Building quantum networks at the local area scale

Qline: A quantum communication architecture by VeriQloud
About VeriQloud

Josh Nunn
University of Bath

Marc Kaplan
VeriQloud

Elham Kashefi
Sorbonne University
University of Edinburgh

- Located in Paris, France
- Quantum networks: architecture, software and application
- Current networks: QKD
- Future networks: toward a quantum internet
- Secure quantum cloud computing
Fundings and ecosystem

Support from french Institutions
DGA (French Darpa), BPI (Public investment bank)

Customers

Research projects

Networks
Qline: A quantum communication architecture

Josh Nunn
University of Bath

Marc Kaplan
VeriQloud

Elham Kashefi
Sorbonne University
University of Edinburgh

Georg Harder
VeriQloud

Anne Marin
VeriQloud

Mina Doosti
University of Edinburgh
Quantum networks around the world

EuroQCI Project

US Quantum Internet
Advantages of quantum key distribution

- Unconditional / Everlasting security implies Long-term security for classified, genomic, energy, healthcare, industry, finance…
- Key distribution for symmetric cryptography (AES)
- Prevents « store now, break later » attacks (Data Harvesting)
- Current encryption is vulnerable to future technical progresses and scientific breakthrough, QKD is not

With quantum key distribution (QKD), quantum networks provide unconditional security.

Main issue: scaling these networks with current technologies is expensive and injects vulnerabilities with trusted nodes
Qline: the quantum ethernet, by VeriQloud

- Fully-connected quantum communication infrastructure
- Trusted-node free
- Scalable with standard telecom components
- Can connect quantum computers in the future

A full-stack solution for quantum cybersecurity at the local-area scale
Qline: the quantum ethernet, by VeriQloud

1. The Qline Protocol
2. Security of Qline in theory and practice
3. Today’s use-cases
4. Future developments
The Qline Protocol

Standard QKD

|φ⟩ = H^r X^a |0⟩

|0⟩

|φ⟩ = H^s |φ⟩

a if r = s

Qline

|0⟩

|φ⟩ = H^r X^a |0⟩

|φ⟩ = H^s |φ⟩

a if r = s
The Qline Protocol

Standard QKD

\[ |0\rangle \]

\[ |\phi\rangle = H^r X^a |0\rangle \]

\[ H^s |\phi\rangle \]

a if \( r = s \)

Qline

\[ |0\rangle \]

\[ |\phi\rangle = H^r X^a |0\rangle \]

\[ X^b H^s |\phi\rangle \]

a \( \oplus \) b if \( r = s \)
The Qline Protocol

Standard QKD

\[|\phi\rangle = H^r X^a |0\rangle\]

\[H^s |\phi\rangle\]

\[a \text{ if } r = s\]

Qline

\[|\phi\rangle = H^r X^a |0\rangle\]

\[X^b H^s |\phi\rangle\]

\[a \oplus b \text{ if } r = s\]
The Qline Protocol

Standard QKD

|0⟩

|φ⟩ = H^r X^a |0⟩

H^s |φ⟩

a if r = s

Qline

|ψ⟩

|φ⟩ = H^r X^a |0⟩

X^b H^s |φ⟩

a ⊕ b if r = s

Up to corrections after ψ is revealed

Randomness injection
The Qline Protocol

Qline vs QKD

Standard QKD

Trusted nodes
Qline vs QKD performances

Key establishment with QKD

Quantum Key Establishment
(Primary keys)

Classical Key Routing
(Derived keys)
Consumes Primary Keys

<table>
<thead>
<tr>
<th></th>
<th>A&amp;C1</th>
<th>C1&amp;C2</th>
<th>C2&amp;B</th>
</tr>
</thead>
<tbody>
<tr>
<td>QKD</td>
<td>QKD</td>
<td>QKD</td>
<td>QKD</td>
</tr>
</tbody>
</table>

A&C1
C1&C2
C2&B
Qline vs QKD performances

Key establishment with Qline

No key routing
No Trusted nodes

Under the following assumptions
- Keys are uniformly distributed among pairs of nodes
- The cost is dominated by the one of detectors

The price-per-bit of keys is the same with QKD and Qline
The security of Qline (Theory)

Standard QKD

Composable security from
A largely self-contained and complete security proof for quantum key distribution
Marco Tomamichel and Anthony Leverrier
Quantum 1, 14 (2017).

Qline

Our goal
Show that an attack on Qline implies an attack on standard QKD
The security of Qline (Theory)

An eavesdropper « sees » the same state at all those points.

Extracting information in Qline is the same as extracting information in QKD
Side-channel attacks on Qline

- QKD Side-channels: Same as QKD
- Trojan Horse: Power-monitoring
- Photon counting: Work in progress
Application: last-kilometer of quantum networks

Qline as the base of metropolitan infrastructures
OpenQKD with Deutsche Telekom
Application: secure storage

Quantum communication protects against data interception

Classical cryptography protects against data leakage

Continuous re-encryption and share redistribution

Computation on shares

Qline: No trusted nodes = less vulnerabilities
Goal: Establish a shared key between N1 and N2
Problem: Who operates the trusted node?
Application: QKD Network interconnection with Qline

Two Qlines can route two independent keys from N1 to N2. None on the intermediate nodes is a trusted node.
Two Qlines can route two independent keys from N1 to N2. None on the intermediate nodes is a trusted node.
Interlude: Verifiable blind quantum computing

The light client delegates a quantum computation to a distant server with the following guarantees:

➡ **Blindness**: the server does not learn anything.

➡ **Verifiability**: any deviation from the original computation will be detected.
Application: Secure quantum cloud computing

- A scalable architecture for secure quantum cloud computing
- Applications to secure distributed quantum computing
Conclusion Qline: the quantum ethernet

➡️ Fully-connected quantum communication infrastructure with performance similar to QKD
➡️ Secure and scalable
➡️ Composable security, security against side-channel attacks
➡️ Application to quantum networks, and secure storage
➡️ A scalable and secure architecture for secure quantum cloud computing
Toward a quantum internet

Secure communication

Secure storage

Secure classical cloud

Secure quantum cloud

Making quantum cybersecurity feasible