

Forschungsprogramm SCA4PQC soll seitenkanalresistente Post-Quanten- Kryptologie entwickeln

31.03.2025, 15:59 | Wissenschaft, Forschung, Bildung

Pressemitteilung von: *idw - Informationsdienst Wissenschaft*



Die rasante Entwicklung leistungsstarker Quantencomputer bedroht bestehende kryptographische Verfahren, die bislang als sicher galten. Da viele der gegenwärtig genutzten Algorithmen in absehbarer Zeit nicht mehr ausreichend Schutz bieten könnten, beschäftigt sich die Forschung intensiv mit Post-Quanten-Kryptographie. Dennoch bleibt die Abwehr von Seitenkanalangriffen eine zentrale Herausforderung. Diese nutzen physikalische Eigenschaften wie Stromverbrauch, elektromagnetische Abstrahlung oder Zeitmessungen, um vertrauliche Daten zu entschlüsseln. Um diesem Risiko zu begegnen, müssen Verschlüsselungstechnologien über mathematische Sicherheit hinaus gegen physische Bedrohungen geschützt werden.

Das Programm SCA4PQC verfolgt die Entwicklung von kryptographischen Verfahren, die sowohl mathematischen als auch seitenkanalspezifischen Angriffen standhalten. Ziel ist es, Methoden zu schaffen, die praktikabel, effizient und nachhaltig sicher sind. Die entwickelten Lösungen sollen nicht nur in der Theorie überzeugen, sondern auch unter realen Bedingungen bestehen.

Drei zentrale Forschungsbereiche stehen dabei im Mittelpunkt. Die erste Forschungsrichtung widmet sich der Sicherheit von Cloud- und Desktop-Umgebungen, insbesondere im Hinblick auf virtualisierte Systeme und geteilte Infrastruktur. Die zweite Forschungsrichtung konzentriert sich auf das Internet der Dinge, wo aufgrund begrenzter Ressourcen besondere Schutzmaßnahmen erforderlich sind. Der dritte Bereich untersucht die Sicherheit von Smartcards, die unter anderem in der digitalen Identitätsverwaltung und im Zahlungsverkehr genutzt werden.

Das Programm ist in mehrere Phasen gegliedert. Zunächst haben interessierte Institutionen die Möglichkeit, sich innerhalb eines Monats für die Teilnahme zu bewerben. Anschließend werden in einer dreimonatigen Konzeptphase detaillierte Forschungs- und Entwicklungsstrategien ausgearbeitet. Die darauffolgende vierjährige Forschungsphase besteht aus zwei Abschnitten: Drei Jahre sind der Grundlagenforschung gewidmet, während das letzte Jahr zur Entwicklung von Demonstratoren und zur Untersuchung ihrer Widerstandsfähigkeit gegen Seitenkanalangriffe dient.

Dr. Matthias Minihold, Leiter des Forschungsprogramms, hebt die strategische Bedeutung dieses Vorhabens hervor. Er unterstreicht, „dass die Absicherung digitaler Infrastrukturen gegen Quanten- und Seitenkanalangriffe eine wesentliche

Voraussetzung für die digitale Souveränität der Zukunft ist. Nur durch gezielte Forschung und Entwicklung könnten kryptographische Verfahren geschaffen werden, die den Bedrohungen der kommenden Jahre standhalten.“

Die Cyberagentur lädt Forschungseinrichtungen und Unternehmen ein, sich an diesem zukunftsweisenden Projekt zu beteiligen. Gemeinsam sollen innovative Lösungen entwickelt werden, um eine robuste digitale Sicherheitsarchitektur für die Post-Quanten-Ära zu gewährleisten.

Im Supplement zum Amtsblatt der Europäischen Union wurde die Ausschreibung mit der Auftragsbekanntmachungsnummer TED 202003-2025 veröffentlicht:
<https://ted.europa.eu/de/notice/-/detail/202003-2025>. Ende des Teilnahmewettbewerbs ist der 05.05.2025.

Weitere Informationen:

<https://www.cyberagentur.de/programme/sca4pqc/>

Auch der März-Podcast „Per Anhalter durch den Cyberspace“ beschäftigt sich mit dem Thema: <https://cyberraum-podcast.podigee.io/7-quantensicherheit>. Prof. Dr. Antonia Wachter-Zeh von der Technischen Universität München und Prof. Dr. Jürgen Freudenberger von der Cyberagentur sprechen über die Sicherheit im Osten.

Kontakt:

Agentur für Innovation in der Cybersicherheit GmbH
Große Steinstraße 19
06108 Halle (Saale)

Michael Lindner
Pressesprecher
Tel.: +49 151 44150 645
E-Mail:

Hintergrund: Cyberagentur

Die Agentur für Innovation in der Cybersicherheit GmbH (Cyberagentur) wurde im Jahr 2020 als vollständige Inhouse-Gesellschaft des Bundes unter der gemeinsamen Federführung des Bundesministeriums der Verteidigung und des Bundesministeriums des Inneren und für Heimat durch die Bundesregierung mit dem Ziel gegründet, einen im Bereich der Cybersicherheit anwendungsstrategiebezogenen und ressortübergreifenden Blick auf die Innere und Äußere Sicherheit einzunehmen. Vor diesem Hintergrund bezweckt die Arbeit der Cyberagentur maßgeblich eine institutionalisierte Durchführung von hochinnovativen Vorhaben, die mit einem hohen Risiko bezüglich der Zielerreichung behaftet sind, gleichzeitig aber ein sehr hohes Disruptionspotenzial bei Erfolg innehaben können. Die Cyberagentur ist Bestandteil der Nationalen Sicherheitsstrategie der Bundesrepublik Deutschland. Der Cyberagentur stehen Prof. Dr. Christian Hummert als Forschungsdirektor und Geschäftsführer sowie Daniel Mayer als kaufmännischer Direktor vor.

wissenschaftliche Ansprechpartner:

Dr. Matthias Minihold, Leiter des Forschungsprogramms und Leiter des Referats Kryptologie

Originalpublikation:

<https://www.cyberagentur.de/presse/post-quanten-sicherheit-als-herausforderung-der-zukunft/>

Agentur für Innovation in der Cybersicherheit GmbH

MichaelLindner (Mitarbeiter in der Presse- und Öffentlichkeitsarbeit)

+49 151 44150645

lindner@cyberagentur.de

News-ID: 1280752 • Views: 659 (Stand: 27.09.2026)

Link zur Pressemitteilung:

<https://www.openpr.de/news/1280752/Forschungsprogramm-SCA4PQC-soll-seitenkanalresistente-Post-Quanten-Kryptologie-entwickeln-idw.html>