Bits & Qubits

Einladung zur Herbsttagung

Mittwoch, 6. September 2023, 13:00 bis 17:00 Uhr

Gleisarena FFHS, Zollstrasse 17, Zürich

Die Teilnahme ist kostenlos.
Anmeldung bis Freitag, 18. August 2023
www.cnlab.ch/herbsttagung

cnlab

Information. Technology. Research_

WORUM GEHT'S?

Kryptographie heute, morgen und übermorgen

Quantencomputer werden unsere Crypto brechen. Wie gefährlich ist das, und was kann man tun?

6. SEPTEMBER **13:00–17:00**

ab 13:00

Eintreffen der Gäste

13:30

Crypto heute

Was ist von Quanten-computern bedroht?

- Kryptographische Primitiven
- Symmetrische und asymmetrische Crypto
- Schwierige mathe-matische Probleme
- Algorithmen und Schlüssellängen

Zuzana Trubini

14:00

Computer von morgen

Was braucht ein Quantencomputer?

- Qubits
- Superposition und Verschränkung
- No-Cloning-Theorem
- Entwicklungsstand und Prognosen

Renato Renner

cnlab

Information. Technology. Research_

www.cnlab.ch/herbsttagung

14:25

Algorithmen von morgen

Wie funktioniert Shors Algorithmus?

- Konzepte
- Qubits, Register & Gates
- Schaltkreise
- Geschwindigkeit
- Andere Anwendungen

Stephan Verbücheln

14:50

Kaffee-Pause

15:20

Crypto morgen & übermorgen

Welche resistenten Verfahren gibt es?

- Postquanten-kryptographie (PQC)
- NIST Standards
- Quantum Key Distribution (QKD)

Urs Wagner
Martin Kaufmann

16:00

Fazit

Was heisst das jetzt?

- Vorbereitung & Planung
- Migration
- Kryptoagilität
- Hybride Lösungen

Paul Schöbi

16:15

Demos und Apéro

- Spielen mit Qubits
- Sprechstunden mit Experten
- Ein polarisierendes Experiment

cnlab

REFERENTEN

Christian Birchler
Geschäftsführer cnlab security AG. B. Sc. in Computer Science, CISA. Mehrjährige Erfahrung in der Überprüfung von sicherheitsrelevanten IT-Systemen. Aktueller Schwerpunkt: Sicherheit zentralisierter und verteilter IT-Systeme bei Finanzdienstleistern und Industrie-Unternehmen.

Paul Schöbi
cnlab security AG. Dipl. El. Ing. ETH, Promotion ETH (Dr. Sc. Techn.) auf dem Gebiet der Datensicherheit. Forschung, Entwicklung und Beratung im Bereich der IT-Sicherheit. Aktueller Schwerpunkt: Sicherheit zentralisierter und verteilter IT-Systeme im internationalen Bankenumfeld.

Stephan Verbücheln
cnlab security AG. Diplom-Informatiker. Aktuelle Schwerpunkte: Technische Sicherheitsexpertisen in der Kryptographie und Security-Reviews von Infrastruktur und Applikationen.

Zuzana Trubini
cnlab security AG. Dipl. Math ETH. Promotion ETH in theoretischer Informatik (Dr. Sc.). Aktuelle Schwerpunkte: Analyse und Design von sicherheitsrelevanten Konzepten, sicheres Onboarding, sichere Aktivierung und Authentisierung.

Urs Wagner
cnlab security AG. M. Sc. Math UZH. Promotion UZH (Dr. Sc. Nat.) im Bereich Kryptologie. Mehrjährige Erfahrung in der Beurteilung von kryptologischen Schutzfunktionen. Aktuelle Schwerpunkte: Analyse von sicherheitsrelevanten IT-Konzepten in der Finanzindustrie.

Stefan Kunz
cnlab security AG. M. Sc. in Informatik. Aktuelle Schwerpunkte: Technische Sicherheits-Expertisen und Security-Reviews von IT-Infrastrukturen und verteilten Anwendungen mit Fokus auf die Bereiche Web, Mobile und Kubernetes.

René Vogt
cnlab security AG. B. Sc. in Computer Science, MAS in Information Security. Fokus auf Security-Reviews von Netzwerken und Applikationen. Aktuelle Schwerpunkte: Mobile Security und Sicherheit von Internet- und Intranet-Technologien.

Martin Kaufmann
cnlab security AG. M. Sc. in Robotics, System & Control, ETH Zürich. Aktuelle Schwerpunkte: Analyse und Design von sicherheitsrelevanten IT-Konzepten, sichere Authentisierung und Autorisierung.

Pasqualino Casciano
cnlab security AG. B. Sc. Informatik, CISSP. Über 20 Jahre Erfahrung in der Software-Entwicklung und in der IT-Architektur (vorwiegend im Finanzsektor). Aktuelle Schwerpunkte: Analyse und Design von sicherheitsrelevanten IT-Konzepten.

Renato Renner
ETH Zürich, Professor für theoretische Physik und Leiter der Forschungsgruppe «Quantum Information Theory». Dipl. Phys. ETH, Promotion ETH in theoretischer Informatik (Dr. Sc.). Aktuelle Schwerpunkte: Quantum Information Science and Foundations of Quantum Physics.