Validation of Photonic Quantum Devices

QUANT-X SECURITY & CODING

https://quant-x-sec.com

consulting@quant-x-sec.com

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 - fQuant-ID, which is funded by the German Government***

This slides are based on research within the tech transfer project https://quant-id.de/

TECHNOLOGY TRANSFER

QUANT-ID

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

https://quant-x-sec.com

consulting@quant-x-sec.com

THEORY & PRACTICE

Theory

Quantum theory promises true randomness for quantum mechanical systems

Use Cases:

- Quantum Random Number Generator (QRNG)
- Quantum Key Distribution (QKD)

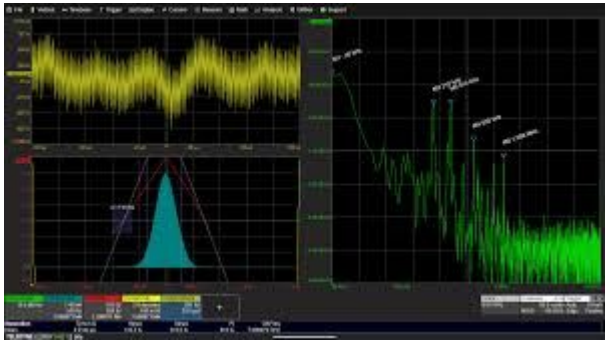
Practice

In practice, it is difficult to prove that a device is truly based on quantum mechanics alone.

There are both classical and quantum noise in an output of a device which is based on quantum mechanics.

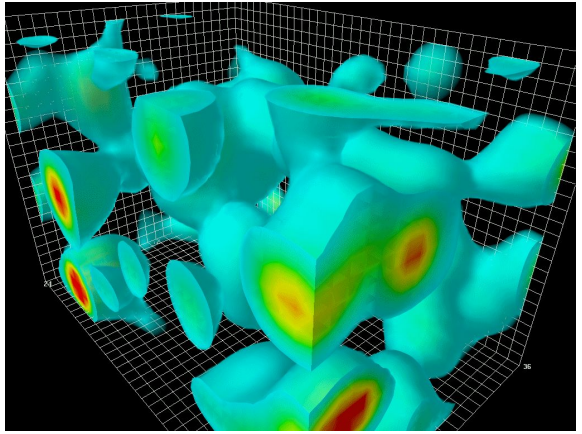
EVALUATED PHOTONIC SOURCES

Phase Noise



Source: [Clock Jitter & Phase Noise Measurement – Teledyne LeCroy]

Vacuum Fluctuations



Source: https://en.wikipedia.org/wiki/Quantum_fluctuation

QUANTUM MECHANICS

Physical Properties

- True Randomness (Unpredictability)
- Manipulation of the system is noticed

“Most of the currently used RNG devices are based upon deterministic processes and classical (deterministic) chaos, that is the generation of randomness is based upon classical physics laws. In this case, in PRNGs randomness is not true, but is fully dependent on the complexity of the system involved in the physical process of randomness generation and in principle can be predicted with sufficient knowledge of initial conditions regarding the physical system and computational power to simulate its behavior.”

Source: EITCI-QSG-EQRNG THEORETICAL CONCEPTS

WHY IS TRUE RANDOMNESS SO IMPORTANT?

Unpredictability of cryptographic systems is ensured by

Algorithm:

Pattern of the data transformation must not reveal any property of the cleartext

Cryptographic secret:

Must not be predictable! If it is predictable, the most secure algorithm does not help.
This applies to:

- Symmetric cryptographic keys
- Asymmetric cryptographic keys

QUANTUM SECURITY DEVICES IN USE

Established QKD networks all over the world

- China (QUESS)
- Austria (SECQC)
- Japan (Tokyo QKD Network)
- Switzerland (SwissQuantum)
- USA (DARPA)
- Many German and EUROPEAN technology transfer projects
  - SQuaD - Quantenkommunikation in Deutschland, umbrella project of QUANT-ID
  - The European Quantum Communication Infrastructure (EuroQCI) Initiative | Shaping Europe's digital future
- etc.

NEW QUANTUM SECURITY DEVICE VALIDATION

German and EUROPEAN technology transfer projects research open questions and methods to validate quantum devices.

Goals

- Measure the deviation of the devices in operation from the quantum theory
- Define standards for classification and certification (BSI, NIST, ETSI, …)

Involved Parties

- BSI (Federal Office for Information Security)
- Universities
- Industry

MINIMUM REQUIREMENTS FOR VALIDATION

- Current research results
- Current available requirements by the security agencies
- Practicality & Usability

Quantum engineers work closely with mathematicians and information security professionals. For a full security proof, a quantum theory expert is needed additionally.

Massive data validation is part of the research!

PROOF / DEVICE CLASSES a)

Device-dependent (practical) QRNGs, fully trusted and calibrated devices by implementation. Randomness of the output relies on the correct modeling and implementation of the physical quantum process.

Device-independent (Self-) Testing QRNGs. The output is tested for randomness due to a lack of confidence in the implementation of the physical process. Classic tests, but also, e.g. verification of the existence of quantum entanglement, by checking the statistical fracture of the so-called Bell inequalities can be combined. Here, we don't trust the source nor (AND) the measurement.

PROOF / DEVICE CLASSES b)

Semi device-independent (Semi-test) QRNGs. This category includes devices in which testing and implementation trust have been combined. This allows the modification of the parameters related to the randomization speed and confidence in the generated randomness. Some components in such a device are considered safe and trusted due to their exact characterization, others cannot be recognized as such and therefore randomization tests need to be performed. Here, we don't trust the source or (XOR) the measurement.

CONTACT US

QUANT-X SECURITY & CODING

https://quant-x-sec.com

consulting@quant-x-sec.com