Deutscher Bundestag **Drucksache 19/4845**

19. Wahlperiode 10.10.2018

Antrag

der Abgeordneten Mario Brandenburg (Südpfalz), Katja Suding, Nicola Beer, Dr. Jens Brandenburg (Rhein-Neckar), Britta Katharina Dassler, Dr. h. c. Thomas Sattelberger, Grigorios Aggelidis, Nicole Bauer, Jens Beeck, Bijan Djir-Sarai, Dr. Marcus Faber, Daniel Föst, Otto Fricke, Markus Herbrand, Torsten Herbst, Katja Hessel, Manuel Höferlin, Reinhard Houben, Olaf in der Beek, Dr. Christian Jung, Dr. Marcel Klinge, Daniela Kluckert, Carina Konrad, Ulrich Lechte, Till Mansmann, Frank Müller-Rosentritt, Hagen Reinhold, Christian Sauter, Jimmy Schulz, Matthias Seestern-Pauly, Frank Sitta, Bettina Stark-Watzinger, Benjamin Strasser, Stephan Thomae und der Fraktion der FDP

Sichere Kryptographieverfahren für Quantencomputer entwickeln

Der Bundestag wolle beschließen:

I. Der Deutsche Bundestag stellt fest:

Quantencomputer ebnen den Weg zum nächsten Level im High-Performance-Computing. Sie können komplexe Berechnungen mit Quanteneffekten durchführen. Übliche Rechner arbeiten mit algorithmischen Verfahren auf Bits, den kleinstmöglichen Unterscheidungseinheiten. Als Bit haben sie den Wert eins oder null. In einem Entweder-Oder-System kann man keinen zwei Wegen gleichzeitig folgen. An einer Verzweigung geht ein herkömmlicher Rechner nach links oder nach rechts. Um beide Wege zu gehen, geht er zuerst nach links und dann nach rechts. Optimierungsprobleme (Probleme bei der Optimierung von linearen Zielfunktionen) führen bei komplexen Aufgaben zu Verzweigungen mit Millionen Richtungen. Selbst der schnellste Supercomputer würde ewig benötigen, jeden einzelnen Weg nacheinander zu berechnen. Die kleinsten Unterscheidungseinheiten eines Quantencomputers, ein Qubit, können einen Überlagerungszustand annehmen und dadurch zugleich eins und null sein. Es befindet sich in einem Sowohl-als-auch-System. Dadurch können viele Lösungswege in Überlagerung berechnet werden. Die verschiedenen Rechenwege können sich verstärken oder gegenseitig aufheben. Zum Abschluss der Berechnung wird dann ein Ergebnis gemessen, das auf klassischem Wege selbst mit stärksten Supercomputern nicht erreichbar gewesen wäre.

Experten gehen davon aus, dass im Jahr 2030 der erste Quantencomputer mit einer Datenverarbeitung von 72 Qubits entwickelt wird (www.faz.net/aktuell/wirtschaft/diginomics/google-stellt-neuen-quantencomputer-namens-bristlecone-vor-15480332.html). Obwohl das von den genaueren Eigenschaften der Qubit-Hardware abhängt, ist das die Größe, bei der ein Quantencomputer nicht mehr durch die schnellsten Supercomputer simuliert werden kann. Anwendungsfelder sind in der Physik, der

Chemie, der Biologie und Medizin zu finden. Es gibt einige Beispiele mit immenser potentieller Bedeutung für die Menschheit: Medikamentenentwicklung, z. B. über die Simulation von Proteinfaltungen, die Entwicklung neuer Materialien wie Hochtemperatursupraleiter, die Strom verlustfrei über große Distanzen leiten können oder effizientere Syntheseverfahren in der Chemie, beispielsweise für die energiesparende Synthese von Stickstoffdünger, der für die Ernährung der Weltbevölkerung benötigt wird. Außerdem könnten Quantencomputer das momentan häufig angesprochene Machine Learning in vielen Bereichen revolutionieren.

Theoretische Arbeiten aber lassen erwarten, dass zukünftige Quantencomputer die Sicherheit derzeit verwendeter Verfahren für Schlüsselaustausch, asymmetrische Verschlüsselungen und Signaturen gefährden. Derzeit sicher verschlüsselte Nachrichten könnten von Angreifern zwischengespeichert und dann mit zukünftigen Quantencomputern nachträglich entschlüsselt werden. Die Nachricht wäre also nicht dauerhaft geheim. Wir benötigen deshalb einen langfristigen Schutz von Daten – zum Beispiel durch Quantenkryptographie zum Austausch von Schlüsseln oder durch sogenannte Post-Quanten-Kryptographie –, damit die Sicherheit gewährleistet ist, selbst wenn der Angreifer über einen Quantencomputer verfügt.

Deutschland könnte mit den richtigen Weichenstellungen ein erfolgreicher Entwicklungsstandort sein und ein Alleinstellungsmerkmal im Bereich Sicherheit und Verschlüsselung erreichen. Deutschland muss die Entwicklung und Anwendung von Verschlüsselungstechnologien intensivieren, damit wir nicht nur Marktführer, sondern auch technologischer Vorreiter werden.

II. Der Deutsche Bundestag fordert die Bundesregierung auf,

1. zusammen mit nationalen Unternehmen die Entwicklung einer anerkannten Software zu unterstützen, die die Datensicherheit in Form einer auch gegen Angriffe mit Quantencomputern sicheren Verschlüsselung gewährleistet und das Qualitätssiegel „Made in Germany“ trägt;
2. die neu gegründete Cyber-Agentur (www.spiegel.de/netzwelt/netzpolitik/agentur-fuer-innovationen-in-der-cybersicherheit-deutsche-darpa-soll-it-sicherheit-staerken-a-1225548.html) in Zusammenarbeit mit den drei Kompetenzzentren zur IT-Sicherheitsforschung – CISPA, CRISP und KASTEL – damit zu beauftragen, Regeln und Standards zu setzen, die die öffentliche Infrastruktur sowie Unternehmen umsetzen sollten, so dass die Sicherheit der Datenkommunikation auch bei Existenz von Quantencomputern sichergestellt ist;
3. die eigene IT-Infrastruktur quantencomputerresistent zu machen, und so mit gutem Beispiel voranzugehen;
4. einen Evaluationsbericht des Rahmenprogrammes „Quantentechnologien – von den Grundlagen zum Markt“ im Jahr 2023 vorzulegen, der den Erfolg des Programmes misst;
5. bei den Ländern und Hochschulen anzuregen beziehungsweise dafür zu werben, die vorhandenen Studiengänge im Bereich der Datenwissenschaften (Data Sciences) an der Entwicklung von Quantencomputern (z. B. durch eigene Module Quantentechnologie bzw. Quantenphysik) anzupassen;
6. optimale Bedingungen für Absolventinnen und Absolventen im Bereich Datenwissenschaften (Data Sciences) und Quantenphysik zu schaffen, damit diese sich im Forschungsumfeld Deutschlands betätigen und ihre Expertise nicht verloren geht;
7. anstelle der Diversifizierung in der Forschungsarbeit eine Konzentrierung der Expertise z. B. durch sogenannte Wissenschaftsleistungszentren zu erleichtern;

8. Forscherinnen und Forschern den Weg zu ebnen, mit führenden Softwareunternehmen schneller in Kontakt zu treten und den Austausch zu fördern;
9. den Transfer von der Grundlagenforschung in die Anwendung durch gezieltere Projekte unter Einbeziehung kleinerer und mittlerer Unternehmen (KMU) zu optimieren;
10. den Zugang zur Patentanmeldung für Grundlagenforscher und -forscherinnen sowie kleinere und mittlere Unternehmen (KMU) durch reduzierte, digitalisierte Prozesse zu erleichtern und zu fördern, um damit die Nachfrage am Markt für quantenbasierte Anwendungen zu erhöhen;
11. die europäische Forschungsstruktur im Bereich Quantencomputing und Quantenkryptographie weiter zu verbessern, mindestens die Flagship-Projects der EU (die EU fördert Projekte dazu über einen Zeitraum von zehn Jahren mit 1 Mrd. Euro) konstruktiv zu unterstützen, die in Grundlagen und Anwendung gegen andere internationale Player standhält und den aktuellen „brain/drain“ reduziert oder sogar verhindert;
12. gemeinsam mit den internationalen Playern Open-Access-Areas aufzubauen, die von deutschen sowie europäischen Forscherinnen und Forschern benutzt werden können, und die den Zugang zu anwendungsorientierten Bereichen erleichtern;
13. sogenannte „Regulatory Sandboxes“ für Forscherinnen und Forscher einzurichten, damit diese kontrolliert, aber ohne Regulierung, ihre Ergebnisse testen können;
14. im Allgemeinen aber auch im Rahmen des Forschungsprogrammes zur IT-Sicherheit „Selbstbestimmt und sicher in der digitalen Welt 2015-2020“ Projekte und KMU zu fördern, die sich mit der Entwicklung quantencomputerresistenter Verschlüsselungstechnologien beschäftigen;
15. neue nationale und europäische Initiativen zur Förderung von Quantentechnologien ins Leben zu rufen und bestehende weiter zu fördern, um die mit diesen Technologien verbundenen wirtschaftlichen und gesellschaftlichen Chancen zu nutzen. Hierbei muss auf geeignete Partnerschaften zwischen Unternehmen und Grundlagenforschern geachtet werden.

Berlin, den 9. Oktober 2018

Christian Lindner und Fraktion

Satz: Satzweiss.com Print, Web, Software GmbH, Mainzer Straße 116, 66121 Saarbrücken, www.satzweiss.com
Druck: Printsystem GmbH, Schafwäsche 1-3, 71296 Heimsheim, www.printsystem.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333