MDI-QKD, Quantum Internet, and QuTech

Joshua A Slater

www.qutech.nl
Quantum Internet

A Communication Network Exploiting the Quantum Properties of Light

I have an important document and I want to authenticate it.

I’m very important. I want to encrypt an entire message.

I’m a Quantum Computer, and I need to entangle with another Quantum Computer.

I want to process my quantum data in a quantum computer!!
Quantum Internet – Roadmap forward

A Communication Network Exploiting the Quantum Properties of Light

- Quantum Computing integrated with the Quantum Internet
- Quantum Memory
- Quantum Entanglement
- Multipoint-to-Multipoint Qubit Transmission
- Point-to-Point Qubit Transmission

Quantum Functionality

- Quantum Key Distribution (QKD) \((\text{with} \text{ end-to-end security})\)
  For Encryption, Authentication, etc. etc.
- Other Applications: Password Identification, Position Verification, and more.
- Quantum Key Distribution (QKD) \((\text{without} \text{ end-to-end security})\)
  for Encryption, Authentication, etc. etc.

Early Field Trials 2021

- Cluster Quantum Computing
- Blind Quantum Computing in a Quantum Cloud
- Quantum Repeaters

QuTech/Others
Quantum Internet – What can it bring?

A Communication Network Exploiting the Quantum Properties of Light

... for two distinct, but similar types of functionality

**First, Quantum Key Distribution (QKD) Networks**

- E2E distribution of Conventional Crypto Keys, via Quantum Key Distribution (QKD)
- Limited “Quantum-Distance” thus, Trusted Nodes
- Today’s Technology

**Second, Quantum Information Network (QIN)**

- E2E distribution of quantum entanglement, for Conventional Crypto keys **AND** Quantum Algorithms on Quantum Computers
- Unlimited “Quantum-Distance”, via Quantum Repeaters
- Very early field trials.
Quantum Networks emerging worldwide

Switzerland, South Korea, China, UK
• Commercial boxes for QKD exist; point-to-point, ~100 km max.
• Multi-hop networks require “trusted nodes”
• Generally seen as insufficiently secure

China
• QKD via trusted satellite
• 2000 km network using multi-hop ‘trusted nodes’ from Beijing to Shanghai

United States
• Quantum Xchange: 20-mile network, Wall Street to New Jersey
• Chicago area: 30-mile network

QKD / QI Networks are taking off soon

Europe
• Quantum Internet Alliance (QIA), and OpenQKD Consortium, building testbed networks
• The Quantum Communication Infrastructure (EuroQCI) Initiative

Quantum Xchange Launches “Phio” the First Commercial QKD Network for Quantum Communications in the U.S.
Quantum Network Applications

Secure a Data Connection Between Two Buildings

**Financial**
- Distribution of Master Keys
- Securing data to disaster recovery centers
- Secure storage of digital tokens

**Governmental**
- Encryption between ministries
- Secure document exchange
- Encryption to government data centers

**Data Centers and Interconnects**
- Encryption to/from cloud storage and computing centers
- Encryption through untrusted interconnects

**Critical Infrastructure**
- Encryption of data for remote monitoring
- Security on the control and/or management plane

**Telecommunications**
- QKD as a service
- Security for control and/or management plane
- 5G message authentication
- Data encryption at layer-1

**Enterprise Networks**

**Health Care**

**Vehicle-to-Everything**

**Intellectual Property Protection**
QuTech is a mission-driven institute that will develop scalable prototypes of a quantum internet... with local quantum processors enabling quantum computation.
• 2015: First time ever: entanglement experimentally and irrefutable proven
• 2018: First time entanglement “on demand” \( \rightarrow \) towards a true quantum internet!

December 2020
Inter-City Deployment Begins

2021
End-Points upgraded to quantum repeater
1) Introduction – Quantum Internet, QuTech

2) Quantum Key Distribution Boxes – What they look like? What they do?

3) Quantum Key Distribution Networks – What might they look like? What might they do?

4) Quantum Key Distribution Protocols – Why to consider MDI QKD
Quantum Key Distribution (in a nutshell):
1. Quantum Devices transmit/receive optical qubits over standard fiber
2. Received Qubits are detected immediately creating Quantum Data that be used as a Cryptographic Key
3. Any eavesdropping with signals on the fiber is detectable by the QKD devices
4. The QKD key can be used by classical symmetric encryptors/decryptors to encrypt/decrypt user data
QKD, what’s the box do?

1. Qubit Channel performs best on Dark Fiber
   - Operates up to a distance-limit
   - Coexisting WDM/Conventional signals decrease performance/operational distance of QKD

2. Quantum Control Channel for “Quantum-physics” control of certain hardware elements
   - Can be WDM with qubits, decreases performance

3. Conventional Control Channel to enable the network, deliver service request messages, etc.
   - Can be WDM with qubits, decreases performance
QKD, the Trusted Node

The Trusted Node – “Solving” the Distance-Limit

Concerns:
- Key is visible at the Center Node
- One must “Trust” every node along a long path
What is the Service?

A) Pure Quantum Hardware?
- Supply only Quantum Boxes
- Provide only quantum secret keys, via boxes
- Users responsible for key use, other security hardware/software, fiber, etc.

B) Dedicated Application Hardware?
- Provide Encryption with Quantum Keys?
- Supply Quantum boxes + Encryptors
- Users provide a network for transmission

C) Managed Service (MSP) ?
- Provide a Secure Communication Network
- Create dedicated physical network
- Users simply request service and send input data
Some Open Questions

**What type of Service to first offer?**
- Pure Quantum Hardware? Dedicated Application Hardware? Managed Services?

**Quantum Secret Key Rates?**
- Depends on the Use Case, what services are requested, and QoS agreements

**What does an SLA look like for Quantum?**
- Priority? QKD key lengths? Availability? Security parameters?
- Pair-wise defined

**Security Level?**
1) Introduction – Quantum Internet, QuTech

2) Quantum Key Distribution Boxes – What they look like? What they do?

3) Quantum Key Distribution Networks – What might they look like? What might they do?

4) Quantum Key Distribution Protocols – Why to consider MDI QKD
QKD; There are many Protocols

Many protocols exist:
BB84, BBM92, EB, MDI, CV, SARG, GG02, COW, DPS, etc. etc...

Many ways to compare them:

Near-Term Importance
• Technological Readiness Level
• Typical Key Rates
• Maximum Distance
• Security proof of the quantum protocol part
• Implementation Difficulty
• Point-to-Multipoint

Long-Term Importance
• Upgradability to QIN
• Susceptibility of hardware to attacks
QKD; There are many Protocols

Most QKD Protocols are point-to-point or requires “trusted node”
MDI-QKD

- Measurement-Device-Independent Quantum Key Distribution (MDI-QKD)

MDI, EB, BBM92: the potential answer to

Point-to-Multipoint
Upgradability to QIN
Susceptibility of hardware to attacks
MDI-QKD

Measurement-Device-Independent (MDI) QKD is Next-Gen QKD

MDI-QKD is more Practical
- MDI-QKD is inherently Networked in a Star network
- Users only need fiber link to Central Node
- Any pair of Users can create secret key

MDI-QKD is more Cost-Effective
- New Users can be added at anytime with a single connection
- Expensive Hardware is at Central Node
- Same Central Node is needed for Future Quantum Internet → MDI-QKD network is upgradable for the future

MDI-QKD is more Secure
- Central Node is not a trusted node.
- Central Node attacks physically cannot reveal key, nor reveal sensitive information. Best attack is a DoS.
- End-Points are send-only and not vulnerable to receiver attacks
MDI-QKD – Better Security

Measurement-Device-Independent (MDI) QKD is Next-Gen QKD

MDI-QKD is more Secure

- Central Node is not a trusted node.
- Central Node attacks physically cannot reveal key, nor reveal sensitive information. Best attack is a DoS.
- End-Points are send-only and not vulnerable to receiver attacks

Table 1 – List of attacks against a typical QKD system and respective countermeasures. The acronyms in the table are listed at the end of the paper.

<table>
<thead>
<tr>
<th>SECURITY ISSUE</th>
<th>DESCRIPTION</th>
<th>COUNTERMEASURES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trojan-horse attack</td>
<td>Eve probes the QKD equipment with light to gain information about the device settings</td>
<td>privacy amplification (PA), isolators, filters</td>
</tr>
<tr>
<td>Multi-photon emission</td>
<td>When more than one photon is emitted in a pulse, information is redundantly encoded on multiple photons</td>
<td>PA, characterisation, decoy states, SARG04 and other protocols</td>
</tr>
<tr>
<td>Imperfect encoding</td>
<td>Initial states do not conform to the protocol</td>
<td>PA, characterisation</td>
</tr>
<tr>
<td>Phase correlation</td>
<td>Non-phase-randomised pulses leak more info to Eve, decoy states fail</td>
<td>phase randomisation, PA</td>
</tr>
<tr>
<td>Bright-light attack</td>
<td>Eve manipulates the photon detectors by sending bright-light to them</td>
<td>active monitoring, measurement device independent QKD (MDI-QKD)</td>
</tr>
<tr>
<td>Efficiency mismatch</td>
<td>Eve can control, at least partially, which detector is to click, gaining information on the encoded bit</td>
<td>MDI-QKD, detector symmetrisation</td>
</tr>
<tr>
<td>and time-shift attack</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Back-flash attack</td>
<td>Eve can learn which detector clicked and hence knows the bit</td>
<td>isolators, MDI-QKD, detector symmetrisation</td>
</tr>
</tbody>
</table>

**Measurement-Device-Independent (MDI) QKD is Next-Gen QKD**

**Upgradability to QIN**
- QIN does Entanglement generation, swapping, teleportation
- Quantum Repeaters not available yet, BUT
  - They require Mid-Point stations, identical to MDI Central Node!

### Physical Network Building: Consider the end Goal: QIN
- Midpoint stations needed
- Asymmetric links degrades performance quickly...
1) Introduction – Quantum Internet, QuTech

2) Quantum Key Distribution Boxes – What they look like? What they do?

3) Quantum Key Distribution Networks – What might they look like? What might they do?

4) Quantum Key Distribution Protocols – Why to consider MDI QKD
Quantum Internet – Top 7 Facts!!

1) Quantum Internet will use quantum-technology to provide quantum-services to Users.

2) Quantum will not replace conventional networks; only supplement with new functionality.

3) Communication channels will be Optical (fiber, free-space, satellites, etc.)

4) Fibers will be used for Quantum Internet
   • Low enough loss for Quantum (<30 dB), with no conventional active elements

5) Quantum Boxes can be made 19’’ rack compatible
   • QuTech and others do it

6) Infrastructure locations will be responsible for support, and own security
   • Energy, cooling, access controls, logging, etc. etc.
   • Specialized dry-cryo cooling? Compressed gasses?

7) Redundancy can be built into the network
   • Though, best techniques haven’t been explored

8) There is a lot of uncertainty still
   • Who’s going to build hardware? Where do we lay down? How much will governments control? Who’s going to invest? How do we get to QIN?
The High-Level Network View – 2 Years

Metro-Scale Chains?

- Metropolitan-Scale Chains
- A few per continent likely
- Focus on developing know-how with Operational Deployment

Composed of:
- High-Bandwidth Super-Users
- Super-Users Acting as Trusted Nodes
- Nearby Users (low-bandwidth or non-quantum) accessing a “backbone”
The High-Level Network View – 5 Years

A Metro-Network

- Metropolitan-Scale Networks, few per continent
- Still developing Operational Deployment
- Further professionalization of hardware, of service, of network designs/management

And then more Metro-Networks

(SDN?) Network Controllers
The High-Level Network View – 10 Years

Connected Metro-Networks

- Long-distance backbone of Trusted nodes
- Agreements between networks
- Nearly whole continent covered (if desired)
- Different Security Levels, Services offered

(SDN?) Network Controllers
The High-Level Network View – 15 Years

Close, but Separate Networks, and slowly QIN

• Multiple Metro-Scale Networks nearby
• IXs start to appear
• First professionalized QIN networks coming on-line

• In 20 years, all long-distance trusted nodes replaced with quantum repeaters
  • Maybe Space plays a role
Some Open Questions

WDM Multiplexing or Dark Fiber?
  • Optimize fiber-use or optimize Quantum performance?

Is Point-to-Point sufficient medium term? Or Point-to-Multipoint needed sooner?

Are Trusted Nodes allowed?
  • Certainly required in some situations...
  • Users & Governments likely to decide. Protection measures needed.

Enrollment into the quantum network?
  • We want to avoid vendor-lock in
  • Can anyone connect to Exchanges?
  • Usage by suspicious actors?

Lawful Interception?
Take aways

• Quantum Key Distribution for now, and Full Quantum Internet will come later

• QuTech’s Dutch Network starts up next month, upgrading to early repeaters next year

• Open Questions in Service to Offer, WDMs, Trusted Nodes, and Network Management

• Many QKD protocols exist, each with benefits and drawbacks
  • MDI-QKD for better security, upgradability, cost-scaling

• We should design the physical topology correctly now, so QIN can come easily later.

Thank you!