agenda, 6. Juni 2018

Meine Antworten beziehen sich lediglich auf die sicherheitsrelevanten Fragen, d.h. die Folgen auf die IT-Sicherheit, die durch die Existenz von Quantencomputern entstehen.

Frage 1: Wie ist der Stand von Forschung und Technik auf dem Gebiet des Quantencomputing?

Nach meiner Kenntnis gab es gerade in den letzten zwei bis drei Jahren erhebliche Fortschritte auf dem Gebiet der Quantencomputer. So hat die Firma Google aktuell einen Quantencomputer mit 72 Qbits entwickelt.

Frage 12: Welche Forschungsstrategie sollte Deutschland bzw. Europa entwickeln, um international anschlussfähig zu bleiben?

Hinsichtlich IT-Sicherheit sollten aktuell Forschungen im Bereich quantencomputerresistenter kryptographischer Verfahren massiv gefördert werden, siehe auch Antworten zu Frage 14.

Frage 14: Ab wann werden heute angewendete Verschlüsselungsalgorithmen und Instrumente aus dem Bereich der IT-Sicherheit (z.B. Verschlüsselungstechnologien, Blockchain-Technologien) voraussichtlich unsicher? Bitte schlüsseln Sie die angenommenen zeitlichen Horizonte für möglichst viele Verschlüsselungsalgorithmen und Instrumente einzeln auf. Warum werden die benannten Verschlüsselungsalgorithmen und Instrumente unsicher? Wie kann sichergestellt werden, dass wir rechtzeitig darauf vorbereitet sind?

Quantencomputer haben erhebliche Auswirkungen auf die Sicherheit heute eingesetzter kryptographischer Verfahren. Bei symmetrischen Verschlüsselungsverfahren (wie z.B. AES) reduziert sich die Schlüsselsuche durch einen von Grover 1996 entwickelten Suchalgorithmus, die Sicherheit kann aber durch die Verdoppelung der Schlüssellänge wieder auf das ursprüng-

liche Niveau gehoben werden. Ähnliche Auswirkungen ergeben sich bei Hashfunktionen (Sha256 usw.). Auch hier kann aber durch die Vergrößerung des Bildbereichs das notwendige Sicherheitsniveau wieder erreicht werden. Darüber hinaus werden hierfür Quantencomputer benötigt, die eine sehr große Anzahl von Qbits benötigen.

Viel stärker wirken sich Quantencomputer aber auf aktuell genutzte Public-Key-Verfahren aus. Ein von Shor 1994 entwickelter Algorithmus bricht sehr effizient kryptographische Verfahren, die auf dem Faktorisierungsproblem basieren (z.B. RSA-Verschlüsselung und RSA-Signatur). Mit einer ähnlichen Idee lassen sich auch Verfahren brechen, die auf dem Problem der Berechnung Diskreter Logarithmen basieren (z.B. Signaturverfahren DSA, Verschlüsselungsverfahren Elgamal oder Schlüsseleinigungsverfahren Diffie-Hellman). Eine Anpassung der Schlüssellänge wie bei symmetrischen Verfahren ist hier nicht möglich. Diese müssten soweit erhöht werden, dass z.B. die Schlüsselgenerierung nicht mehr effizient durchführbar ist. Im Gegensatz zu den Folgen auf symmetrische Verfahren genügen hier schon Quantencomputer mit deutlich weniger Qbits.

Damit werden nahezu alle der heute eingesetzten Public-Key-Verfahren (Signatur-, Schlüsselaustausch- und Verschlüsselungsverfahren) unsicher. Da die in symmetrischen Verfahren genutzten kryptographischen Schlüssel auf Basis der oben aufgeführten Public-Key-Verfahren vereinbart werden (authentisierte Schlüsselaustauschverfahren), ist auch die symmetrische Verschlüsselung betroffen. Angreifer können mit Hilfe von Quantencomputern die Sicherheit von Schlüsselaustauschverfahren aushebeln und so die kryptographischen Schlüssel extrahieren oder Man-in-the-Middle-Angriffe durchführen. Dies betrifft alle aktuell verwendeten kryptographisch abgesicherten Internetverbindungen (z.B. über https oder Virtual Private Network (VPN)).

Die meisten Experten gehen davon aus, dass spätestens ab 2030 Quantencomputer existieren, die die heute eingesetzten Verfahren brechen. Gerade für Dokumente, für die die Vertraulichkeit über mehrere Jahre garantiert werden muss, besteht damit aber schon heute Handlungsbedarf. Seit Snowden wissen wir, dass die amerikanischen Geheimdienste große Mengen an Internetkommunikation für eine spätere Auswertung speichern. Damit lassen sich die heute verwendeten Schlüsselaustauschverfahren später mittels Quantencomputer brechen und die darauf aufgebaute sichere Verbindung mitlesen.

Frage 15: Was wird für die Weiterentwicklung von Quantenkryptografie benötigt? Wie können alle notwendigen Fachgebiete in der Wissenschaft bei der Weiterentwicklung von Quantenkryptografie eingebunden werden? Wie können die Entwicklungen der Quantenkryptografie breit zugänglich gemacht werden in Industrie, Ausbildung und für die End User? Wie kann Quantentechnologie auch kleinen Start-ups oder Einzelpersonen zugäng-

lich gemacht werden, um Anwendungen zu entwickeln? Gibt es mögliche Implikationen für den Datenschutz, wenn Quantenkryptografie weit verbreitet ist?

Quantenkryptographie sollte nicht mit quantencomputerresistenten kryptographischen Verfahren oder Quantencomputer allgemein verwechselt werden. Zur Umsetzung von Quantenkryptographie (Umsetzung sicherer Schlüsselaustausch, der auf quantenmechanischen Effekten basiert) werden keine Quantencomputer benötigt.