Dienstag, 24. Mai 2022, 13 – 18 Uhr
Fraunhofer-Institut für Angewandte und Integrierte Sicherheit AISEC
Lichtenbergstr. 11, 85748 Garching b. München

Fraunhofer AISEC

MÜNCHNER KREIS

Einladung

Workshop »Post-Quanten-Kryptografie«

Workshop »Post-Quanten-Kryptografie«

Quantencomputer werden in naher Zukunft gängige kryptografische Verfahren und Protokolle brechen. Die Wettbewerbsfähigkeit und technologische Souveränität der Wirtschaft sind in Gefahr. Um sich auf diese Herausforderung vorzubereiten, fördert das Bundesministerium für Bildung und Forschung (BMBF) die Zusammenarbeit von Unternehmen und Forschungseinrichtungen auf diesem Gebiet. Seit 2019 entstehen in insgesamt sieben Forschungsprojekten der Förderlinie »Post-Quanten-Kryptografie« effiziente, sichere Soft- und Hardwarelösungen für Quantencomputer-resistente Verfahren.

Am 24. Mai 2022 stellen die Partner den Stand ihrer Arbeiten am Fraunhofer-Institut für Angewandte und Integrierte Sicherheit AISEC vor.

Dienstag, 24. Mai 2022, 13:00 – 18:00 Uhr

Fraunhofer AISEC
Lichtenbergstr. 11, 85748 Garching b. München

Anfahrt: https://s.fhg.de/anfahrtaisec

Anmeldung: https://s.fhg.de/WorkshopPQK

Die Veranstaltung findet in Präsenz unter 3G-Bedingungen statt. Eine virtuelle Teilnahme ist möglich.

Workshop »Post-Quanten-Kryptografie«

Dienstag, 24. Mai 2022

13:00 Begrüßung (Georg Sigl, Fraunhofer AISEC)

13:15 Die Quantum Computing Roadmap der IBM (Jan-Rainer Lahmann, IBM)

13:45 Kryptografie quantensicher gestalten (Manfred Lochter, BSI)

14:15 Pause

14:45 Wissenschaftliche Highlights aus dem Programm

- Mixed Certificate Chains for the Transition to Post-Quantum Authentication in TLS 1.3 (Sebastian Paul, Robert Bosch GmbH)
- Re-encryption as the Bane of Securely implementing lattice-based Key Exchanges (Peter Pessl, Infineon Technologies AG)
- Post-Quantum Virtual Private Networks (Stefan-Lukas Gazdag, genua GmbH)
- Accelerating Stateful Hash-Based Signatures in Hardware (Jan Thoma, Ruhr-Universität Bochum)

16:00 Pause

16:30 Podiumsdiskussion
»Welchen Mehrwert hat Post-Quanten-Kryptografie für Unternehmen?« mit
Juliane Krämer, Universität Regensburg
Manfred Lochter, BSI
Kim Nguyen, D-Trust GmbH
Jörn Eichler, Volkswagen AG
Moderation: Marian Margraf, Fraunhofer AISEC

17:45 Verabschiedung und Ausblick (Georg Sigl, Fraunhofer AISEC)

18:00 Fingerfood & Networking