

Quantum Technology Transfer Catalysers

How we Enable the Integration of Quantum Technology in Classical Infrastructures



QUANT-X SECURITY & CODING



BUSINESS STRUCTURE

Information Security Consulting

Customers: Critical infrastructure providers

Projects:

- Information and IT Security consulting for infrastructure migration and software engineering projects
- Focus on post-quantum cryptography integration and migration

R&D

Projects:

- Software development
- Security proof for photon-based QRNG

Area: (Post-)quantum secure identity access management

Current status: Prototyping



COMPANY INFO

- ❑ Family Business (GmbH)
- ❑ Bootstrapped in Hanover in 2019
- ❑ 7 employees and 1 permanent freelancer
- ❑ 4 ladies & 4 lads (employed since 2020/21)
- ❑ Main income from infosec consulting
- ❑ 1 R&D project - funded by the German Government





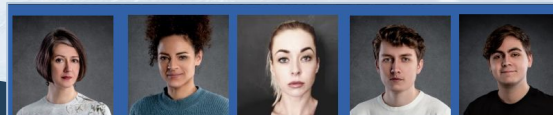
TEAM MENTALITY



#Team
#Office
#Safety



#Adventure



Quant-X (C)ERT

#Defense

<https://quant-x-sec.com>

consulting@quant-x-sec.com



THE QUANTUM THREAT

Evolving Quantum Computing technologies will make it possible to break currently used cryptography such as DH, RSA, Elliptic Curves and AES-128

Affected Infrastructure: All OSI layers, virtual networks, containers, databases, all applications using public key cryptography

Affected data: Data in transport, data in processing, data at rest

Affected network protocols: TLS, SSH, SFTP, VPN, etc.

Affected use cases: Communication, authentication, authorization, data integrity validation



THE THREAT Quantum Computing Capability

The Quantum-Threat-Timeline-Report estimates the risk of broken public-key cryptography in the next 4 years as follows:

- 30 of 37 experts expect the threat to be < 5%
- 6 of 37 experts believe it to be between 30% and 50%
- A single expert estimated the likelihood to be > 70%

Overall, there seems to be a non-negligible chance of an impactful surprise within what would be considered a very short-term future.

However, the scenario **“collect now, decrypt later”** applies in the past and NOW!



COUNTERMEASURES

Post-quantum cryptographic algorithms for encryption, key exchange and signatures

Software-based, flexible integration, less expensive, recommended by most security agencies

Quantum Communication including QKD for key exchange and QRNG for key generation

Hardware-based, restricted use cases, additional security properties





THE SOLUTION Post-Quantum Cryptography

Security of Post-Quantum cryptography is based on mathematics which is not efficiently solved by Quantum Computers.

Post-Quantum secure cryptosystems standards by the **NIST**, **ANSSI** and other agencies.

QKD devices often use Post-Quantum cryptography for authentication. Quantum Random Number Generators promise true randomness.

However, standardization activities are less advanced for QKD and QRNG protocols and devices.



$$\begin{aligned} p^{(1)}(x_1, \dots, x_n) &= \sum_{i=1}^n \sum_{j=i}^n p_{ij}^{(1)} \cdot x_i x_j + \sum_{i=1}^n p_i^{(1)} \cdot x_i + p_0^{(1)} \\ p^{(2)}(x_1, \dots, x_n) &= \sum_{i=1}^n \sum_{j=i}^n p_{ij}^{(2)} \cdot x_i x_j + \sum_{i=1}^n p_i^{(2)} \cdot x_i + p_0^{(2)} \\ &\vdots \\ p^{(m)}(x_1, \dots, x_n) &= \sum_{i=1}^n \sum_{j=i}^n p_{ij}^{(m)} \cdot x_i x_j + \sum_{i=1}^n p_i^{(m)} \cdot x_i + p_0^{(m)} \end{aligned}$$



COUNTERING THE QUANTUM THREAT



[Forschung](#) [Förderung](#) [Programme](#) [Projekte](#) [Konferenz 2025](#) [Service](#)

Projekte

Quant-ID

Quantensichere digitale Identitäten



Quantensichere Identifikation in digitalen Netzen.
© Adobe Stock / peach_adobe

MOTIVATION

Der Zugang zu Onlinediensten und Netzwerkdatenbanken wird mittels digitaler Identitäten geregelt. Um diese Identitäten sicher über das Netzwerk zu übertragen, werden sogenannte asymmetrische Verschlüsselungsverfahren genutzt. Zukünftig werden Quantencomputer aber in der Lage sein, diese klassischen Verschlüsselungsverfahren zu knacken. Unter dem Stichwort „Post-

PROJEKTINFORMATION

Verbundkoordinator
Quant-X Security & Coding, Hannover

Partner

- Fraunhofer IPMS, Dresden
- MTG AG, Darmstadt
- Universität Regensburg

Volumen
2,20 Mio. € (davon 85% Förderanteil durch BMBF)

Laufzeit
09/2022 - 08/2025

Bekanntmachung
Innovationshub für Quantenkommunikation

STAND DER PROJEKTDATEN

Angaben entsprechen dem Stand zum Zeitpunkt des Projektstartes.

<https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/quant-id>

The project Quant-ID is funded by the Federal Ministry of Education and Research under the grant number 16KISQ108K. Responsibility for the content of this publication is subject to Quant-ID.

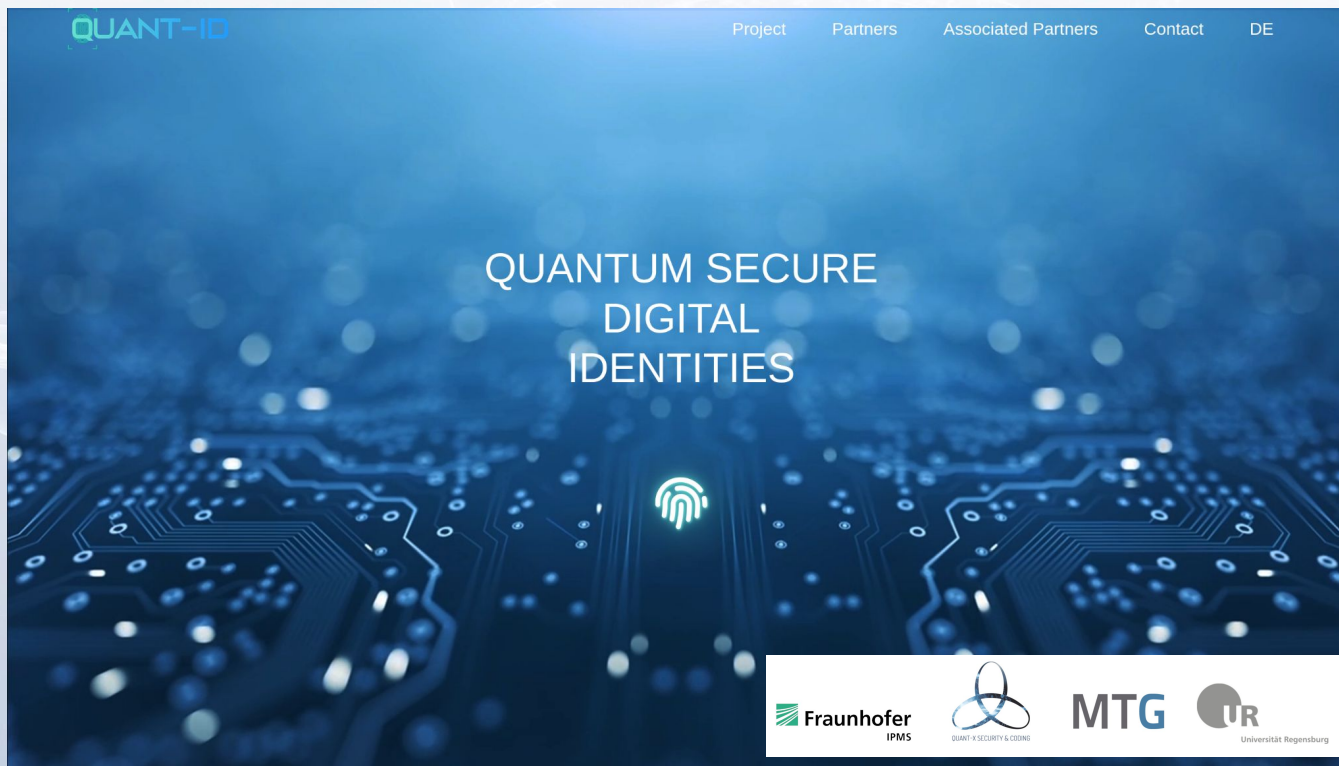
GEFÖRDERT VOM



Bundesministerium
für Bildung
und Forschung



COUNTERING THE QUANTUM THREAT



GEFÖRDERT VOM



Bundesministerium
für Bildung
und Forschung

The project Quant-ID is funded by the Federal Ministry of Education and Research under the grant number 16KISQ108K. Responsibility for the content of this publication is subject to Quant-ID.

<https://quant-id.de/>

<https://quant-x-sec.com>

consulting@quant-x-sec.com



WHY (POST-)QUANTUM SECURITY FOR IAM?



"QRNG Entropy and Post-Quantum Security for globally used IAM Protocols"

FACTS

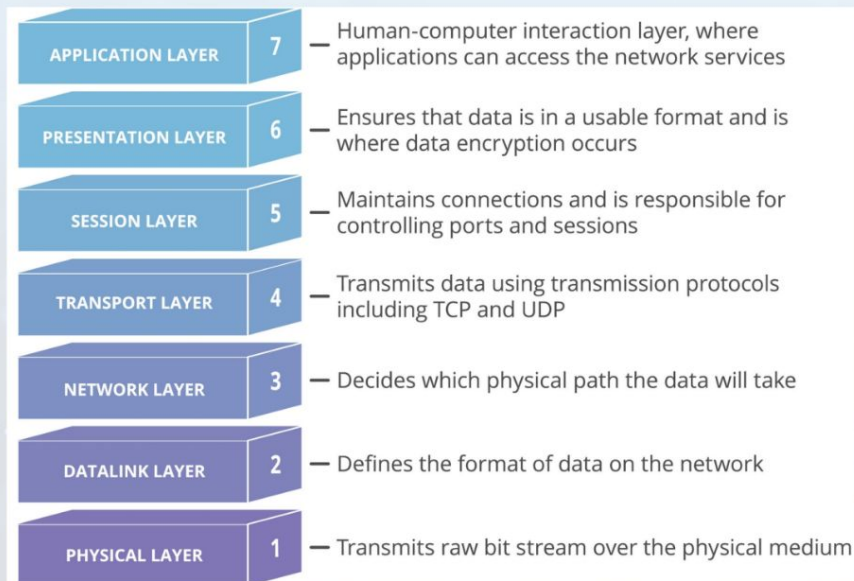
- Cloud and IOT → web protocols for Identity Access Management (IAM)
- Most cyber attacks are based on some identity misuse (person, device or application account)
- Cryptography is the backbone of IAM security!
- High Entropy is essential for access security!



Image Source: iStock



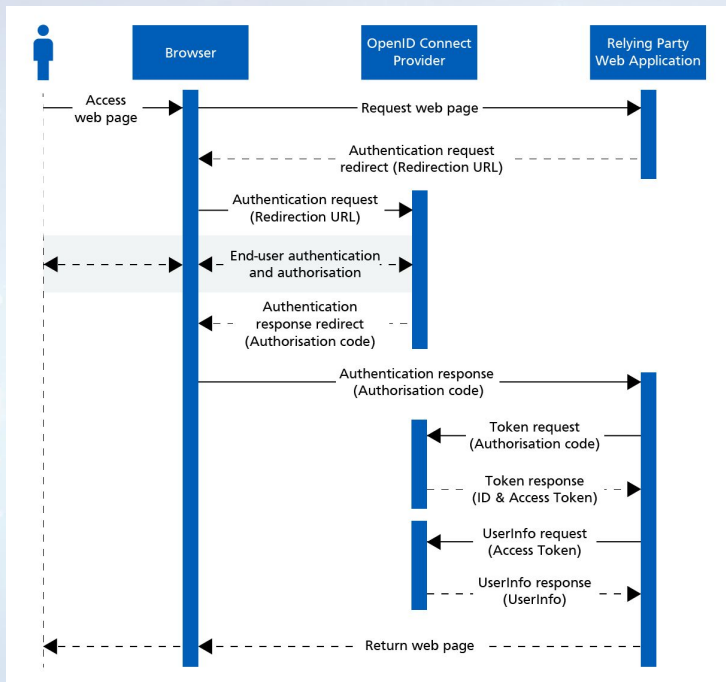
ENABLING QUANTUM TECHNOLOGIES IN CLASSICAL INFRASTRUCTURES



The project Quant-ID is funded by the Federal Ministry of Education and Research under the grant number 16KISQ108K. Responsibility for the content of this publication is subject to Quant-ID.



ENABLING QUANTUM TECHNOLOGIES IN CLASSICAL INFRASTRUCTURES



Source: UK National Health Service

- Login and authorization flows are complex
- Cryptography is the backbone of the security on network and application layer
- 8 x entropy in a simple authorization code flow access!
- QRNGs are theoretically truly random
- **Any RNG must be validated!**



VALIDATED QRNG FOR IDENTITY ACCESS

Gain-Switching in Phase Noise Quantum Random Number Generators: An Experimental and Stochastic Analysis

Mehrzaad Firoozi (Fraunhofer IPMS), Maximiliane Weishäupl (Universität Regensburg),
René Kirnbach (Fraunhofer IPMS), Fabian Klingmann (Fraunhofer IPMS)



Fraunhofer Institute for Photonic
Microsystems IPMS



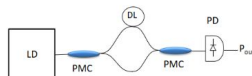
Universität Regensburg

1. Introduction We consider two new gain-switched (GS) phase-noise QRNGs and compare them with their continuous-wave (CW) counterparts. Alongside experiments, we conduct simulations which reveal parameters that influence the QRNG output. We analyze samples from each setup with statistical methods including the residual sum of squares and the min-entropy.

Notation

- LD: laser diode
- PMC: polarization maintaining coupler
- DL: delay line (1km for GS, 1m for CW)
- PD: photodetector

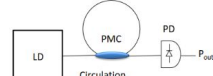
A: Standard phase-noise QRNG



$$P_{\text{out}} \propto \cos(\omega_0 T_d + \Delta\theta(t))$$

$\Delta\theta(t)$ = quantum phase noise of the LD, T_d = time delay difference between two arms, ω_0 = angular frequency of LD, β = gain of the optical field in the circulation, A = amplitude of the electric field, N = number of circulations, k = integer in $[1, N]$, $\delta\hat{X}_\varphi$ = fluctuation of the quadrature component of the LD's optical field, φ = optical phase shift applied by T_d

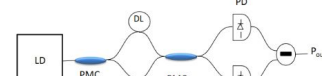
B: Phase-noise QRNG with a single beam splitter [1]



$$P_{\text{out}} \propto A^2 \sum_{k=1}^N \left(\frac{\beta}{2} \right)^{\frac{k}{2}} (-\cos(k\omega_0 T_d - \Delta\theta_{N-j}^{k-j})) +$$

$$A^2 \sum_{k=1}^N \left(\frac{\beta}{2} \right)^{\frac{k}{2}} \sum_{j=1}^{k-1} \left(\frac{\beta}{2} \right)^{\frac{j}{2}} \cos((k-j)\omega_0 T_d + \Delta\theta_{N-j}^{k-j})$$

C: Phase-noise QRNG with balanced detection



$$P_{\text{out}} \propto \frac{1}{2} A (\delta\hat{X}_\varphi(t - T_d) + \delta\hat{X}_\varphi(t))$$

(Note: For the GS variant of all three configurations, the laser is modulated by a signal generator and the DL is reduced.)



QUANTUM SECURE AUTHORIZATION

QUANT-ID

LOGIN

Email address

Password

[Forgot password?](#)

 **SUBMIT**

[New to Quant-ID?](#)

[CREATE ACCOUNT](#)



SCIENTIFIC ACTIVITIES

Investigation of open questions in Post-Quantum Security

Industrial Speaker for

Fachgruppe Computeralgebra

Co-Organisation of *Industrial Computeralgebra Conference with Focus Cryptography*

Memberships and Associations

Gesellschaft für Informatik



Deutsche Mathematiker-Vereinigung



European Mathematical Society



Quantum Business Network



European Quantum Flagship



CONTACT US



QUANT-X SECURITY & CODING

<https://quant-x-sec.com>

consulting@quant-x-sec.com