Quantensichere Verschlüsselung: Quantum Brilliance, CyberSeQ und LuxProvide treiben gemeinsam Post-Quanten-Kryptografie voran

Hersteller von Quantencomputern, Spezialist für Cybersecurity und HPC-Betreiber geben Partnerschaft bekannt und entwickeln Algorithmen für Post-Quanten-Kryptografie auf Basis echter Zufallszahlen

-- Hersteller von Quantencomputern, Spezialist für Cybersecurity und HPC-Betreiber geben Partnerschaft bekannt und entwickeln Algorithmen für Post-Quanten-Kryptografie auf Basis echter Zufallszahlen

-- Certified Randomness als zentraler Erfolgsfaktor für künftige IT-Sicherheit

STUTTGART, 1. Oktober 2025 --- Quantum Brilliance, deutsch-australischer Anbieter von großflächig einsetzbarer und bei Raumtemperatur funktionierender Quantentechnologie auf Diamantbasis, gibt eine strategische Partnerschaft mit CyberSeQ, Spezialist für quantenbasierte Cybersecurity, und LuxProvide, Betreiber des Supercomputers MeluXina, bekannt: In einer gemeinsamen Absichtserklärung kündigen die drei Partner ein Programm zur Entwicklung von Verschlüsselungsverfahren an, die im Sinne einer Post-Quanten-Kryptografie (PQC) auch vor Cyberangriffen mit Quantencomputern sicher sind.

Echte Zufallszahlen für Certified Randomness

Als Basis der quantensicheren Verschlüsselungen dienen echte Zufallszahlen (engl. True Random Numbers oder TRN), erzeugt durch den virtuellen Quantenchip (vQPU) von Quantum Brilliance. Diese sollen in allen vom amerikanischen NIST und ihren europäischen Pendants wie BSI, ENISA, ANSSI & Co. entwickelten oder sich aktuell in Arbeit befindenden PQC-Standards zum Einsatz kommen. Anders als klassische Pseudozufallszahlen, deren Erstellung sich potenziell rekonstruieren lässt, entstehenden TRN durch quantenphysikalische Messprozesse. Diese sind nicht deterministisch, sondern nur durch Wahrscheinlichkeiten beschreibbar, was Quantencomputer nutzen, um Certified Randomness zu erzeugen. Diese sorgt dafür, dass die erzeugten Zufallsbits weder gefälscht noch vorhersehbar oder beeinflussbar sind. Auch dann nicht, wenn ein möglicher Angreifer die Quelle bzw. der Ausgeber der Zahlenquelle ist. Damit ist Certified Randomness ein zentraler Erfolgsfaktor für künftige Sicherheit im Zeitalter der Quantencomputer. Besonders wichtig dabei sind die Aspekte Verfügbarkeit und Skalierbarkeit. Die diamantbasierten Quantenbeschleuniger von Quantum Brilliance arbeiten bei Raumtemperatur und benötigen weder aufwendige Kryotechnik noch große Infrastruktur. Dadurch lassen sie sich stark miniaturisieren und in großer Stückzahl parallel in Rechenzentren installieren.

Spezialisierte Algorithmen für Post-Quanten-Kryptografie

Die von den Quantenbeschleunigern generierten Zahlen werden in Blocks von 32 Bytes extrahiert, von CyberSeQ in spezialisierte PQC-Algorithmen integriert und hinsichtlich statistischer Qualität, Entropie und Zertifizierbarkeit der TRN geprüft. Für die Validierung kommt der Supercomputer MeluXina von LuxProvide zum Einsatz. Post-Quanten-Kryptografie ist eines der wichtigsten Zukunftsfelder in der Cyber-Security. Speziell die Finanzbranche und weitere Wirtschaftsteile haben ein großes Interesse an neuen Wegen der Verschlüsslung und Authentifizierung, da viele der bisherigen Verfahren der Rechenweise und den Möglichkeiten von Quantencomputern nicht standhalten.

"Diese Partnerschaft ist ein wichtiger Meilenstein auf dem Weg zu Cybersicherheit und Verschlüsselung in der sehr nahen Zukunft. Post-Quanten-Kryptografie wird ohne Certified Randomness nicht gelingen - und unsere Quantenbeschleuniger sind ideal dafür geeignet, hier eine tragende Rolle zu spielen. Wir freuen uns darauf, gemeinsam mit unseren Partnern quantenbasierte manipulations- und zukunftssichere IT-Security zu entwickeln", erklärt Mark Mattingley-Scott, Europachef von Quantum Brilliance.

"Mit dieser Partnerschaft werden wir gemeinsam die Sicherheit im Zeitalter der Quantencomputer vorantreiben. Wir integrieren TRN in unsere PQC-Referenzarchitektur und untermauern damit unser Versprechen: Quantum-secure, AI-smart und Cloud-native", sagt Mark Tehrani, Gründer und CEO von CyberSeQ.

"Unser Supercomputer MeluXina bietet in Kombination mit unseren Tools die optimale Umgebung zum Generieren und Speichern von True Random Numbers. Wir freuen uns, Teil dieses leistungsstarken Konsortiums zu sein und zu einer IT-seitig sicheren Zukunft beizutragen", betont Vittorio Santonocito, Head of Startup bei LuxProvide.

ca. 3.800 Zeichen

Pressekontakt

Dr. Haffa & Partner GmbH

Herr Philipp Moritz
Karlstraße 42
80333 München

haffapartner.de
postbox@haffapartner.de

Firmenkontakt

Quantum Brilliance GmbH

Herr Dr. Mark Mattingley-Scott
Colorado Tower Industriestraße 4
70565 Stuttgart

https://quantumbrilliance.com
mark.mattingley-scott@quantum-brilliance.com

Quantum Brilliance wurde 2019 gegründet und ist ein wagniskapitalfinanzierter australisch-deutscher Hersteller von Quantencomputing-Hardware. Das Unternehmen bietet Quantenbeschleuniger aus synthetischen Diamanten sowie ein Set aus Softwaretools und Applikationen. Die Vision ist es, einen breiten Einsatz von Quantenbeschleunigern zu ermöglichen - um die Industrie in die Lage zu versetzen, Edge-Computing-Anwendungen und Supercomputer der nächsten Generation zu nutzen. Quantum Brilliance verfügt über Partnerschaften in Nordamerika, Europa sowie Asien-Pazifik und arbeitet mit Regierungen, Supercomputing-Centern, Forschungseinrichtungen und führenden Köpfen aus der Industrie zusammen.

Anlage: Bild