Securing Practical Quantum Cryptography with Optical Power Limiters

Gong Zhang¹,*, Ignatius William Primaatmaja², Jing Yan Haw¹, Xiao Gong¹, Chao Wang¹,†, and Charles C.-W. Lim¹,²,‡

*zhanggong@nus.edu.sg †wang.chao@nus.edu.sg ‡charles.lim@nus.edu.sg

¹Department of Electrical & Computer Engineering, National University of Singapore, Singapore
²Centre for Quantum Technologies, National University of Singapore, Singapore
Outline

- Background
  - Importance of power limiter in quantum cryptography
  - Introduction of thermo-optic defocusing
- Experimental and simulation results
- Possible attack consideration
- Application in plug-and-play MDI-QKD
- Conclusion
# Hacking Practical QKD

<table>
<thead>
<tr>
<th>Attack Type</th>
<th>Authors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detector-blinding attack</td>
<td>Makarov 2009, Lydersen 2010</td>
</tr>
<tr>
<td>Receiver laser damage attack</td>
<td>Bugge 2014, Makarov 2016</td>
</tr>
<tr>
<td>Time-shift attack</td>
<td>Qi 2007, Zhao 2008</td>
</tr>
<tr>
<td>Wavelength attack</td>
<td>Huang 2013, Li 2011</td>
</tr>
<tr>
<td>Back-flash attack</td>
<td>Kurtsiefer 2001</td>
</tr>
<tr>
<td>Channel calibration</td>
<td>Jain 2011</td>
</tr>
<tr>
<td>Detector deadtime</td>
<td>Weier 2011</td>
</tr>
<tr>
<td>Spatial efficiency mismatch</td>
<td>Rau 2015, Sajeed 2015</td>
</tr>
<tr>
<td>Trojan-horse attack</td>
<td>Gisin 2006, Jain 2014</td>
</tr>
<tr>
<td>Intensity information</td>
<td>Jiang 2012</td>
</tr>
<tr>
<td>Modulation pattern effect</td>
<td>Yoshino 2016</td>
</tr>
<tr>
<td>Source laser damage attack</td>
<td>Huang 2020</td>
</tr>
<tr>
<td>Phase-remapping attack</td>
<td>Fung 2007, Xu 2010</td>
</tr>
<tr>
<td>Phase information</td>
<td>Sun 2012, 2015, Tang 2013</td>
</tr>
</tbody>
</table>

**Solution**

Measurement-device-independent MDI-QKD

**Target:** Receiver

**Target:** Source

---

Trojan-Horse Attack

Current countermeasures

• Phase randomize (Reduce $I_{eve}$)
• Watchdog detector (Can be bypassed)
• Passive components such as isolators (Limited degree-of-freedom, one-way application only, high isolation)

Basic idea is to limit the amount of unauthorized input power.


• Bound on the mean energy is one way to provide a practical Semi-Device-Independent (Semi-DI) framework.

• Use energy bound to bound the overlap between the prepared states.

• Energy bound could lead to certifiable quantum randomness.

Again, a power limiting device is important here!
Proposal: Quantum Optical Fuse / Power limiter

The device should ideally have the following properties:

- Provides a **reliable and characterizable** power limiting threshold (in the order of a few photons to hundreds of photons).
- If the input energy exceeds the threshold, the device will stop the communication channel.
- **Cost-effective, passive, and easily replaceable.**
- Power limiting effects are **independent of other degree of freedoms**, e.g., frequency, polarization, etc.

It is **timely to develop such devices**, for we now have **a wide range of security proof methods with possible energy constraints features**:

Review of Optical Power Limiter

Fiber damage
- 10^2 – 10^3 mW level

Filter based
- Using thermo-optic effect or optical force to tune the filter center wavelength
- Narrow operation bandwidth, limited extinction ratio
- 10 – 10^2 mW level

Nonlinear effect
- 10 – 10^3 mW level

Two-photon absorption
- 10 – 10^3 mW level

Thermo-optical defocusing
- 10 – 10^2 mW level

Fig. 1. Schematic illustration of TPA in silicon. (a) degenerate TPA, (b) non-degenerate TPA.
Our Choice: Thermo-Optical Defocusing

- Negative thermo-optic coefficient of acrylic: $\frac{dn}{dT} = -1.3 \times 10^{-4} \text{ K}^{-1}$
- Higher absorbed power diverges the input light more
- A tunable diaphragm controls the received power
- Robust and stable performance, compact and cost-effective design
Our Choice: Thermo-Optical Defocusing

- Negative thermo-optic coefficient of acrylic: \( \frac{dn}{dT} = -1.3 \times 10^{-4} \text{ } K^{-1} \)
- Higher absorbed power diverges the input light more
- A tunable diaphragm controls the received power
- Robust and stable performance, compact and cost-effective design

Patent filed: SG Non-Provisional Application No.10202006635S
**Theoretical Modeling**

- Angular divergence of a paraxial light ray passing through a refractive index gradient

\[
\frac{\partial \theta_r}{\partial z} = \frac{1}{n} \left( \frac{\partial n}{\partial T} \right) \left( \frac{\partial T}{\partial r} \right)
\]

- Absorbed laser power \( I \) is balanced with the heat transfer mechanism (Assume heat transfer in \( r \)-direction only)

\[
\alpha I = -\frac{k \partial}{r \partial r} \left( r \frac{\partial T}{\partial r} \right)
\]

- Laser intensity at position \((r, z)\)

\[
I(r, z) = I(r, 0) \cdot \exp \left( -\alpha z + \frac{\partial n}{\partial T} Pe^{-\frac{r^2}{a^2}} \left( z - \frac{1}{\alpha} (1 - e^{-\alpha z}) \right) \right) / \pi kna^2
\]

- COMSOL simulation

Input-Output Power Relationship

Prism length

- Output Power (dBm)
- Input Power (dBm)
- Prism length (cm)
- Maximum Output Power
- Fiber damage threshold

Diaphragm width

- Output Power (dBm)
- Input Power (dBm)
- Diaphragm width (mm)
- Maximum Output Power
- Fiber damage threshold

Response Time Consideration

![Graph showing response time consideration with different output powers and input powers. Graphs illustrate shorter pulse leading to higher output power.]

**Simulation Results**

**Experimental Results**

Shorter pulse → Higher output power
Assume 20 mW average input power (Based on prior experiment)

Pulsed input experiences greater power-limiting effect comparing to the continuous-wave cases
Wavelength Dependence

Thermo-optic coefficient

\[
TOC = \frac{dn}{dT} = \frac{(n^2 - 1)(n^2 + 2)}{6n} (\Phi - \beta)
\]

- Electronic polarizability \( \Phi > 0 \) typically
- Volumetric expansion \( \beta \) is dominant in polymer

<table>
<thead>
<tr>
<th>Wavelength (nm)</th>
<th>( \frac{dn}{dT} \times 10^4 ) /K</th>
</tr>
</thead>
<tbody>
<tr>
<td>472.9</td>
<td>-1.37</td>
</tr>
<tr>
<td>780.4</td>
<td>-1.37</td>
</tr>
<tr>
<td>1055.7</td>
<td>-1.30</td>
</tr>
<tr>
<td>1308.9</td>
<td>-1.33</td>
</tr>
<tr>
<td>1550</td>
<td>-1.3</td>
</tr>
</tbody>
</table>

Material absorption

- Consider fiber damage threshold 12.8W
- Silicon absorber limit visible light
Laser Damage Attack

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Melting Point (K)</td>
<td>404</td>
</tr>
<tr>
<td>Boiling Point (K)</td>
<td>473</td>
</tr>
<tr>
<td>Evaporation rate (g/s)</td>
<td>( \log w = 5.87 - 6.77 \times 10^3 / T )</td>
</tr>
</tbody>
</table>

- Material could be **melted and evaporated** under strong laser beam. As a result of the evaporation and assist gas pressure, the material is thrown out of the hole.
- A reflection structure could be implemented to permanently fuse the optical path.

Laser Damage Attack

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Melting Point (K)</td>
<td>404</td>
</tr>
<tr>
<td>Boiling Point (K)</td>
<td>473</td>
</tr>
<tr>
<td>Evaporation rate (g/s)</td>
<td>$\log w = 5.87 - 6.77 \times 10^3 / T$</td>
</tr>
</tbody>
</table>

- Material could be **melted and evaporated** under strong laser beam. As a result of the evaporation and assist gas pressure, the material is thrown out of the hole.

- A reflection structure could be implemented to permanently fuse the optical path.

Application: Plug-and-Play MDI-QKD

- Plug-and-play phase-encoding measurement-device-independent (MDI) QKD
  - **Robust performance with simple setup.**
  - Common laser source for all users, enables **identical central wavelength** and **accurate clock synchronization**.
  - Automatically compensate for any **birefringence effects** and **polarization-dependent losses** in optical fibers.
  - The average Trojan photon number $\nu$ could provide Eve with information about the encoded phase.

---

Secret Key Rate against THA

Consider a repetition rate of 1 GHz, the Trojan-horse photon power is about $1.28 \times 10^{-10}$ mW.

- Assume average Trojan photon leakage $\nu$ from coherent state (CW and Pulse).

- Proof technique taken here: 

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detector efficiency</td>
<td>70%</td>
</tr>
<tr>
<td>Dark count rate</td>
<td>$10^{-7}$</td>
</tr>
<tr>
<td>Misalignment error</td>
<td>2%</td>
</tr>
<tr>
<td>Fiber loss</td>
<td>0.2 dB/km</td>
</tr>
</tbody>
</table>
Conclusions and Outlooks

<table>
<thead>
<tr>
<th>Ideal model</th>
<th>Our scheme</th>
</tr>
</thead>
<tbody>
<tr>
<td>❐ Provides a reliable and characterizable power limiting threshold (in the order of a few photons to hundreds for photons).</td>
<td>✓ Passive power limiter at mW level. Using additional attenuation for few-photon level limitation.</td>
</tr>
<tr>
<td>❐ If the input energy exceeds the threshold, the device will stop the communication channel.</td>
<td>✓ If the input energy exceeds the threshold, the output power will be limited, and start decrease.</td>
</tr>
<tr>
<td>❐ Cost-effective, passive, and easily replaceable.</td>
<td>✓ Cost-effective, passive, and easily replaceable.</td>
</tr>
<tr>
<td>❐ Power limiting effects are independent of other degree of freedoms, e.g., frequency, polarization, etc.</td>
<td>✓ Power limiting effects for both CW and pulsed light, wavelength and polarization independent.</td>
</tr>
</tbody>
</table>

- To do: Security analysis of MDIQKD with untrusted light source
- To do: Measurement with visible wavelength and high-power laser
Acknowledgement

We are hiring postdoctoral researchers (theory/experiment)!

Please contact us at charles.lim@nus.edu.sg for more information.
Securing Practical Quantum Cryptography with Optical Power Limiters

Gong Zhang\textsuperscript{1,*}, Ignatius William Primaatmaja\textsuperscript{2}, Jing Yan Haw\textsuperscript{1}, Xiao Gong\textsuperscript{1}, Chao Wang\textsuperscript{1,†}, and Charles C.-W. Lim\textsuperscript{1,2,‡}

\textsuperscript{*}zhanggong@nus.edu.sg \textsuperscript{†}wang.chao@nus.edu.sg \textsuperscript{‡}charles.lim@nus.edu.sg

\textsuperscript{1}Department of Electrical & Computer Engineering, National University of Singapore, Singapore

\textsuperscript{2}Centre for Quantum Technologies, National University of Singapore, Singapore