Status Quo of Quantum Computing

Dr. Stavros Kousidis

Quantum Symposium, 25 March 2021
Information security

If a universal quantum computer pops up tomorrow.

Renders all currently deployed public-key cryptography useless
- RSA ('76), Diffie-Hellman ('76), ElGamal ('85), ECIES (2000)
- DSA (1991)
- ECC (since 1980s)

Nothing of the following remains
- Key exchange – „Store now decrypt later“
- Digital Signature
- Public-Key Encryption
Security level

Digital Computer

Age of Universe (in s)

Supercomputer

BSI Security level (VS-NfD)

RSA2048 AES128

Operations

Quantum computer

GHz

NIST Security level 1

RSA2048 AES128 AES256

Operations
Central question

Do we expect a quantum computer that – including overhead coming from error correction – can solve a GHz problem?
Development status of quantum computers

A BSI funded study: Available under www.bsi.bund.de/qcstudie

Extrapolation (2D-Transmons + Quantum error correction):

Quantum (elementary) operations für RSA2048 ≈ $10^{15} \approx 2^{30} \cdot 10^6$
It’s alive!

Quantum as a Service (QaaS)

- Amazon Braket
- Azure Quantum
- IBM Quantum (Experience), e.g. 65 Qubit ibmq_manhattan (NISQ-Device)
BSI’s positions

- Working hypothesis for high security applications: Cryptographically relevant Quantum Computers early 2030s

- Portfolio (BSI TR-02102-1):
  FrodoKEM, Classic McEliece, Hash-based Signatures

- Quantum Key Distribution:
  Only in hybrid mode with Post-Quantum Cryptography

- BSI-Recommendations “Migration zu Post-Quanten-Kryptografie’
Contact

Dr. Stavros Kousidis
Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189
53175 Bonn

Mobile: +49 (0) 151 61325086
E-Mail: stavros.kousidis@bsi.bund.de