Threats to quantum cryptography in presence of losses

Davide Li Calsi, Paul Kohl, JinHyeock Choi and Janis Nötzel

Arbeitsgruppe Theoretisches Quantensystemdesign (TQSD)
Lehrstuhl für Theoretische Informationstechnik (LTI)
Technische Universität München (TUM)

November 7, 2023
• Theoretical Quantum Systems Design (TQSD)
  • Research activities

• Problems of direct transmission
  • Qubit, transmission and transducer limit

• Quantum crypto background
  • Public key, authentication, oblivious transfer

• Vulnerabilities
  • Public key, authentication, oblivious transfer

• Mitigation
  • Quantum teleportation via entanglement distribution
Theoretical Quantum Systems Design (TQSD)

- Working group in Technische Universität München (TUM) for theoretical foundations of quantum system design.

- Research agenda
  - Emulation of future hybrid quantum communication networks.
  - Quantum system design, in particular the interaction of the different resources that can be used for high data rates and reliable communication.
  - Investigating new potential use cases enabled by adding quantum communication resources, especially, entanglement-assisted communication.
  - Secure message transmission over quantum channels.
TQSD current projects

• Q.TOK
  • Quantum token-based authentication and secure data storage
  • In collaboration with 7 memory projects in Grand Challenge of Quantum Communication.

• QD-CamNetz
  • Working on a quantum internet demonstrator with three nodes
  • Joint project with TU Dresden

• QuaPhySI
  • Investigating quantum technologies for Physical Layer Service Integration
  • and more
Qubit limits

• Constraints from quantum mechanics
  • No measurement without state alteration
  • No cloning
  • No copy and retransmission.

• The sender may not know the qubit to send.
  • For BB84 QKD, the sender may know the qubit state.
  • For quantum money, the owner can’t know.

• Sometimes nobody knows the qubit state.
  • E.g. QPUF-based quantum token.
  • Prevents malicious cloning but the loss from a link failure is irrevocable.
Transmission Limits: Losses & Absorption

- Losses due to bending
- Impurities, splicing, and connections lead to absorption/scattering
- Intrinsic absorption in every material
- Dependent on implementation, absorption may effect qubit loss in transmission
Transmission Limits: Absorption

- e.g. Absorption in standard SiO$_2$ fibres
Transmission Limits: Dispersion and Broadening Effects

- Wavelength dependency of refractive index/propagation speed

- In reality nonzero spectral linewidth of signal pulse (thermal & intrinsic effects)

- Thus temporal broadening of pulses

- Wavelength dependency of optical hardware may lead to loss

- Degraded indistinguishability of photons => failure rate of quantum operations
Transduction Limits

• Losses in conversion from flying to stationary qubit

• Highly dependent on implementation

• Most often light-matter interaction

• Described by cavity quantum electrodynamics (QED)

• Two-level system (TLS) in resonator cavity as stationary qubit

• Light entering cavity as flying qubit
Crypto background

- Public-key encryption and digital signature
- Identity Authentication
- 1-2 Oblivious Transfer: Alice has two messages \{m_0, m_1\}, Bob chooses one to receive. They DO NOT TRUST each other
  - Alice cannot guess Bob’s choice
  - Bob cannot learn the other message
Vulnerability: Public-key encryption

• Public-key scheme, based on qubit rotations*
  • classical message encrypted through a quantum public key
  • yields a quantum ciphertext
  • receiver decrypts via a classical private key

• Key-pair generation
  • Example (using 4-bits numbers):
    • private_key = { 7, 1, 2, 12} (random)
    • Consider angles {7/16 *Pi, 1/16 *Pi, 2/16 *Pi, 12/16 *Pi}
    • Get 4 qubits in |0> state, rotate them by the above angles

• Encryption
  • Rotate public-key qubits by 0 or Pi

• Decryption
  • Apply inverse (w.r.t key-gen phase) rotations

Vulnerability: Public-key encryption and digital signature

- Problems of quantum keys
  - with enough copies, adversaries can learn the private key
  - receiver must make sure there is a limited number of copies at all times
  - what if a public key is lost? (while encrypting, while sending it…)

<table>
<thead>
<tr>
<th>Reality: Benign Loss</th>
<th>Assumed: Benign Loss</th>
<th>Assumed: Malicious Steal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Receiver re-sends the key to the honest user who lost it</td>
<td></td>
<td>Receiver refuses retransmission, honest user can no longer send an encrypted message</td>
</tr>
<tr>
<td>Reality: Malicious Steal</td>
<td>Attackers gain more copies of the key, and later leak the private key</td>
<td>Receiver refused retransmission, successfully prevents an attack</td>
</tr>
</tbody>
</table>
Vulnerability: Public-key encryption and digital signature

• Similar problem in quantum digital signature scheme by Gottesman and Chuang*
• Other protocols under investigation

Consider (a simplified version of) this protocol by Hong et al*.

- Alice and Bob **pre-share a classical key**
- Alice maps every two bits of her key to one of the BB84 states
  \{ |0>, |1>, |+>, |-> \}
- Bob measures and compares according to his bits
- **Example**

**Vulnerability: Authentication**

- Multiple copies of the same qubit leak the corresponding key
- what if a qubit is lost?

<table>
<thead>
<tr>
<th>Reality: Benign Loss</th>
<th>Assumed: Benign Loss</th>
<th>Assumed: Malicious Steal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice resends the qubit to Bob, who can verify her key</td>
<td>Alice will not allow Bob to verify her identity, authentication failed</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Reality: Malicious Steal</th>
<th>Assumed: Malicious Steal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attackers gain more copies of the qubit, and later leak the private key bit</td>
<td>Alice avoids an attack</td>
</tr>
</tbody>
</table>
Vulnerability: Oblivious transfer

- BBCS* protocol implements secure OT
- Alice and Bob start a BB84 key exchange

\[ \text{RandBits()} = 0, 1, 1 \]

- The rest is classical post-processing and communication
- Bob didn't guess some bases in some positions, won't learn both messages

Vulnerability: Oblivious transfer

• What if the qubits are lost?

<table>
<thead>
<tr>
<th>Reality: Benign Loss</th>
<th>Assumed: Benign Loss</th>
<th>Assumed: Malicious Claim</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice resends the qubits to Bob, so that the protocol may continue</td>
<td>Alice will not resend the qubits, threatening the protocol’s correctness.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Reality: Malicious Claim</th>
<th>Assumed: Benign Loss</th>
<th>Assumed: Malicious Claim</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bob gains more copies of the qubits, possibly learning corresponding key bits</td>
<td>Alice avoids an attack by Bob trying to guess both messages</td>
<td></td>
</tr>
</tbody>
</table>

• Fortunately, there is a simple mitigation
  • Alice just replaces lost qubits with new random qubits (random value and basis)
  • Negligible overhead, preserves security
Mitigations

• Some protocols are inherently immune
  • BBCS for OT, Kanamori et al*’s authentication
• For some protocols, teleportation mitigates the threat
  • Error happens when sharing entanglement -> still recoverable
  • Following the procedure suggested in RFC9340
• Use of decoy states
  • First proposed by Hwang* for QKD
  • Hong et al. propose their use to detect eavesdroppers.
  • Active adversaries are still a threat, requires information on the channel


Thanks for your attention.
Transduction Limits

• System dynamics described via:

  • **Emitter decay rate** $\gamma$: TLS decay in the cavity mode, approx. by lifetime $\tau$ of TLS excited state via $\gamma \approx 1/\tau$

  • **Cavity loss rate** $\kappa$: rate of photons exiting cavity, depends on quality factor $Q$ of resonator via $\kappa \propto 1/Q$

  • **Coupling strength** $g_0$ *between TLS and photon*, depends on mode volume $V_0$ of resonator: $g_0 \propto \sqrt{1/V_0}$.

• Different cavity designs with different $Q$ and $V_0$, like micropillars or photonic crystals, etc.

• Different TLS like quantum dots (QD), vacancy centres, etc.
Crypto Primitives

- **Public-key crypto**: generate a public and private key
  - Anybody can **use the public key to encrypt** a message
  - Only you can **use the private key to decrypt** it
- **Digital signature**: generate a public and private key
  - Only you can **sign a message** with your **private key**
  - Anybody can **verify** your signature with the **public key**
Retransmissions in classical communication

• Messages are lost in modern telecom
• **TCP/IP** stack designed to tolerate losses
• Classically, the solution is simple: **retransmit**
  • Before sending a message, always duplicate it
  • Send the copy, keep original for later retransmissions
• In TCP, receivers send **ACKs** for each packet
  • If no ACK is received for one packet, retransmit
• No threat to classical cryptography
  • Classical information is copyable
  • Computational hardness is not affected
Rotations used in public-key scheme

Rotation by angle $x$ around the $y$ axis: $R(x)$

$$R(x) = \exp\{-ix * Y/2\}$$

Operator $Y=i(|1><0|-|0><1|)$

Maps $|0>$ into $\cos(x/2) |0> + \sin(x/2) |1>$