Securing optical networks in the post-quantum world

Chris Janson
Nokia
June 2022
Agenda

1. Introductory context
2. Current cryptography and Quantum-safe security
3. Emerging standards
4. Secure optical transport
Quantum Mechanics

“ If you think you understand quantum mechanics, you don’t understand quantum mechanics. ”

Richard P. Feynman
Quantum vs. Classic Computing
Quantum Computing Benefits

- Chemistry
- Cryptography
- Material science
- Machine learning
- Optimization
- Big data
- Weather services
- Measurement
Quantum Computer Types

Analog Quantum Computer  Noisy Quantum Computer  Universal Quantum Computer
# Quantum Computing Race

Many countries have well defined quantum programs

<table>
<thead>
<tr>
<th>Country</th>
<th>Programs/Initiatives</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Canada</strong></td>
<td></td>
</tr>
</tbody>
</table>
| • National strategy established in 2016  
| • Canadian Space Agency Quantum Encryption and Science Satellite (QEYSSat) mission  
| • National Research Council of Canada’s Security and Disruptive Technologies Research Centre: Quantum Sensors and Security program |
| **China** |  |
| • Chinese Academy of Sciences Center for Excellence in Quantum Information and Quantum Physics  
| • Quantum Experiments at Space Scale (QUESS) project (the Micius satellite)  
| • Beijing-Shanghai Quantum Secure Communication Backbone  
| • National Quantum Laboratory—backed by a massive **US$10 billion** in funding over five years |
| **EU** |  |
| • EuroQCI Declaration  
| • QTEdu  
| • Quantum Industry Consortium  
| • QuantERA  
| • OpenQKD  
| • European Quantum Communication Infrastructure (EuroQCI) |
| **France** |  |
| • National Strategy for Quantum Technologies, with some **US$1.8 billion** promised the sector  
| • Grand Challenge on first-generation NISQ quantum accelerators |
| **Germany** |  |
| • National strategy established in 2018 with **US$3.1 billion** in fudging  
| • Quantum Technologies—From Basic Research to Market supports quantum technology research  
| • Grand Challenge competition in quantum communication  
| • QuNET Initiative set up in 2018 to develop a quantum network for secure data transmission between federal authorities |
| **Russia** |  |
| • Quantum Technologies Roadmap established in 2019 backed by **US$663 million** over five years  
| • National Quantum Laboratory |
| **UK** |  |
| • National Quantum Technologies Programme with **US$540 million** in funding for the first phase covering the period from 2014–2019, and **US$473 million** the second phase  
| • National Quantum Computing Centre  
| • Rigetti Computing, a leading quantum computing company, has partnered with the government and leads a consortium to develop the UK’s first quantum computer by 2023 |
| **US** |  |
| • National Quantum Initiative set up in 2018 with **US$1.275 billion** allocated  
| • National Quantum Coordination Office, part of the White House Office of Science and Technology Policy  
| • National Science Foundation, within it three Quantum Leap Challenges Institutes  
| • Quantum Foundry, a Center for Quantum Networks  
| • Five Quantum Information Science Centers backed by the DoE  
| • Quantum Economic Development Consortium (QED-C) |

Symmetric vs. Asymmetric Cryptography

**Symmetric Algorithms**
- Block ciphers (require chaining)
- Stream ciphers

**Symmetric Encryption**
The same key is used for encryption and decryption.

**Asymmetric (Public Key) Encryption**
The keys are different but are mathematically linked.

**Asymmetric Algorithms**
- Digital Signatures
- Key Agreement
- Public Key Encryption
- Key Encapsulation
Quantum Computing Impact on Today’s Cryptography
Some algorithms we rely on today will be completely broken

- **Shor’s** algorithm discovered in 1994 by Peter Shor that can find prime factors of an integer and find discrete logs
- **Grover’s** is a quantum search algorithm devised in 1996 by Lov Grover that improves search by a quadratic root factor

<table>
<thead>
<tr>
<th>Type</th>
<th>Algorithm</th>
<th>Key Length</th>
<th>Effective Key Length (Classic Computing)</th>
<th>Quantum Computing</th>
<th>Quantum Attack</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asymmetric</td>
<td>RSA-1024</td>
<td>1024 bits</td>
<td>80 bits</td>
<td></td>
<td>Shor’s</td>
</tr>
<tr>
<td>Asymmetric</td>
<td>RSA-2048</td>
<td>2048 bits</td>
<td>112 bits</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asymmetric</td>
<td>ECC-256</td>
<td>256 bits</td>
<td>128 bits</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asymmetric</td>
<td>ECC-384</td>
<td>384 bits</td>
<td>256 bits</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Symmetric</td>
<td>AES-128</td>
<td>128 bits</td>
<td>128 bits</td>
<td>64 bits</td>
<td>Grover’s</td>
</tr>
<tr>
<td>Symmetric</td>
<td>AES-256</td>
<td>256 bits</td>
<td>256 bits</td>
<td>128 bits</td>
<td></td>
</tr>
</tbody>
</table>
Quantum Acronyms
Not all technologies imply quantum-safe

Quantum Computing (QC)
Machines that use the properties of quantum physics to store data and perform computations

Quantum Random Number Generator (QRNG)
Quantum random number generators create randomness by measuring quantum processes

Quantum-safe Cryptography (QSC) / Post-quantum Cryptography (PQC)
Algorithms resistant to attacks by both classical and quantum computers because they are based on hard math problems for which an efficient solution using a quantum algorithm does not exist

Quantum Key Distribution (QKD)
Distribution using properties found in quantum physics to exchange cryptographic keys in such a way that is provable and guarantees security
“As the replacements for currently standardized public key algorithms are not yet ready, a focus on maintaining crypto agility is imperative. Until new quantum-resistant algorithms are standardized, agencies should continue to use the recommended algorithms currently specified in NIST standards.”

_NIST Report on Post-Quantum Cryptography, April 2016_
Types of Post-Quantum Cryptography

**Codes**
- Introduced by McEliece in 1978
- Relies on hardness of decoding unknown codes
- Very large public keys
- Fast encryption and decryption

**Lattices**
- First commercial version was NTRU (1996)
- Two most important hard problems:
  - Shortest Integer Solution (SIS)
  - Learning With Errors (LWE)
- Competitive key sizes and fast operations

**Multivariate**
- Introduced by Matsumoto and Imai in 1998
- Based on the fact that solving $n$ randomly chosen non-linear equations in $n$ variables is NP-complete
- Trade offs between key sizes and operation time

**Supersingular Isogenies**
- Introduced by Jao in 2009
- Relies on difficulty of finding isogenies (mappings) between Elliptic Curves
- Competitive key sizes, but slower operations
## Secure Optical Transport Options

<table>
<thead>
<tr>
<th></th>
<th>Handshake</th>
<th>Data Encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Authentication</td>
<td>Key Establishment</td>
</tr>
<tr>
<td>1</td>
<td>Classic</td>
<td>Asymmetric (RSA/ECDSA)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Quantum-vulnerable</td>
</tr>
<tr>
<td>2</td>
<td>Classic</td>
<td>Pre-shared Key</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Quantum-safe</td>
</tr>
<tr>
<td>3</td>
<td>Quantum Key</td>
<td>Pre-shared Key</td>
</tr>
<tr>
<td></td>
<td>Distribution (QKD)</td>
<td>Quantum-safe</td>
</tr>
<tr>
<td></td>
<td></td>
<td>or</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Asymmetric (Dilithium/Rainbow)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Quantum-safe but not standardized</td>
</tr>
<tr>
<td>4</td>
<td>Post-quantum</td>
<td>Asymmetric (Dilithium/Rainbow)</td>
</tr>
<tr>
<td></td>
<td>Cryptography (PQC)</td>
<td>Quantum-safe but not standardized</td>
</tr>
<tr>
<td>5</td>
<td>Hybrid</td>
<td>Asymmetric (RSA/ECDSA)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Quantum-vulnerable</td>
</tr>
<tr>
<td></td>
<td></td>
<td>+</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Asymmetric (KIBER/SIKE/McEliece)</td>
</tr>
</tbody>
</table>
Preparing for Quantum-safe Migration
Symmetric encryption and pre-shared keys are quantum-safe

Global government agencies will transition to quantum-safe algorithms

Until new algorithms are available, we need to rely on current algorithms

Existing safety mitigations:

- Use larger key sizes in encryption algorithms
- Use key agreement schemes that leverage large, symmetric, pre-shared keys
Summary
Quantum Computing & Quantum-safe Security

• Quantum computing is no longer a theoretical idea
• Billions are being invested around the world in quantum computer development
• It is possible we won’t immediately learn about the first universal quantum computer
• Governments indicate that systems will be migrated to a suite of algorithms to mitigate the quantum threat (QKD and QRNG are not the solution)
• Global standards bodies are working on new quantum-safe algorithms and new encryption protocol specifications
• Some information is already vulnerable today to the future quantum-threat
• While hybrid mechanisms using asymmetric cryptography can help mitigate the quantum threat, the only 100% certain approach is to use large symmetric encryption keys and key establishment schemes that rely on large pre-shared symmetric keys
Back-up materials
Threat to Encryption
Information we transmit today is already vulnerable

An encryption protocol session, like TLS, consists of the handshake and the data encryption part.

- **Handshake**
  - Authentication & Key Establishment
    - (both typically use asymmetric algorithms)
  - Best available attack is Shor’s
    - Breaks key establishment completely
    - Recover established encryption keys

- **Data Encryption**
  - Symmetric Encryption of Data
    - (uses keys established during handshake)
  - Best available attack is Grover’s
    - Cuts effective key length in half
Threat to Encryption vs Authentication
The threat might be different, but the migration urgency is the same

• While both asymmetric encryption and authentication are vulnerable to quantum-enabled attacks, the threats are different
• Asymmetric encryption used today to encrypt information makes this encrypted information already vulnerable to the harvest & decrypt attack
• In the case of authentication in encryption protocol, the authenticity of information is only useful during a very short time – during handshake to authenticate the key establishment keys
• In the case of authentication in document signing, the signatures can be invalidated and replaced with quantum-safe ones
• In the case of code signing, we really need to look at long-lived devices that are expected to last more than a decade and where replacing trust anchors can be challenging
Global Quantum-safe Cryptographic Standards
# NIST Round 3 PQC Algorithms

<table>
<thead>
<tr>
<th>Type</th>
<th>Name</th>
<th>Math</th>
</tr>
</thead>
<tbody>
<tr>
<td>Finalists</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Key Encapsulation</td>
<td>Classic McEliece</td>
<td>Codes</td>
</tr>
<tr>
<td></td>
<td>CRYSTALS-KYBER</td>
<td>Lattices</td>
</tr>
<tr>
<td></td>
<td>NTRU</td>
<td>Lattices</td>
</tr>
<tr>
<td></td>
<td>SABER</td>
<td>Lattices</td>
</tr>
<tr>
<td>Digital Signature</td>
<td>CRYSTALS-DILITHIUM</td>
<td>Lattices</td>
</tr>
<tr>
<td></td>
<td>FALCON</td>
<td>Lattices</td>
</tr>
<tr>
<td></td>
<td>Rainbow</td>
<td>Multivariate</td>
</tr>
<tr>
<td>Alternate Candidates</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Key Encapsulation</td>
<td>BIKE</td>
<td>Codes</td>
</tr>
<tr>
<td></td>
<td>FrodoKEM</td>
<td>Lattices</td>
</tr>
<tr>
<td></td>
<td>HQC</td>
<td>Codes</td>
</tr>
<tr>
<td></td>
<td>NTRU Prime</td>
<td>Lattices</td>
</tr>
<tr>
<td></td>
<td>SIKE</td>
<td>Supersingular Isogenies</td>
</tr>
<tr>
<td>Digital Signature</td>
<td>GeMSS</td>
<td>Multivariate</td>
</tr>
<tr>
<td></td>
<td>Picnic</td>
<td>Other</td>
</tr>
<tr>
<td></td>
<td>SPHINCS+</td>
<td>Stateless Hashes</td>
</tr>
</tbody>
</table>
Nokia Optical Encryption – NE Portfolio

Nokia supports AES encryption at L1 using 256-bit quantum-safe key sizes

Key Management: 1830 SMS

1830 PSS

1830 PSSx

1830 PSI

Clients

10G

10G

10G

10G

10G

40G

100G

40G

100G

100G

100G

100G

100G

200G

200G

200G

200G

200G

400G

400G

400G

400G

400G

600G

Future

2022

2023

© 2022 Nokia
Nokia Layer 1 Quantum-safe Key Management
Uses symmetric algorithms and pre-shared keys to ensure quantum safety

High-quality quantum-safe keys are generated in certified hardware and distributed via SNMPv3 (AES-256)