Er möchte den Computer der nächsten Generation bauen

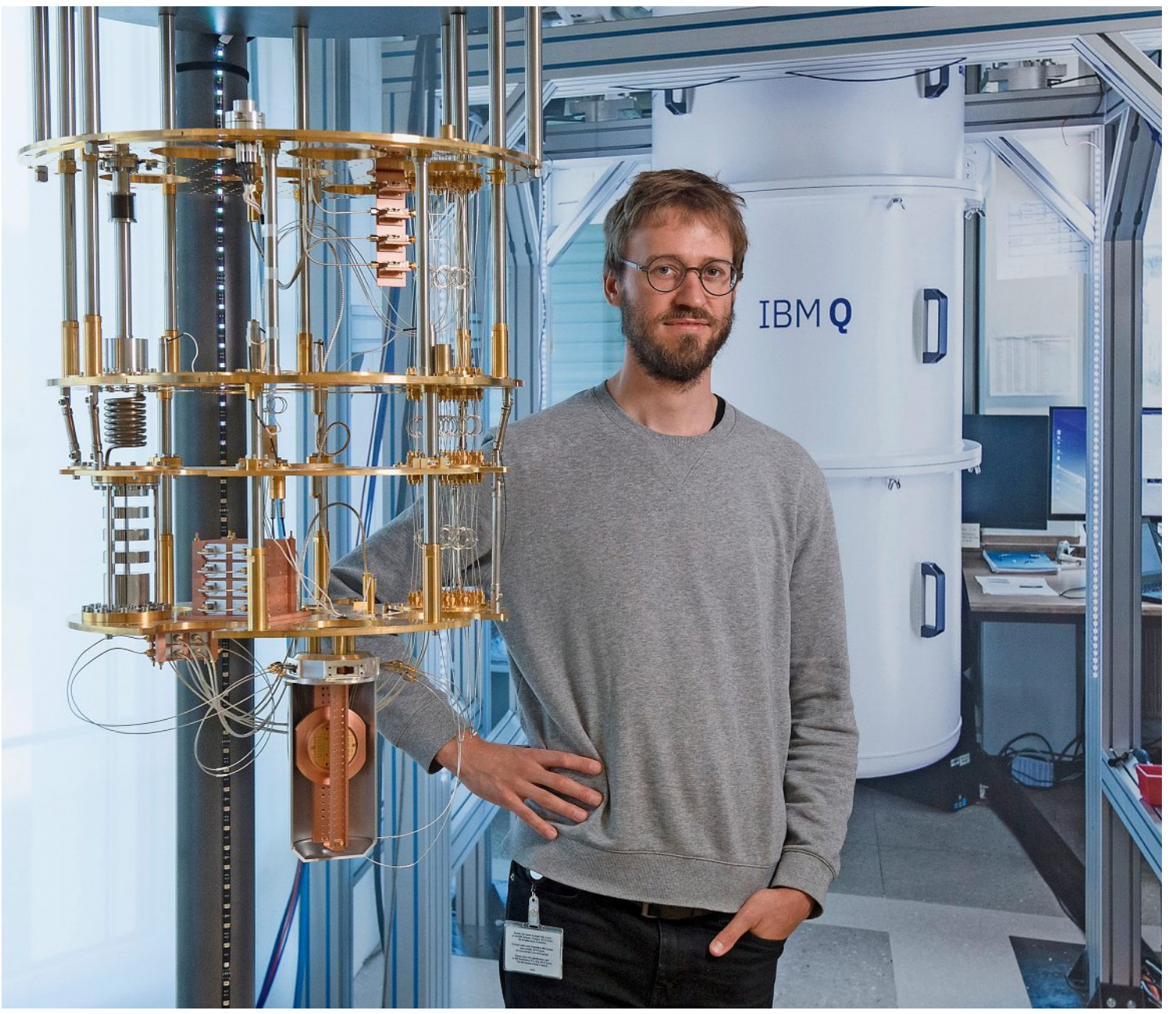
Quantencomputer Weltweit wird am «Next Big Thing» geforscht, auch am IBM Research Zurich in Rüschlikon. IBM-Verschlüsselungsexperte Gregor Seiler spricht von einer Revolution – im industriellen Bereich.

Thomas Schär

Forscher in aller Welt – darunter auch am Forschungslabor von IBM in Rüschlikon – arbeiten intensiv daran, Computer einer ganz neuen Generation zu bauen, die die Möglichkeiten der Quantenphysik nutzen. In der Theorie ist klar, dass diese sogenannten Quantencomputer gewisse Probleme erheblich schneller oder überhaupt erst lösen können, an denen heutige Computer scheitern.

Spezielle, quantenmechanische Eigenschaften erlauben es Quantencomputern, parallele Rechnungen durchzuführen statt nur einer wie bei klassischen Computern. Damit werden heutzutage noch extrem rechenaufwendige Verfahren wie die Primzahlzerlegung grosser Zahlen deutlich schneller gelöst, sodass die heute verwendeten Verschlüsselungstechniken unbrauchbar werden.

Gregor Seiler, wann kommt der Quantencomputer?
Wenn wir das wüssten, wäre das natürlich schön. Es ist noch sehr viel Forschung nötig. Klar, es kann in sehr kurzer Zeit einen Durchbruch geben, wenn jemand eine bahnbrechende Idee hat. Genauso gut kann es jedoch Probleme geben, die sich als sehr schwierig zu lösen herausstellen. Wahrscheinlich wird es noch mehr als zehn Jahre dauern. Ich rechne mit einem Zeitraum von acht bis zwanzig Jahren.



IBM-Forscher Gregor Seiler neben dem Modell eines Quantencomputers: «Es ist noch sehr viel Forschung nötig.» Foto: Michael Trost

Werden Quantencomputer den PC-Markt revolutionieren?
Bei ganz bestimmten Anwendungen sicher. Aber die Quantencomputer werden die klassischen Computer, die heute im Einsatz sind, nicht verdrängen. Es gibt ganz konkrete Anwendungen, für die Quantencomputer viel besser sind, etwa in der chemischen Forschung, um Moleküle zu simulieren. Quantencomputer können schwierige mathematische Problemstellungen lösen. Sie sind aber nicht geeignet für sehr grosse Datenmengen. Für unwahrscheinlich halte ich auf lange Sicht, dass sie im privaten Bereich zum Einsatz kommen. Die ersten Quantencomputer werden auf grossen Maschinen laufen, im industriellen und im Forschungsbereich. Interessierte Firmen werden sie aber nicht einmal kaufen müssen, sondern in der Cloud darauf zugreifen können.

Quantencomputer sollen in der Lage sein, heutige Sicherheitsmechanismen und Verschlüsselungstechniken relativ einfach zu knacken: Ist es nicht widersinnig, einen neuen Computer zu entwickeln, der es potenziellen Angreifern einfacher macht, auf IT-Systeme zuzugreifen und sie unter ihre Kontrolle zu bringen?
Das glaube ich nicht. Die Gefahr, die von den Verschlüsselungen ausgeht, ist eher ein Nebenprodukt. Das fundamentale Problem im Bereich der IT-Sicherheit ist, dass wir heute Daten verschlüsseln, von denen wir wollen, dass sie auf sehr lange Sicht sicher verschlüsselt sind, speziell auf staatlicher Ebene, etwa bei Gesundheitsdaten. Für unser Risikomanagement ist es wichtig, zumindest die Möglichkeit in Betracht zu ziehen, dass es in der Zukunft Computer geben wird, die die heutigen Verschlüsselungstechniken brechen können.

> **«Wir müssen schon heute auf Verfahren umstellen, die auch noch in 20 Jahren sicher sind.»**
>
> **Gregor Seiler**
> Forscher IBM Research Zurich, Rüschlikon

Was bedeutet das für die Industrie?
Wir müssen schon heute auf Verfahren umstellen, die auch in 20 Jahren noch sicher sind. Wir können nicht einfach abwarten, bis die ersten Quantencomputer im Einsatz sind. Wir müssen jetzt etwas dagegen unternehmen.

Droht also den IT-Sicherheitsfirmen die Zeit davonzulaufen, in der sie ihre Produkte noch zukunftssicher machen können für das Zeitalter der Quantencomputer?
Die Versuchung ist tatsächlich gross, bei dem langen Zeitraum, bis die Quantencomputer auf den Markt kommen, zu sagen, wir können uns noch Zeit lassen. Je nachdem, an welche Prognose man glaubt, ist es für einige heutige Verschlüsselungen aber schon fast zu spät.

Welchen Beitrag leistet das Forschungslabor IBM Research Zurich in Rüschlikon zu dieser neuen Technologie?
Derzeit läuft in den USA beim National Institute of Standards and Technology (Nist) ein Standardisierungsverfahren für quantensichere Algorithmen. Diese Algorithmen sind gegenüber durch Quantencomputer verursachte mögliche Sicherheitsprobleme immun. Insgesamt wurden gegen 80 Verfahren eingereicht, von denen das Nist in einer ersten Runde 69 akzeptierte. Am Wettbewerb nimmt auch IBM in Rüschlikon mit drei selber entwickelten Algorithmen teil. Unser Team am Zürichsee besteht aus zwei Personen, aber natürlich arbeiten wir mit Kooperationspartnern, bestehend aus Universitäten und industriellen Partnern, zusammen. Mittlerweile läuft die zweite von drei Runden, und wir sind noch dabei. Sicher ist, dass die Handvoll Verfahren, die am Ende ausgewählt werden, auch die sind, die dann im Markt breit eingesetzt werden.

Welches sind Ihre Mitbewerber?
Grosse Namen wie Google oder Microsoft, aber auch ein kalifornisches Start-up namens Rigetti Computing.

Wo steht IBM im Rennen um den ersten Quantencomputer?
Wir können nur für uns selbst sprechen. Und da hat IBM eben erst eine Kooperation mit der deutschen Bundesregierung beschlossen, um einen IBM-Quantencomputer nach Deutschland zu bringen. Insgesamt will Deutschland über die nächsten zwei Jahre 650 Millionen Euro in die Quantentechnologie investieren. In dem Projekt, das IBM betrifft, wollen wir einen sogenannten Hub aufbauen, in dem Wissenschaftler, Forscher, IT-Spezialisten und Industrieexperten an dieser Zukunftstechnologie arbeiten. Dazu wird nächstes Jahr in einem IBM-Datencenter in Deutschland ein Exemplar des ersten kommerziellen Quantencomputers in Betrieb gehen, den IBM im Februar an der CES 2019 in Las Vegas vorgestellt hat.

Zur Person

Gregor Seiler ist seit 2017 als Doktorand am IBM Research Zurich in Rüschlikon tätig und insbesondere direkt an der Entwicklung der quantensicheren Algorithmen beteiligt. Der 33-Jährige hat in Berlin und an der ETH Zürich Mathematik studiert. *(red)*

Erst verschlüsseln – dann erpressen

Der IT-Sicherheitsexperte Ivan Bütler teilt die Hacker, die feindliche Angriffe auf Firmen und deren Netzwerke starten, in vier Bereiche ein: einerseits die spielverliebten Hacker, die sich einen Spass daraus machen, eine Website zu verunstalten und ihre Trophäe auf ein Hacker-Portal hochzuladen. Die zweite Gruppe ist wesentlich gefährlicher. Sie interessiert sich für Geld und hat Bereicherungsabsichten. Sind die Daten nur für den Besitzer wertvoll, so werden diese verschlüsselt, danach beginnt die Erpressung.

Auch bei den beiden kürzlich von einer Hackerattacke betroffenen Firmen in der Region – Crealogix in Zürich/Bubikon und Meier Tobler in Schwerzenbach/Nebikon LU – wurde eine sogenannte Ransomware installiert, also ein Schadprogramm, das den Computer sperrt und darauf befindliche Daten verschlüsselt. Die dritte Gruppe hackt aus moralischen Motiven. Die vierte Gruppe umfasst die Aktivitäten von «staatlichen» Akteuren. In die Systeme von Staaten und Regierungen einzubrechen, bezeichnet Bütler als die gefährlichste Art und in puncto Schutz als die schwierigste.

Am besten geschützt ist laut Bütler die Finanz- und Versicherungsbranche. Die anderen Branchen hinkten hinterher. Es brauche einen Digitalen Experten in der Geschäftsleitung von Unternehmen, betont der Gründer der Compass Security AG in Rapperswil-Jona. Die IT-Sicherheitsfirma greift Computer an, um Sicherheitslücken aufzudecken. Auftraggeber sind Firmen, die sich um ihre Daten sorgen. Die Zahl der Cyberattacken hat nach Angaben von Bütler deutlich zugenommen.

Compass Security habe vor zwei Jahren einen 24-Stunden-Notfall-Service eingeführt, nachdem die Finanzaufsichtsbehörde (Finma) allen Schweizer Banken vorgeschrieben habe, rund um die Uhr auf Cyber-Ereignisse reagieren zu können: «Wir haben ständig mehr und mehr Anfragen von Unternehmen, die gehackt wurden.» Was das Thema der öffentlichen Sicherheit – Stichwort Stromnetz – betrifft, so gibt Bütler Entwarnung. Er habe schon ein paar Energieversorger auf ihre Sicherheit untersucht und dabei festgestellt, dass diese die Gefahren kennten und sich ihrer Verantwortung bewusst seien. *(ths)*