idw - Informationsdienst Wissenschaft
Nachrichten, Termine, Experten

Pressemitteilung

Fraunhofer-Institut für Photonische Mikrosysteme (IPMS)
Franka Balvin

06.02.2023
http://idw-online.de/de/news808800

Forschungs- / Wissenstransfer, Forschungsprojekte
Elektrotechnik, Informationstechnik, Physik / Astronomie
überregional

Quantensichere Identitäten für eine digitale Zukunft

Die Sicherheit digitaler Identitäten wird durch zukünftige Quantentechnologien bedroht. In den Händen von Angreifern werden Quantencomputer auch in der Lage sein, klassische Verschlüsselungsverfahren zu brechen. Um solche Angriffe abzuwehren, forschen vier Partner in dem Projekt Quant-ID an der Entwicklung von neuartigen Verfahren und Systemen, die auf Basis von Quantenzufallszahlen und Post-Quantum-Kryptographie die Sicherheit auch langfristig garantieren. Gerade hochsensible Bereiche, wie staatliche Einrichtungen, Banken oder Versicherungen werden dadurch den notwendigen Schutz erhalten. Das vom BMBF geförderte Projekt startete im September 2022 mit einer Laufzeit von drei Jahren.

Um eine größere Akzeptanz für die Digitalisierung von Dienstleistungen und Geschäftsprozessen in der Gesellschaft zu erreichen, müssen benutzerfreundliche, zuverlässige und die Privatsphäre schützende Verfahren etabliert werden. Im Projekt »Sichere Quantenkommunikation für Kritische Identity Access Management Infrastrukturen (Quant-ID)« forschen deshalb die Quant-X Security & Coding GmbH, das Fraunhofer-Institut für Photonische Mikrosysteme IPMS, die MTG AG sowie die Universität Regensburg gemeinsam an verlässlichen digitalen Identitäten. Die Verwendung von aktuell genutzten Netzwerkprotokollen soll hierbei den Übergang von klassischen Verschlüsselungsalgorithmen zu quantensicheren Verfahren erleichtern. Abweichend vom ursprünglichen physikalischen Begriff bezeichnet Quantensicherheit dabei hier den Schutz gegen Angriffe durch Quantencomputer.

»Unser Ziel ist die Entwicklung einer quantensicheren Autorisierung von Nutzern in einer IAM-Architektur (Identity Access Management) unter Zuhilfenahme von Quantenzufallszahlen und Post-Quanten-Kryptographie«, erklärt Dr. Alexander Noack, Gruppenleiter am Fraunhofer-Institut für Photonische Mikrosysteme IPMS. Unter Post-Quanten-Kryptographie (PQC für engl. Post Quantum Cryptography) werden kryptographische Algorithmen verstanden, die zwar auf klassischer Hardware verwendet werden, welche jedoch Sicherheit gegenüber Angriffen mit Quantencomputern versprechen. Die für diese Verfahren notwendigen echten Zufallszahlen sollen im Projekt zur Steigerung der Sicherheit durch einen Quantum-Random-Number-Generator (QRNG) erzeugt werden. »Zusätzlich wollen wir auch die Netzwerkkommunikation, Signaturen und Datenbankverschlüsselung durch Post-Quanten-Kryptographie absichern«, so Dr. Alexander Noack. Ein weiteres Ziel des Gemeinschaftsprojekts ist die Entwicklung eines quantensicheren »Single-Sign-On« Ansatzes, der den Zugriff auf verschiedene Dienste mit einer einzigen zentralen Anmeldung ermöglicht.
Zum Projektende werden die digitalen Identitäten und die quantensichere Autorisierung in einem Demonstrator in einer realistischen Anwendung über bestehende Netzwerkprotokolle erprobt. Dabei werden die Fähigkeiten des entwickelten Systems mit klassischen Verfahren verglichen. Die Ergebnisse der Teilprojekte werden auch modular anwendbar sein. Dies bietet Netzwerkadministratoren und Systemverantwortlichen die Möglichkeit, entweder das gesamte System oder nur Teilaspekte zu integrieren.

Durch die Konzeptentwicklung in Deutschland wird die Souveränität mit Blick auf die Sicherheit nationaler informationstechnischer Systeme gestärkt. Vor diesem Hintergrund ergibt sich ein besonders hohes Marktpotenzial der Projektlösung in hochsensiblen Bereichen und kritischen Infrastrukturen wie im Bereich der Banken, Versicherungen,

Unternehmen des Gesundheitsbereiches sowie Behörden und staatlichen Einrichtungen. Gerade diese Marktteilnehmer sind darauf angewiesen, hohe Sicherheitsstandards zu erfüllen, da sie vielfach immer komplexer werdenden Angriffsstrukturen ausgesetzt sind. Um die Verwertung des Quantenzufallsgenerators zu unterstützen, wird zudem eine Zertifizierung durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) angestrebt.
Motivation des Konsortiums ist es, ein interdisziplinäres Projektteam aufzubauen, Partnerschaften in Deutschland für Gesamtlösungen zu etablieren und Absicherungstechnologien gegen Angriffe mit Quantencomputern jedermann zugänglich zu machen. »Mit diesem Projekt wollen wir die Grundlage für interdisziplinäre Kooperationen zur effizienten Realisierung von Quantensicherheit in Deutschland schaffen«, so der Gruppenleiter des Fraunhofer IPMS. Die daraus entstehende quantensichere Version von OpenID Connect soll der Allgemeinheit für geringe Kosten als Open-Source-Bibliothek zugänglich gemacht werden.

Somit schafft Quant-ID die Grundlage für einen hochsicheren Schutz in kritischen Infrastrukturen in einer End-to-End-Lösung in Deutschland. Durch den Use Case »Quantensichere eID« wird das Sicherheitsniveau gegen Cyberangriffe für alle ansässigen Unternehmen und staatlichen Einrichtungen erhöht. Gleichzeitig wird eine Grundlage für die langfristige Sicherheit von Identitätsdaten und anderen sensiblen Daten deutscher Bürger geschaffen. »Das Projekt verfolgt über diesen Weg den Ansatz, die ethischen, gesellschaftlichen und wirtschaftlichen Werte Deutschlands früh genug vor fremden staatlichen und kriminellen Angriffen zu schützen«, so Dr. Alexander Noack abschließend. Die internationale Positionierung als deutsches Konsortium in einer neu zu schaffenden öffentlichen OpenID-Working-Group mit dem Ziel der Definition von »OpenID-Quantum« garantiert außerdem den parallelen Anschluss an internationale Standardisierungsvorhaben. Weitere Informationen finden sich auf der Webseite zum Projekt unter: https://quant-id.de/.

Beteiligte Einrichtungen des Quant ID

Verbundkoordinator:
Quant-X Security & Coding GmbH ist ein Startup mit Schwerpunkt Informationssicherheit. Die Expertise der Firma beruht auf 10 Jahren Beratungserfahrung für Fintechs und Banken. Die Beratungsleistungen umfassen Konzeption, Planung, Entwicklung, Steuerung, und Qualitätssicherung im Bereich Informationssicherheit. Experten von Quant-X wurden mit Implementation und Troubleshooting von IAM-Infrastrukturen in mehreren Projekten beauftragt. Mit verschiedene Quantentheorie- und Sicherheits-Experten untersucht Quant-X ausgewählte offene Fragen zum Thema Quantensicherheit mit Fokus auf konkrete Anwendungen.

Das Fraunhofer-Institut für Photonische Mikrosysteme IPMS erforscht mikroelektronische und mikromechanische Low-Power-Sensoren, Aktoren sowie optische, drahtlose Hochgeschwindigkeitsdatenkommunikation. Als innovativer Entwicklungsdienstleister für elektronische und photonische Mikrosysteme finden sich in allen großen Märkten – wie Information und Kommunikation, Fahrzeugtechnik, Halbleiter, Mess- und Medizintechnik - innovative Produkte, die auf am IPMS entwickelten Technologien basieren. Auch Hochgeschwindigkeits-FPGA- und Mixed-Signal-ASIC-Design gehören zum Portfolio. Die elektronische Ansteuerung und Auswertung von Qubits und aktiven photonischen Einzelelementen bis hin zu Rechenbeschleunigern über dedizierte integrierte Elektronik liegen dabei im Fokus.

Seit der Gründung im Jahr 1995 ist die MTG AG einer der führenden Spezialisten für anspruchsvolle Verschlüsselungstechnologien in Deutschland. Die innovativen IT-Security Lösungen von MTG sichern kritische Infrastrukturen und das Internet der Dinge effektiv ab. MTG beteiligt sich an dem Förderprojekt QuantumRISC des Bundesministeriums für Bildung und Forschung (BMBF) und hat das Förderprojekt Use-A-PQClib des Hessischen Ministerium für Wissenschaft und Kunst (HMWK) erfolgreich abgeschlossen. Im Rahmen dieser beiden Forschungsprojekte hat MTG umfangreiche Erfahrungen in der Entwicklung und Integration von PQC- Verfahren in Software gesammelt.

Die Universität Regensburg (UR) ist eine bayrische Volluniversität, deren jüngste Fakultät, die Fakultät für Informatik und Data Science (FIDS), erst im Jahr 2020 gegründet wurde. Seit 2021 wird der Lehrstuhl für Datensicherheit und Kryptographie von Prof. Dr. Juliane Krämer besetzt. Die Arbeitsgruppe QPC (Quantum and Physical attack resistant Cryptography) von Prof. Krämer erforscht alle fünf Familien der Post-Quantum- Kryptographie bzgl. verschiedener Aspekte, z.B. [ABB+20, GHK+21, GKS21, KS20, RKK20]. Die Gruppe ist Teil verschiedener Forschungsprojekte, z.B. DFG-SFB CROSSING, QuantumRISC, Aquorypt, 6G-RIC. In das vorliegende Projekt Quant-ID bringt Prof. Krämer ihre umfangreiche Expertise in der Analyse, Entwicklung und Integration von PQC-Verfahren ein.

Ergänzung vom 08.02.2023:

Verbundkoordinator:
Quant-X Security & Coding GmbH ist ein Startup mit Schwerpunkt Informationssicherheit. Die Expertise der Firma beruht auf 10 Jahren Beratungserfahrung für Fintechs und Banken. Die Beratungsleistungen umfassen Konzeption, Planung, Entwicklung, Steuerung, und Qualitätssicherung im Bereich Informationssicherheit. Experten von Quant-X wurden mit Implementation und Troubleshooting von IAM-Infrastrukturen in mehreren Projekten beauftragt, unter anderem für VWFS und die Deutsche Bank. Mit verschiedene Quantentheorie- und Sicherheits-Experten untersucht Quant-X ausgewählte offene Fragen zum Thema Quantensicherheit mit Fokus auf konkrete Anwendungen.

Projekt »Sichere Quantenkommunikation für Kritische Identity Access Management Infrastrukturen – Quant-ID«
©Fraunhofer IPMS