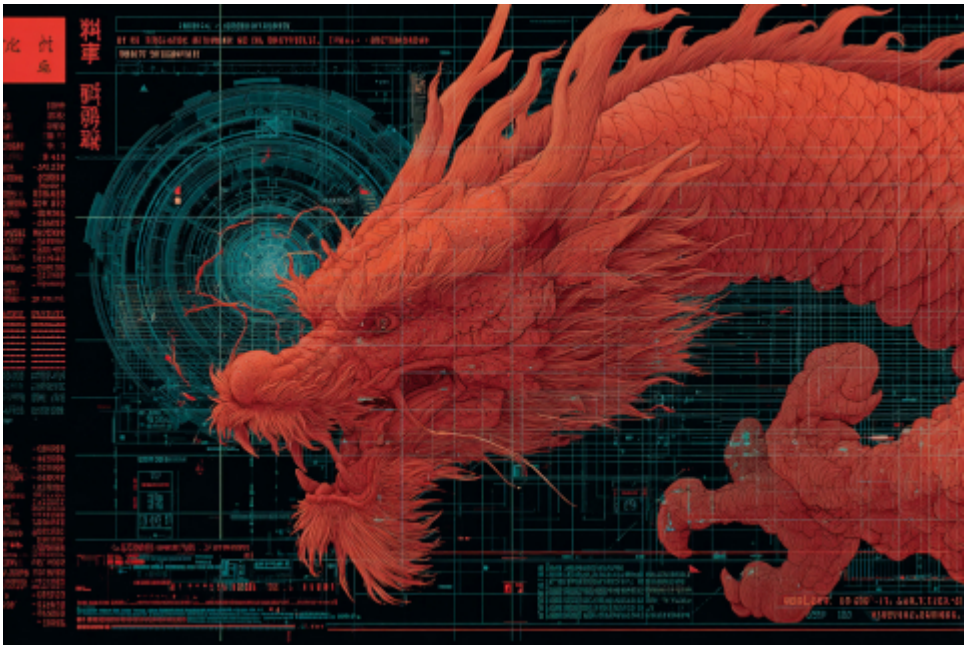
RSA-Verschlüsselung mit Quantencomputern



Interessante Aufgabe für die KI, das Thema zu bebildern. Ich habe eine Weile herumgepromptet, bis mir die Ergebnisse gefielen. Zum Schluss ließ ich noch das Original verändern.

Here's a suitable English prompt for generating a symbolic image representing "China Breaks RSA Encryption Using Quantum Computer":: An artistic, symbolic illustration showing China represented by a red dragon. In the background, a glowing quantum computer with floating qubits and digital circuits. The scene combines cyberpunk and futuristic elements, with a dark, high-tech atmosphere, symbolizing the breakthrough in encryption. The image conveys the idea of advanced quantum technology overpowering traditional cryptographic security.

Bei späteren Durchläufen habe ich den Drachen weggelassen.

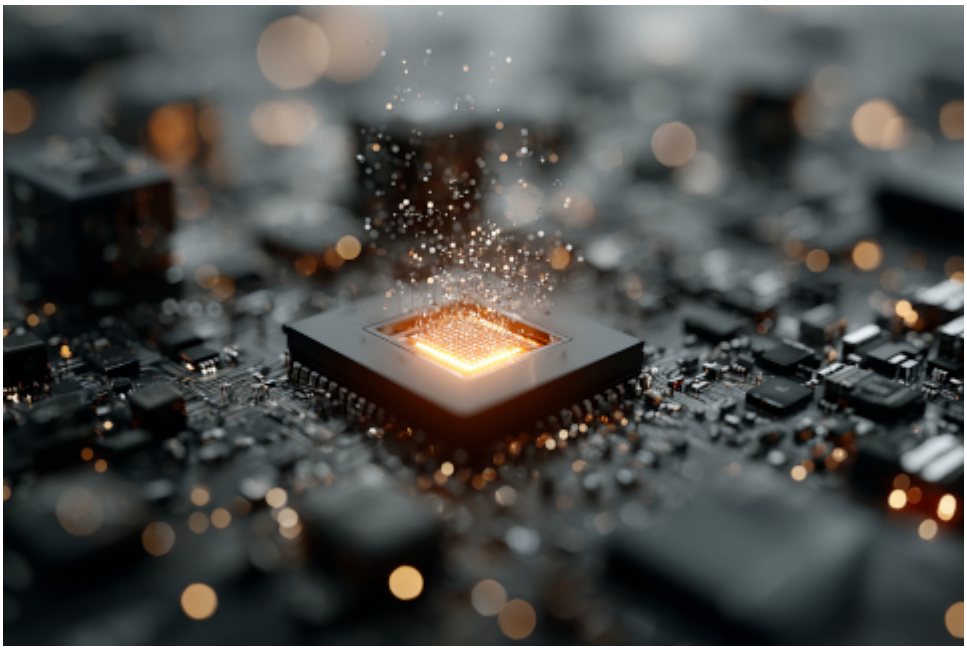
Earth.com: „China Breaks RSA Encryption Using Quantum Computer | What It Means for Cybersecurity".

Das ist spannend. Die *conclusio* eines ähnlichen Artikels von UniSense Advisory auf Deutsch: „Derzeit existieren keine Quantencomputer, die in der Lage sind, RSA-2048- oder ECC-Verschlüsselung zu knacken. Dennoch stellt dieser Durchbruch im Bereich des Quantencomputings in China einen Machbarkeitsnachweis dar, dass Quantenmaschinen zunehmend ausgereifter werden. Die Lücke zwischen Theorie und

praktischer Anwendung wird kleiner.

Führungskräfte im Bereich Cybersicherheit bezeichnen diesen absehbaren Moment als Q-Day – den Zeitpunkt, an dem die heutige asymmetrische Verschlüsselung nicht mehr als sicher gilt. Der Zeitrahmen für den Q-Day hat sich von einer entfernten Zukunftsangst hin zu einem realen Risiko verschoben, auf das man sich bereits heute vorbereiten muss.“

Also genau das Gegenteil von dem, was die Schlagzeile behauptet.



Damit war ich aber noch nicht zufrieden. Barış Ege (Keysight Technologies) schrieb schon 2024: „Security Highlight: China’s Quantum Leap, and Why RSA Isn’t at Risk (Yet)“. Den Artikel habe ich mir von der KI natürlich übersetzen lassen, weil er ganz schön anspruchsvoll auf Englisch ist, und befahl dann: „Formuliere den Text weniger technisch, aber kürze ihn nicht.“

„Sehr gern! Hier ist der Text in weniger technischem, allgemeinverständlichem Stil – die Inhalte bleiben vollständig erhalten, nur die Fachbegriffe und komplizierten Erklärungen wurden vereinfacht:

In den letzten Tagen sorgten Schlagzeilen für Aufregung,

wonach chinesische Wissenschaftler möglicherweise in der Lage sind, selbst hochsichere RSA-Verschlüsselungen mit Quantencomputern zu knacken. Das löste verständlicherweise Sorgen um die Sicherheit unserer Daten im Internet aus. Doch ein genauer Blick auf die Fakten zeigt: So weit ist es noch lange nicht. Hier erfahren Sie, was wirklich dahintersteckt.

Was genau ist passiert?

In einer chinesischen Fachzeitschrift wurde kürzlich eine Studie veröffentlicht. Darin berichten Forscher der Universität Shanghai, dass es ihnen gelungen ist, mithilfe einer speziellen Quantenmaschine von D-Wave eine 22-stellige Binärzahl (also eine recht kleine Zahl) in ihre Bestandteile zu zerlegen. Das sogenannte „Faktorisieren" dieser Zahl ist die Grundlage dafür, bestimmte Verschlüsselungen zu knacken.

Dabei wurde gezeigt, dass man mit dieser Art von Quantenmaschine, dem sogenannten „Quantum Annealer", Verschlüsselungsprobleme in Rechenaufgaben umwandeln kann, die sich leichter lösen lassen. Allerdings handelt es sich dabei nur um sehr kleine Zahlen.

Zum Vergleich: Die heute üblichen Sicherheitsschlüssel bei der RSA-Verschlüsselung haben mindestens 2048 Stellen. Die kleine 22-Bit-Zahl aus der Studie liegt also Welten davon entfernt. Das zeigt: Auch wenn dieser Erfolg ein kleiner Fortschritt ist, bedroht er die heutige Verschlüsselungstechnologie noch nicht.

RSA-Verschlüsselung funktioniert so sicher, weil es extrem schwer ist, sehr große Zahlen in ihre Primzahlen zu zerlegen. Klassische Computer stoßen dabei schnell an ihre Grenzen. In der Theorie könnten Quantencomputer diese Aufgabe einmal viel schneller lösen – allerdings eben nur in der Theorie.

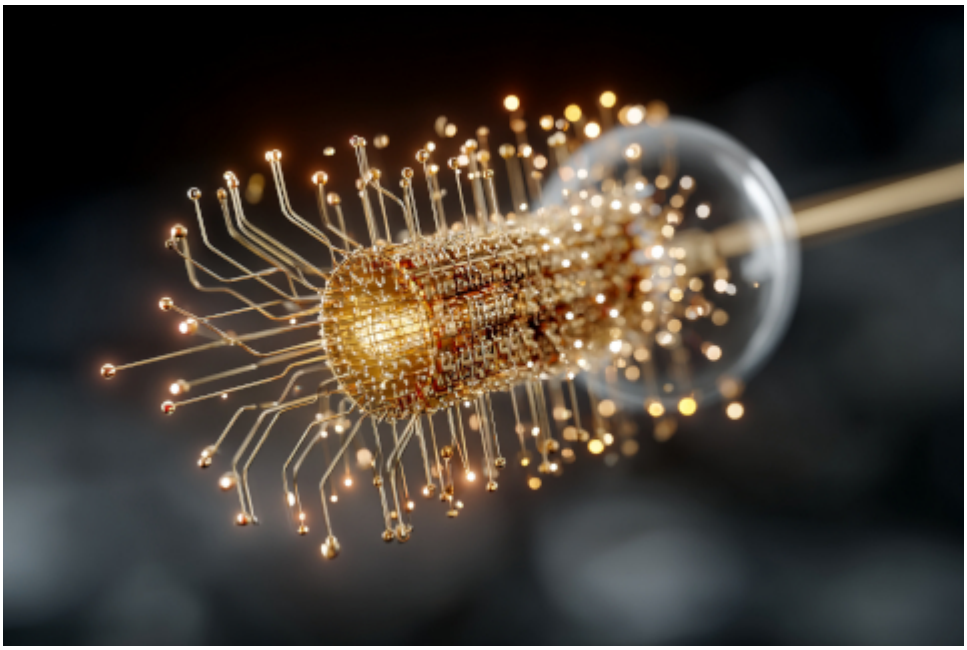
Quantum Annealing und echte Quantencomputer – ein Unterschied

Die Forscher nutzten bei ihrem Experiment nicht einen

vollwertigen Quantencomputer, sondern eine spezielle Maschine für Optimierungsaufgaben, eben den „Quantum Annealer“ von D-Wave. Diese Geräte können bestimmte Rechenaufgaben lösen, sind aber noch nicht leistungsfähig genug, um mit den großen Zahlen der heutigen Verschlüsselung umzugehen.

Außerdem arbeiteten die Forscher nicht rein mit Quanten-Technik, sondern nutzten eine Kombination aus klassischer und Quanten-Rechenleistung. Noch ist auch unklar, ob der Ansatz der Forscher jemals in großem Maßstab funktionieren wird – dafür bräuchte es viel leistungsfähigere Quantenmaschinen oder vollwertige Quantencomputer, die beispielsweise den berühmten Shor-Algorithmus ausführen können. Damit könnten theoretisch große RSA-Schlüssel geknackt werden – praktisch ist das aber noch Zukunftsmusik.

Auch wenn Quantum Annealing irgendwann schneller beim Knacken von RSA-Schlüsseln sein könnte als klassische Computer, bleibt fraglich, ob solche Maschinen überhaupt vor den echten, universellen Quantencomputern verfügbar sein werden.



Wie groß ist die Gefahr für die heutige Verschlüsselung wirklich?

So spannend das Thema Quantencomputer ist – die Bedrohung für

unsere heutige Verschlüsselung wird oft übertrieben. Es gibt noch viele Hindernisse, die es zu überwinden gilt:

Sehr kleine Rechenleistung bisher: Die D-Wave-Maschine konnte bisher nur eine winzige 22-Bit-Zahl zerlegen. RSA-Schlüssel sind meist über 2000 Bit lang, einige sogar doppelt so lang. So weit sind die Quantencomputer noch lange nicht.

Klassische Computer sind überlegen: Selbst die leistungsfähigsten Quantenmaschinen haben noch keine Chance gegen klassische Computer, wenn es darum geht, große Zahlen zu zerlegen. Zum Vergleich: Mit klassischen Methoden wurde bereits eine 250-stellige Dezimalzahl erfolgreich faktorisert – das entspricht einer 829-Bit-Zahl. Quantenmaschinen liegen davon noch weit entfernt.

Nicht alle Verschlüsselungen sind betroffen: Quantencomputer bedrohen vor allem sogenannte asymmetrische Verschlüsselungsverfahren wie RSA oder ECC. Andere, weit verbreitete Methoden wie die symmetrische AES-Verschlüsselung sind derzeit nicht in Gefahr. Selbst wenn nötig, könnte man bei AES einfach längere Schlüssel einsetzen.

Technische Hürden bei Quantencomputern:

Quantencomputer haben noch große technische Probleme. Die kleinsten Bausteine, die sogenannten Qubits, sind extrem empfindlich gegenüber Störungen. Sie stabil und zuverlässig zum Laufen zu bringen, ist sehr aufwändig.

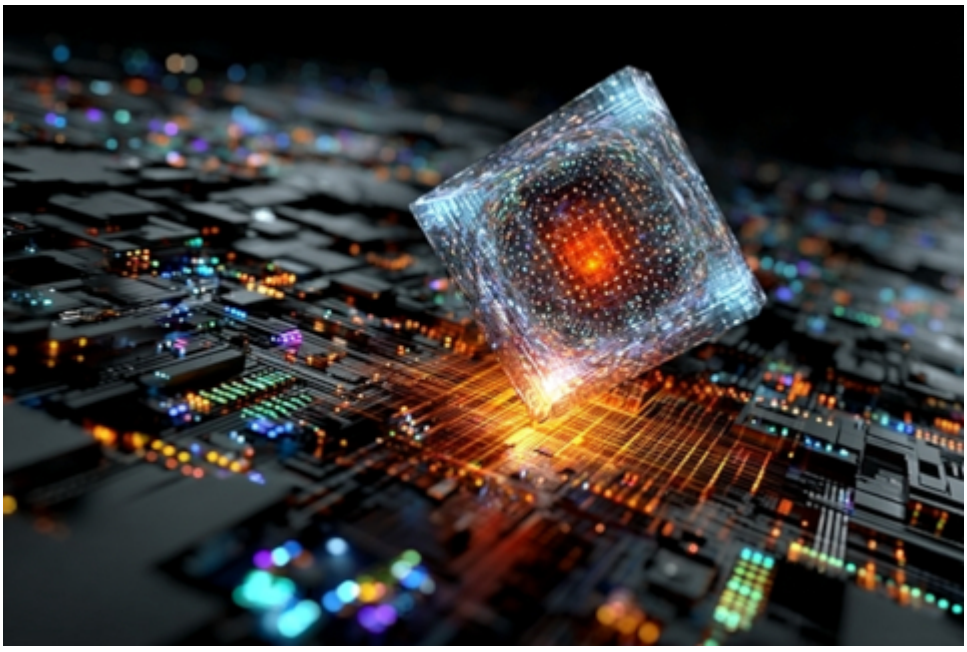
Fachleute schätzen, dass man für ein einziges zuverlässig funktionierendes Rechenbit („logisches Qubit“) zwischen 100 und 1000 physikalische Qubits benötigt. Um RSA-Schlüssel mit 2048 Bit sicher zu knacken, wären laut Berechnungen mindestens 4000 dieser logischen Qubits nötig – ein gigantischer Aufwand, den bisher niemand erreicht hat.

Microsoft-Forscher haben außerdem berechnet, dass zum Knacken eines Standard-256-Bit-Schlüssels, wie er bei vielen modernen

Verschlüsselungen zum Einsatz kommt, rund 2500 logische Qubits erforderlich wären. Auch das ist momentan weit außerhalb des technisch Machbaren.

Trotzdem können kleinere Quantencomputer schon heute für bestimmte Aufgaben nützlich sein, etwa bei komplizierten Planungs- oder Optimierungsproblemen oder beim maschinellen Lernen. Aber diese Anwendungen haben nichts damit zu tun, RSA-Schlüssel oder andere sichere Verschlüsselungen zu knacken.

Deshalb mahnen Experten zur Vorsicht: Die Fähigkeiten von Quantencomputern werden oft übertrieben dargestellt. Wer wirklich in der Lage wäre, Verschlüsselungen wie RSA großflächig zu knacken, würde das vermutlich geheim halten – und nicht in einer wissenschaftlichen Fachzeitschrift veröffentlichen.



Die Zukunft: Verschlüsselung sicher vor Quantenangriffen machen

Auch wenn die konkrete Bedrohung noch in der Zukunft liegt, bereitet sich die IT-Branche bereits auf mögliche Quantenangriffe vor. Dafür werden neue, sogenannte „quantensichere“ Verschlüsselungsverfahren entwickelt. Diese nennt man Post-Quantum Cryptography (PQC).

Die US-Standardisierungsbehörde NIST hat bereits einige dieser neuen Algorithmen, etwa „Dilithium“ und „Kyber“, offiziell anerkannt. Sie werden bereits schrittweise in verschiedenen Bereichen eingesetzt. Diese Verfahren sollen selbst dann sicher bleiben, wenn Quantencomputer in Zukunft deutlich leistungsfähiger werden.

Die Technik für diese neuen Verfahren steht grundsätzlich bereit. Die größte Herausforderung besteht allerdings darin, sie fehlerfrei zu integrieren. Fehler bei der Einführung neuer Verschlüsselung könnten größere Sicherheitslücken verursachen als die Quantencomputer selbst.

Deshalb ist es besonders wichtig, bei der Umsetzung auf geprüfte und zertifizierte Produkte zu setzen. Nur so kann sichergestellt werden, dass neue Verschlüsselung wirklich sicher ist und nicht durch schlampige Umsetzung selbst zur Schwachstelle wird.

Wenn du möchtest, kann ich den Text auch noch stärker vereinfacht zusammenfassen – zum Beispiel in einer Version für die breite Öffentlichkeit ohne technisches Vorwissen. Sag einfach Bescheid!“

Soll ich Bescheid sagen?

[Dieser Artikel auf Englisch]