Wann, *wenn nicht jetzt?*

INTERVIEW Alexandra Resch

*Quantencomputer kommen. So viel steht fest. Doch wann sie tatsächlich leistungsfähig genug sind, um in Industrie und Kryptografie großflächig zum Einsatz zu kommen, ist eine Frage, auf die sich viele Wissenschaftler*innen nicht festlegen wollen. Trotzdem arbeiten Forschende und Unternehmen bereits jetzt an Anwendungsmöglichkeiten sowie an Wegen, um sensible Daten vor der erwarteten Rechenpower zu schützen. Ein Gespräch mit Juliane Krämer, Expertin für Post-Quanten-Kryptografie, und Stefan Seegerer, Education Lead bei einem der führenden Hersteller von Quantencomputern.*

Frau Krämer, man könnte meinen, Sie arbeiten an Lösungen für ein Problem, das es noch gar nicht gibt. Sehen Sie das ähnlich?

JULIANE KRÄMER Jein. Es stimmt, dass die bisher existierenden Quantencomputer noch keine Bedrohung für die aktuell verwendete Kryptografie sind. Aber: Obwohl es diese großen Rechner noch nicht gibt, weiß man schon heute, was sie können werden. Wir müssen hier zwischen zwei kryptografischen Funktionen unterscheiden: Verschlüsselungsverfahren und digitale Signaturen. Letztere sind in der IT-Landschaft weit verbreitet und kommen etwa zum Einsatz, wenn unser PC ein neues Software-Update eingespielt bekommt. Sie müssen aber nur einmal überprüft werden. Bei Verschlüsselung ist das anders. Angreifer, die ein langfristiges Interesse an gewissen Daten haben, können diese theoretisch jetzt schon abgreifen, speichern und sie dann in der Zukunft sehr einfach entschlüsseln. Daher ist die post-quantensichere Verschlüsselung von besonders sensiblen Daten, die langfristig sicher sein sollen, schon jetzt anzuraten.

Und wenn wir von Angreifern sprechen …

JK … sind das voraussichtlich erst einmal eher Regierungen und Geheimdienste.

Sie könnten also für Spionage genutzt werden. Hemmt diese Gefahr die Entwicklung? Halten Hersteller sich zurück, wenn sie große Fortschritte machen?

JK Den Eindruck habe ich nicht. Es gibt zwar einerseits diese Bedrohung für die Kryptografie, aber Quantencomputing hat ja auch viele Potenziale, der wirtschaftliche Faktor ist enorm hoch. Auf mich wirkt es eher so, als ob Unternehmen in ihren Pressemitteilungen oft mehr Leistung verkünden, als die entwickelten Rechner tatsächlich schon leisten können.

STEFAN SEEGERER Bei IQM orientieren wir uns da schon an unseren wissenschaftlichen Ergebnissen, aber es gibt durchaus Firmen, die manchmal doch etwas mehr versprechen, als aktuell vielleicht bereits möglich ist. Das ist aber auch eine Frage der Zielgruppe: Viele dieser Texte sollen vor allem Menschen an der Börse für das Unternehmen und seine Produkte begeistern. Was Hemmnisse angeht, gibt es einige Länder, die bereits Exportbeschränkungen für Quantentechnologien beschlossen haben oder sie zumindest in Betracht ziehen.

Wie steht Deutschland da, was das Thema Quantencomputing angeht?

StS Eigentlich sehr gut. Es gibt viele starke Standorte in der Forschung. Auch aufseiten der Endanwender setzen sich viele Firmen bereits heute mit dem Thema auseinander und bauen zumindest schon einmal kleine Teams auf. Das ist nicht in jedem Land gegeben, glaube ich.

JK Das sehe ich auch so. Es gibt eine große Offenheit vonseiten der Unternehmen in Deutschland, gerade

auch in dem Bereich Post-Quanten-Kryptografie, weil es hier noch nicht so viele Fachkräfte gibt und wenig Expertise auf dem Arbeitsmarkt verfügbar ist. Unternehmen sind oft auf gemeinsame Forschungsprojekte mit wissenschaftlichen Einrichtungen angewiesen, um an dieses Know-how zu kommen.

Herr Seegerer, wie nehmen Sie den Arbeitsmarkt in diesem Feld wahr?

StS Es gibt viele Firmen in diesem Bereich, die stark wachsen. Das führt natürlich auch zu einem Kampf um Talente. Gerade im Bereich der Quantentechnologie braucht es zudem oft eine sehr interdisziplinäre Aufstellung: Da sind zum einen jene, die sich mit Materialien und Hardware befassen, zum anderen Mitarbeitende mit der theoretischen, algorithmischen Expertise und wieder andere, die die experimentellen Messungen im Labor durchführen. Das ist eine sehr große Bandbreite und öffnet somit Türen für Menschen mit unterschiedlichen Hintergründen und Lebensläufen.

Gibt es viel internationalen Austausch in Forschung und Wirtschaft?

StS Mich überrascht immer wieder, wie viel Austausch es auch zwischen Unternehmen gibt. Wir haben gerade eine Konferenz organisiert, bei der sich eine Vielzahl an Firmen aus dem Feld beteiligt hat. Das finde ich toll! Und klar ist: Allein ist so ein großes Vorhaben nicht zu schaffen. Jedes Rädchen spielt eine wichtige Rolle, wenn man mit so stark heruntergekühlten Geräten und Chips arbeitet. Wenn da eine Komponente nicht gut genug abgeschirmt ist, kann das fatale Folgen haben. Es braucht also viele smarte Köpfe.

JK In der Forschung zur Post-Quanten-Kryptografie wird sehr viel über Ländergrenzen hinweg zusammengearbeitet. Das sieht man an den Verfahren, die sich im aktuellen Standardisierungsprozess durchsetzen. Da stehen bis zu zehn Namen dahinter, immer aus unterschiedlichen Ländern.

> **„In der Forschung zur Post-Quanten-Kryptografie wird sehr viel über Ländergrenzen hinweg gearbeitet. Das sieht man auch an den Verfahren, die sich im aktuellen Standardisierungsprozess durchsetzen."**
>
> JULIANE KRÄMER

Wie läuft dieser Standardisierungsprozess ab?

JK Tatsächlich beschäftigt die Frage nach Standards die Forschung schon seit einigen Jahren. Ganz entscheidend ist dabei eine US-Behörde, das National Institute of Standards and Technology, kurz NIST. Das Institut hat bereits 2016 einen Prozess gestartet, in dem quantensichere Verschlüsselungs- und Signaturverfahren eingereicht werden konnten. Diese wurden dann nicht nur vom NIST selbst, sondern von der internationalen Forschungsgemeinschaft evaluiert. Heißt: Forschende weltweit haben versucht, diese Verschlüsselungen zu brechen. Kürzlich wurden erste Verfahren als Standards festgelegt, darunter auch zwei, an denen die Ruhr-Universität Bochum beteiligt war. Standards werden dazu führen, dass Post-Quanten-Kryptografie nun viel breiter eingesetzt wird. Da es nicht so einfach ist, solche Verfahren im Nachhinein wieder auszutauschen – und die Bedrohung auch noch nicht so akut ist, haben viele Unternehmen auf diese Standards gewartet.

Kommen wir zur unbeliebten Frage: Wann gelingt Ihrer Meinung nach der Sprung von der Theorie zur Praxis, also zu industriell und kryptografisch relevanten Quantencomputern?

JK Es gibt diesen Witz: Quantenphysiker sagen, dass es in zehn Jahren große leistungsfähige Quantencomputer geben wird – und das sagen sie schon seit 20 Jahren. Aus meiner Sicht gibt es schon noch sehr große physikalische Aufgaben

Juliane Krämer und Stefan Seegerer sind sich einig: Sowohl in der Forschung als auch in der Praxis gibt es viel internationalen Austausch, was Quantentechnologie angeht.

> ***„Klar ist: So ein Vorhaben ist allein nicht zu schaffen. Jedes Rädchen spielt eine wichtige Rolle, wenn man mit so stark heruntergekühlten Geräten und Chips arbeitet."***
>
> STEFAN SEEGERER

zu lösen. Ich rechne nicht damit, dass das in fünf Jahren geschieht. Ob jetzt 20 oder 50 Jahre, das kann kaum jemand abschätzen.

StS Ohne Glaskugel will ich mich da auch ungern zu einem Statement hinreißen lassen. Letztlich können wir wissenschaftliche Durchbrüche nicht vorhersagen. Ich verweise immer auf die Roadmaps vieler Hersteller, die sich alle in diesem Jahrzehnt bewegen, was die ersten nützlichen Anwendungen angeht. Wie jede andere Firma haben wir bei IQM Pläne, was wir wann an Hardwareleistung bieten wollen, aber auf der anderen Seite muss man ja auch die Algorithmen weiterentwickeln und neue erarbeiten. Was ich noch spannend finde: Wenn man theoretische Fortschritte im Bereich des Quantencomputing bei bestimmten Anwendungen erzielt, spornt man damit auch Leute an, die an klassischen Lösungen arbeiten.

Als Education Lead leisten Sie viel Aufklärungsarbeit. Gibt es da Missverständnisse, die Ihnen häufiger begegnen?

StS Was Leute immer wieder überrascht: Bezogen auf die Anzahl der Operationen pro Zeiteinheit arbeitet ein Quantencomputer im Megahertz-Bereich. Jedes Handy hingegen hat heute ein paar Gigahertz als Prozessortakt. Dass diese Technologie so bahnbrechend sein wird, liegt also nicht an ihrer Schnelligkeit, sondern daran, dass sich ganz andere Rechenmöglichkeiten ergeben, um ein Problem zu lösen: andere, nicht schnellere.

- **Prof. Dr. Juliane Krämer** ist Professorin für Datensicherheit und Kryptografie an der Universität Regensburg. Sie forscht dort zu Post-Quanten-Kryptografie mit Fokus auf physikalische Angriffe. Sie ist Mitglied des Leitungsgremiums der GI-Fachgruppe KRYPTO und wurde 2016 als Junior-Fellow der GI ausgezeichnet.

- **Dr. Stefan Seegerer** arbeitet bei IQM Quantum Computers als Education Lead. Er beschäftigt sich intensiv damit, Informatiksysteme zugänglicher zu machen, informatische Konzepte und Ideen zu vermitteln und Werkzeuge und Systeme zu entwickeln, die das Lernen, Denken und Arbeiten erleichtern. Für seine Beiträge zur informatischen Bildung wurde er 2022 mit dem Helmut und Heide Balzert Preis ausgezeichnet.