Simple Side Channel Analysis on Plug-and-Play Quantum Key Distribution

CHES 2018 Rump Session
2018. 09. 10

Suhri Kim, Sunghyun Jin, HanBit Kim, ByeongGyu Park, Seokhie Hong
Korea University
Single Trace Side Channel Analysis on Quantum Key Distribution

**QKD (Quantum Key Distribution)**

- **Classic channel**
  - DH, ECDH key exchange
- **Quantum Channel**
  - Quantum Key Distribution Protocol

Plug-and-Play QKD System

- Proposed by A. Muller
- Stable and Not required path having specific length ➔ No timing leakage

Block diagram of the P&P QKD system implemented in [2].

(Bit, Bases) = (Voltage, Phase)

<table>
<thead>
<tr>
<th></th>
<th>0v</th>
<th>2.5v</th>
<th>5v</th>
<th>-2.5v</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bit</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Bases</td>
<td>+</td>
<td>×</td>
<td>+</td>
<td>×</td>
</tr>
<tr>
<td>Phase</td>
<td>0</td>
<td>π/2</td>
<td>π</td>
<td>3π/2</td>
</tr>
</tbody>
</table>

Different voltage is LEAKAGE !!

Single Trace Attack on P&P QKD system

PLAINTEXT!
Thank you for your attention

sunghyunjin@korea.ac.kr