Recent progress on Measurement-Device-Independent (MDI) Quantum Key Distribution (QKD)

Marco Lucamarini
Quantum Information Group
Cambridge Research Laboratory
Toshiba Research Europe Ltd
A couple of useful links

Joshua Slater’s tutorial on MDI-QKD
QCrypt 2014 (Paris, France)
https://youtu.be/WL7OPSO0s_s

ML’s video lecture on MDI-QKD
1st QCall school (2018, Baiona, Spain)
http://tv.uvigo.es/matterhorn/36609
MDI QKD - Notation

QKD

Alice → Eve → Bob

MDI-QKD

Alice → Eve → Charlie → Bob

EPR Source

Source/Transmitter

Detector/Receiver

Bell Measurement

BELL MEASUREMENT

EPR SOURCE

DETECTOR/RECEIVER

MEASUREMENT

SOURCE/TRANSMITTER

TOSHIBA
Leading Innovation
Outline of this tutorial

1. Motivation and Introduction of MDI-QKD
   • Detector vulnerabilities and trusted networks
   • Basic features of MDI-QKD
2. MDI-QKD origin and working mechanism
   • Optical Interference
   • Entanglement swapping
3. Experiments
4. Variants
   • Twin-Field QKD
Outline of this tutorial

1. Motivation and Introduction of MDI-QKD
   • Detector vulnerabilities and trusted networks
   • Basic features of MDI-QKD

2. MDI-QKD origin and working mechanism
   • Optical Interference
   • Entanglement swapping

3. Experiments

4. Variants
   • Twin-Field QKD
Motivation 1: Implementation Security

ASSUMPTIONS

Alice

encoded single photons

NO ASSUMPTIONS

Eve

ASSUMPTIONS

Bob
Motivation 1: Implementation Security

Typical fibre-based one-way QKD setup

ASSUMPTIONS

Alice

NO ASSUMPTIONS

Eve

Bob

ASSUMPTIONS

CAUTION

Laser Diode: 1GHz repetition rate, characterised to have phase stabilisation.
Intensity Modulator: BB84 with 3 decoy states, + stronger stabilisation pulses.
AMZI: Information encoded on phase. Polarisation used to increase efficiency.
Attenuator: Feedback controlled to 0.5 photons per pulse. Increases loss for Trojan horse.
Isolator: Increases loss for incoming Trojan horse light.
Band Pass Filter: Limits Trojan horse to 1550nm

Delay Line: Trojan horse security.
Monitor Diode: Monitors input power for basic checks against APD blinding attacks.
Polarisation Control: Automatic stabilisation to correct for polarisation drift in fibre.
Interferometer Control: Automatic stabilisation to match Alice and Bob interferometer path lengths.
Detector gate: Automatic stabilisation to match gate with photon arrival.
APDs: Self-differenced for GHz gating. Temperature monitored for basic APD blinding attack prevention.
**Most targeted components**

### Secure quantum key distribution

Hoi-Kwong Lo\(^{1\ddagger}\), Marcos Curty\(^{2\ddagger}\) and Kiyoshi Tamaki\(^{3\ddagger}\)


<table>
<thead>
<tr>
<th>Attack</th>
<th>Target component</th>
<th>Tested system</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time-shift [76–79]</td>
<td>Detector</td>
<td>Commercial system</td>
</tr>
<tr>
<td>Time-information [80]</td>
<td>Detector</td>
<td>Research system</td>
</tr>
<tr>
<td>Detector-control [81–83]</td>
<td>Detector</td>
<td>Commercial system</td>
</tr>
<tr>
<td>Detector-control [84]</td>
<td>Detector</td>
<td>Research system</td>
</tr>
<tr>
<td>Detector dead-time [85]</td>
<td>Detector</td>
<td>Research system</td>
</tr>
<tr>
<td>Channel calibration [86]</td>
<td>Detector</td>
<td>Commercial system</td>
</tr>
</tbody>
</table>

It would be good to remove assumptions from detectors in QKD \(\rightarrow\) **MDI-QKD**

<table>
<thead>
<tr>
<th>Attack</th>
<th>Target component</th>
<th>Tested system</th>
</tr>
</thead>
<tbody>
<tr>
<td>Faraday-mirror [88]</td>
<td>Faraday mirror</td>
<td>Theory</td>
</tr>
<tr>
<td>Wavelength [89]</td>
<td>Beam-splitter</td>
<td>Theory</td>
</tr>
<tr>
<td>Phase information [90]</td>
<td>Source</td>
<td>Research system</td>
</tr>
<tr>
<td>Device calibration [91]</td>
<td>Local oscillator</td>
<td>Research system</td>
</tr>
</tbody>
</table>
Motivation 2: Trusted-node Networks

Typical architecture

It would be good to connect the users via untrusted nodes → MDI-QKD

Problem: the central node needs to be trusted
Measurement-Device-Independent Quantum Key Distribution over Untrustful Metropolitan Network

Yan-Lin Tang,¹,² Hua-Lei Yin,¹,² Qi Zhao,³ Hui Liu,¹,² Xiang-Xiang Sun,¹,² Ming-Qi Huang,¹,² Wei-Jun Zhang,⁴ Si-Jing Chen,⁴ Lu Zhang,⁴ Li-Xing You,⁴ Zhen Wang,⁴ Yang Liu,¹,² Chao-Yang Lu,¹,² Xiao Jiang,¹,²,* Xiongfeng Ma,³,¹ Qiang Zhang,¹,²,‡ Teng-Yun Chen¹,²,§ and Jian-Wei Pan¹,²,∥

• 8-by-4 mechanical optical switch to route the three users to the relay
• randomly switch any two users to the relay every two hours
MDI/QKD Reconfigurable Network

- MDI-QKD well matches star networks: it connects all the nodes with a minimum amount of optical links.

- Fully connected network with \(N+1\) nodes
  - \(N(N+1)/2\) physical links

- Fully connected MDI-QKD network with \(N+1\) nodes
  - \(N\) physical links

See also the 11:25 am talk by Mike Wang
“Enabling a scalable high-rate MDI-QKD network: theory and experiment”.

- 3 nodes, 3 links (fully connected network)
- 3 nodes, 3 links (1 relay)
- 3 nodes, 2 links (1 relay/node)
MDI/QKD Reconfigurable Network

MDI/QKD Reconfigurable Network

MDI-QKD ~ 10 kb/s

Alice- Bob (MDI)

real fibre

Alice- Charlie (QKD)

QKD ~ Mb/s

Bob- Charlie (QKD)

G. L. Roberts et al., Nature Communications 8, 1098 (2017).
Measurement-device-independent (MDI) QKD

**Pros & Cons**

- *Any* detector vulnerability is removed
- Users are linked by an untrusted relay
- Operational range is longer than QKD
- The key rate is smaller than QKD
Measurement-device-independent (MDI) QKD

Pros & Cons

- *Any* detector vulnerability is removed
- Users are linked by an untrusted relay
- Operational range is longer than QKD
- The key rate is smaller than QKD

If we consider the progress in the last 4 months we have to revise the last statement.
Measurement-device-independent (MDI) QKD

Pros & Cons

➤ Any detector vulnerability is removed
➤ Users are linked by an untrusted relay
➤ Operational range is longer than QKD
➤ The key rate is smaller than QKD for standard MDI-QKD, not for Twin-Field QKD

If we consider the progress in the last 4 months we have to revise the last statement.
Outline of this tutorial

1. Motivation and Introduction of MDI-QKD
   • Detector vulnerabilities and trusted networks
   • Basic features of MDI-QKD
2. MDI-QKD origin and working mechanism
   • Optical Interference
   • Entanglement swapping
3. Experiments
4. Variants
   • Twin-Field QKD
Outline of this tutorial

1. Motivation and Introduction of MDI-QKD
   • Detector vulnerabilities and trusted networks
   • Basic features of MDI-QKD
2. MDI-QKD origin and working mechanism
   • Optical Interference
   • Entanglement swapping
3. Experiments
4. Variants
   • Twin-Field QKD
Simple interferometric MDI-QKD scheme

\[ P_1 = \frac{1 + \cos(\varphi_a - \varphi_b)}{2} \]

\[ P_2 = \frac{1 - \cos(\varphi_a - \varphi_b)}{2} \]

security perimeter

Alice

Bob

Charlie

Eve

(|1v\rangle + |v1\rangle)/\sqrt{2}

\[ |v\rangle \]

\[ |1\rangle \]
Simple interferometric MDI-QKD scheme

\[ P_1 = \frac{1 + \cos(\varphi_a - \varphi_b)}{2} \]
\[ P_2 = \frac{1 - \cos(\varphi_a - \varphi_b)}{2} \]

With this scheme we achieve the MDI goals:
1) Detectors are outside the security perimeter
2) The relay is untrusted
Simple interferometric MDI-QKD scheme

$P_1 = \frac{1 + \cos(\varphi_a - \varphi_b)}{2}$

$P_2 = \frac{1 - \cos(\varphi_a - \varphi_b)}{2}$

Bob

Alice

Charlie

Eve

security perimeter

$\varphi_a = \{0, \pi\}$

$\varphi_b = \{0, \pi\}$

$(|1\rangle + |v1\rangle)/\sqrt{2}$

$|v\rangle$

$|1\rangle$

However, how do we distribute the entangled state to distant parties? We start from separable states and then use entanglement swapping.
Phase-encoding MDI-QKD

\[ I_1 = |\alpha|^2 [1 + \cos(\varphi_a - \varphi_b)] \]
\[ I_2 = |\alpha|^2 [1 - \cos(\varphi_a - \varphi_b)] \]

\[ |\alpha\rangle \approx e^{-\frac{|\alpha|^2}{2}} (|\nu\rangle + \alpha |1\rangle) \quad \text{for } \alpha \ll 1 \]

\[ |\alpha\rangle|\beta\rangle \approx e^{-\frac{|\alpha|^2 + |\beta|^2}{2}} (|\nu\rangle|\nu\rangle + \alpha |1\rangle|\nu\rangle + \beta |\nu\rangle|1\rangle + \alpha \beta |1\rangle|1\rangle) \]
Phase encoding schemes for measurement-device-independent quantum key distribution with basis-dependent flaw

Kiyoshi Tamaki,¹,² Hoi-Kwong Lo,³ Chi-Hang Fred Fung,⁴ and Bing Qi³


Limitations:
1) needs phase stabilization
2) limited distance

\[ |\alpha e^{i\varphi_a}\rangle \]

Alice

\[ |\alpha e^{i\varphi_b}\rangle \]

Bob

phase locked!
Phase-encoding MDI-QKD

| \( |\alpha e^{i\varphi_a}\rangle \) | | \( |\alpha e^{i\varphi_b}\rangle \) |

Charlie

Alice

Bob

Eve
Phase-encoding MDI-QKD

separable states, without any phase relation
Phase-encoding MDI-QKD

Hong-Ou-Mandel interference

|1\rangle |1\rangle

separable states, without any phase relation
Phase-encoding MDI-QKD

Hong-Ou-Mandel interference

separable states, without any phase relation
Phase-encoding MDI-QKD

It is not easy to perfectly generate the states $|1\rangle$, but we have approximations:

1. Heralding single-photon sources
2. Coherent states and decoy-state technique
Schemes with heralding single photons

Quantum cryptographic network based on quantum memories

Eli Biham
Computer Science Department, Technion, Haifa 32000, Israel

Bruno Huttner
Group of Applied Physics, University of Geneva, CH-1211, Geneva 4, Switzerland

Tal Mor
Department of Physics, Technion, Haifa 32000, Israel


Private spaces

Security of Practical Time-Reversed EPR Quantum Key Distribution

Hitoshi Inamori

Centre for Quantum Computation, Oxford University, Oxford, England.

Algorithmica 34, 340 (2002)

Side-Channel-Free Quantum Key Distribution

Samuel L. Braunstein and Stefano Pirandola
Computer Science, University of York, York YO10 5GH, United Kingdom


- S. Pirandola et al., Nature Photon. 9, 397 (2015)
- F. Xu et al., Nature Photon. 9, 772 (2015)
- S. Pirandola et al., Nature Photon. 9, 773 (2015)
Scheme using coherent decoy states

Measurement-Device-Independent Quantum Key Distribution

Hoi-Kwong Lo, Marcos Curty, and Bing Qi


Phase randomization + Decoy states

\[ \int_0^{2\pi} \frac{d\varphi}{2\pi} |\alpha e^{i\varphi}\rangle\langle \alpha e^{i\varphi}| = \sum_n p_n |n\rangle\langle n| \]

Privacy amplification to “postselect” |1\rangle\langle 1|

intensity |\alpha|^2 is varied for decoy states

encoding is done using polarization

\[ |\alpha e^{i\varphi_a}\rangle \]

Alice

\[ |\alpha e^{i\varphi_b}\rangle \]

Bob

\[ \varphi_a \text{ and } \varphi_b \text{ are random variables} \]
First MDI-QKD key rate

\[ R \geq P_{Z}^{1,1} Y_{Z}^{1,1} [1 - H_{2}(e_{X}^{1,1})] - Q_{Z} f_{e}(E_{Z}) H_{2}(E_{Z}) \]

Decoy states

\[ Q_{Z}^{q_{a}q_{b}} = \sum_{n,m=0}^{\infty} e^{-(q_{a}+q_{b})} \frac{q_{a}^{n} q_{b}^{m}}{n! m!} Y_{Z}^{n,m} \]

measured  known  unknown
First MDI-QKD key rate, finite size effects

\[ R \geq P_Z^{1,1} Y_Z^{1,1} \left[ 1 - H_2(e_X^{1,1}) \right] - Q_Z f_e(E_Z) H_2(E_Z) \]

Decoy states

\[ Q_Z^{a,b} = \sum_{n,m=0}^{\text{measured}} e^{-p(a+b)} \frac{q_a^n q_b^m}{n! m!} Y_Z^{n,m} \]

M. Curty et al., Nature Commun. 5, 3732 (2014)

Finite-size
Decoy states and finite size effect

The original decoy-state MDI-QKD adopts 2 bases \((X, Z)\) and 3 independent intensities \((u, v, w)\) \(\rightarrow\) 36 combinations

<table>
<thead>
<tr>
<th></th>
<th>(Z)</th>
<th>(X)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Z)</td>
<td>(u)</td>
<td>(v)</td>
</tr>
<tr>
<td>(u)</td>
<td>(p_{zz}^{uu})</td>
<td>(p_{zz}^{uv})</td>
</tr>
<tr>
<td>(v)</td>
<td>(p_{zz}^{vu})</td>
<td>(p_{zz}^{vv})</td>
</tr>
<tr>
<td>(w)</td>
<td>(p_{zz}^{wu})</td>
<td>(p_{zz}^{vw})</td>
</tr>
</tbody>
</table>

Data used in the decoy-state parameter estimation, relevant for finite-size effects
The new protocol\(^(*)\) adopts 2 bases \((X, Z)\) and 4 coupled intensities \((s, u, v, w)\) → 16 combinations

<table>
<thead>
<tr>
<th></th>
<th>$Z$</th>
<th>$s$</th>
<th>$u$</th>
<th>$v$</th>
<th>$w$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$Z$</td>
<td>$s$</td>
<td>$p_{ZZ}^{ss}$</td>
<td>$p_{ZZ}^{su}$</td>
<td>$p_{ZZ}^{sv}$</td>
<td>$p_{ZZ}^{sw}$</td>
</tr>
<tr>
<td>$X$</td>
<td>$u$</td>
<td>$p_{XX}^{us}$</td>
<td>$p_{XX}^{uu}$</td>
<td>$p_{XX}^{uv}$</td>
<td>$p_{XX}^{uw}$</td>
</tr>
<tr>
<td></td>
<td>$v$</td>
<td>$p_{XX}^{vs}$</td>
<td>$p_{XX}^{vu}$</td>
<td>$p_{XX}^{vv}$</td>
<td>$p_{XX}^{vw}$</td>
</tr>
<tr>
<td></td>
<td>$w$</td>
<td>$p_{XX}^{ws}$</td>
<td>$p_{XX}^{wu}$</td>
<td>$p_{XX}^{ww}$</td>
<td>$p_{XX}^{ww}$</td>
</tr>
</tbody>
</table>

- This protocol was first implemented in *Comandar et al., Nature Photon.* **10**, 312 (2016), where its composable security is proven and the highest MDI-QKD key rate is achieved.
- Then it was implemented in *Yin et al., Phys. Rev. Lett.* **117**, 190501 (2016), to achieve the longest fibre-based MDI-QKD transmission.
Equivalent description with Time Bins
1. Motivation and Introduction of MDI-QKD
   - Detector vulnerabilities and trusted networks
   - Basic features of MDI-QKD

2. MDI-QKD origin and working mechanism
   - Optical Interference
   - Entanglement swapping

3. Experiments

4. Variants
   - Twin-Field QKD
Outline of this tutorial

1. Motivation and Introduction of MDI-QKD
   • Detector vulnerabilities and trusted networks
   • Basic features of MDI-QKD
2. MDI-QKD origin and working mechanism
   • Optical Interference
   • Entanglement swapping
3. Experiments
4. Variants
   • Twin-Field QKD
Watch Joshua Slater’s talk @ QCrypt 2014 website

MEASUREMENT-DEVICE-INDEPENDENT QUANTUM KEY DISTRIBUTION

Joshua A. Slater

Vienna Centre for Quantum Science & Technology
University of Vienna, Austria

> + 1

Institute for Quantum Science & Technology
University of Calgary, Canada

https://youtu.be/WL7OPSO0s_s
EXPERIMENTS

Calgary, Canada (A. Rubenok, JAS, et al. PRL 111, 130501 (2013))

Control Systems:
- Timing Feedback
- Polarization Control
- Frequency Shift

Charlie measured & Alice corrected with linear phase chirp < 10 MHz difference
EXPERIMENTS

Calgary, Canada  (A. Rubenok, JAS, et al. Ph. D.

Specifications
CW Laser, 1553nm
2 MHz rep rate
500 ps / 2 GHz
1.4 ns time-bin qubits
Decoy-States (0.5*, 0.05, 0)
EXPERIMENTS

Rio de Janeiro, Brazil (T. F. da Silva et al., PRA 88, 052303 (2013))

Specifications
- cw laser, 1546 nm
- 1.5 ns / 650 MHz
- Polarization qubits
- Decoy-States (0.5, 0.1, 0)

Rep 1 MHz
- Multiplexed - time / polarization sync

Extracted data
- $Q_r^{11} = 6.88 \times 10^{-6}$
- $E_d^{11} = 0.018$
- $Q_{rect} = 1.36 \times 10^{-5}$
- $E_{rect} = 0.057$
- $R = 1.04 \times 10^{-6}$
EXPERIMENTS

Hefei, China (Y. Liu, et al. PRL 111, 130502 (2013))

Specifications
Pulsed, 1550 nm
2 ns / 10 pm
85 ns time-bin qubits
Decoy-States (0.5, 0.2, 0.1, 0)

0.1 pm frequency precision
10 ps time precision
Random modulations
Phase-stabilized interferometers
EXPERIMENTS

Toronto, Canada (Z. Tang et al., PRL 112, 190503 (2014))

Specifications
- CW laser, 1542 nm
- Phase randomized states
- 1.5 ns / 650 MHz
- Polarization qubits
- Decoy-States (0.3, 0.1, 0.01)

\[ e^X = 26.2\% \]
\[ e^Z = 1.8\% \]
\[ S = 1e^{-8} \]
THE CUTTING-EDGE OF MDI-QKD

Long Distance / High Loss
Hefei, China
(Y.-L. Tang et al., arxiv:1407.8012)
Also @ Phys. Rev. Lett. 113, 190501 (2014)

75 MHz Rep-Rate
@ 200 km, 0.009 b/sec
@ 100 km, 3 kbps
Key rate performance gap of MDI-QKD

State of the art up to 2015

<table>
<thead>
<tr>
<th></th>
<th>Clock (MHz)</th>
<th>Pulse width (ps)</th>
<th>Eq. distance (km)</th>
<th>Max key rate (bit/s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ref. [18]</td>
<td>75</td>
<td>2500</td>
<td>50</td>
<td>$6.7 \times 10^1$</td>
</tr>
<tr>
<td>Ref. [19]</td>
<td>2</td>
<td>250</td>
<td>45</td>
<td>$3.4 \times 10^0$</td>
</tr>
<tr>
<td></td>
<td>20</td>
<td>290</td>
<td>80</td>
<td>$6.2 \times 10^2$</td>
</tr>
<tr>
<td>Ref. [14]</td>
<td>2</td>
<td>500</td>
<td>45</td>
<td>$3 \times 10^0$</td>
</tr>
<tr>
<td>Ref. [16]</td>
<td>1</td>
<td>1500</td>
<td>17</td>
<td>$1 \times 10^0$</td>
</tr>
</tbody>
</table>

- In May 2016 the key rate was improved
- In June 2016 the distance was extended

Experimental setup and novel light source

(*) L. Comandar et al., Nature Photon. 10, 312 (2016)
## Going high-rate

### Increased key rate in 2016

<table>
<thead>
<tr>
<th>Ref.</th>
<th>Clock (MHz)</th>
<th>Pulse width (ps)</th>
<th>Eq. distance (km)</th>
<th>Max key rate (bit/s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>[18]</td>
<td>75</td>
<td>2500</td>
<td>50</td>
<td>$6.7 \times 10^1$</td>
</tr>
<tr>
<td>[19]</td>
<td>2</td>
<td>250</td>
<td>45</td>
<td>$3.4 \times 10^0$</td>
</tr>
<tr>
<td></td>
<td>20</td>
<td>290</td>
<td>80</td>
<td>$6.2 \times 10^2$</td>
</tr>
<tr>
<td>[14]</td>
<td>2</td>
<td>500</td>
<td>45</td>
<td>$3 \times 10^0$</td>
</tr>
<tr>
<td>[16]</td>
<td>1</td>
<td>1500</td>
<td>17</td>
<td>$1 \times 10^0$</td>
</tr>
<tr>
<td><strong>This work (</strong>)**</td>
<td><strong>1000</strong></td>
<td><strong>35</strong></td>
<td><strong>0</strong></td>
<td><strong>$1.660 \times 10^6$</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>$1.286 \times 10^6$</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>9.7 \times 10^4</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>$1.6 \times 10^4$</strong></td>
</tr>
</tbody>
</table>


(*) L. Comandar *et al.*, Nature Photon. 10, 312 (2016)
MDI-QKD: Finite sample size included

Finite-size QKD

Finite-size MDI-QKD


X. Ma et al, Phys. Rev A 2012

(*) L. Comandar et al., Nature Photon. 10, 312 (2016)
Going long distance

- Phase randomised WCP
- Time bin encoding and 4 intensities for decoy states
- 5 IMs in each user! 1 pulse shaping, 2 decoys, 2 time-bin encoding (ToA)
- 3 months: 2584 bits (0.00034 bits/s), no EC, no PA
- Detectors: SNSP efficiency 65%, dark counts 30 Hz
Going long distance

Longest fibre-based secure quantum communication until recently
Still the longest distance for experimental fibre-based MDI-QKD

Long distance performance of MDI QKD

How far can we go with a decent key rate?

see N. Gisin et al., Rev. Mod. Phys. 74, 145 (2002)
<table>
<thead>
<tr>
<th>Outline of this tutorial</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Motivation and Introduction of MDI-QKD</td>
</tr>
<tr>
<td>• Detector vulnerabilities and trusted networks</td>
</tr>
<tr>
<td>• Basic features of MDI-QKD</td>
</tr>
<tr>
<td>2. MDI-QKD origin and working mechanism</td>
</tr>
<tr>
<td>• Optical Interference</td>
</tr>
<tr>
<td>• Entanglement swapping</td>
</tr>
<tr>
<td>3. Experiments</td>
</tr>
<tr>
<td>4. Variants</td>
</tr>
<tr>
<td>• Twin-Field QKD</td>
</tr>
</tbody>
</table>
Outline of this tutorial

1. Motivation and Introduction of MDI-QKD
   • Detector vulnerabilities and trusted networks
   • Basic features of MDI-QKD

2. MDI-QKD origin and working mechanism
   • Optical Interference
   • Entanglement swapping

3. Experiments

4. Variants
   • Twin-Field QKD
**Fundamental limit of QKD**

Fundamental rate-loss tradeoff for optical quantum key distribution

**“TGW” bound for the secret key capacity (SKC)**

\[
SKC(\eta) \leq \log_2 \left( \frac{1 + \eta}{1 - \eta} \right)
\]

In a point-to-point configuration it is *impossible* to overcome the SKC bounds.

**“PLOB” bound**

\[
SKC(\eta) = \log_2 \left( \frac{1}{1 - \eta} \right)
\]
Can we go beyond the direct-link bounds?

See 14:15 talk by Alberto Boaron:
"2.5 GHz clocked QKD over 379 km"
Other solutions

**Measurement-device-independent quantum key distribution with quantum memories**

Silvestre Abruzzo, Hermann Kampermann, and Dagmar Bruß


---

**Memory-assisted measurement-device-independent quantum key distribution**

C. Panayi, M. Razavi, X. Ma, N. Lütkenhaus

New Journal of Physics 16 (2014) 043005
Other solutions

The implementation of these schemes is still challenging!

It turns out that we can overcome the direct-link bounds with a scheme nearly as simple as MDI-QKD.
Twin-Field QKD

Overcoming the rate-distance limit of quantum key distribution without quantum repeaters


doi:10.1038/s41586-018-0066-6
Download Citation
Received: 27 April 2017
Accepted: 05 February 2018
Published: 02 May 2018
Twin-Field QKD

Phase locking

Global phase randomisation

Alice

RNG

LS

IM

$\mu_a$

$\varphi_a$

PM

VOA

Bob

RNG

LS

IM

$\mu_b$

$\varphi_b$

PM

VOA

Charlie

0

1

$\delta_a$

$\delta_b$
Twin-Field QKD

Phase slices

global phase randomisation

phase locking

Alice

Bob

RNG

PM

VOA

LS

IM

µ_a

φ_a

µ_b

φ_b

0

1

Charlie

Δ_4

Δ_2

Δ_1

Δ_0

Δ_8

Δ_12

Δ_4

Δ_2

Δ_1

Δ_0

Δ_8

Δ_12

Phase slices
Twin-Field QKD

Phase locking

Global phase randomisation

discard
Twin-Field QKD

Phase locking

Global phase randomisation

Phase slices
These fields are twins: accept!

The users end up in a situation similar to decoy-state QKD, but with a twice-as-long fibre in between.
The graph illustrates the secure key gain (bit/clock) as a function of Alice-Bob fibre length (km) and Alice-Bob attenuation (dB). Various QKD protocols are compared, including MDI-QKD, DV-QKD, CV-QKD, PLOB-QKD, and TWG-QKD. The curves represent different bounds and configurations, such as 1, 2, and 3 repeaters, with the ideal and realistic bounds highlighted. The graph also shows the relationship between secure key gain and fibre length, with the key gain scaling as \( \eta^{1/4} \), \( \eta^{1/3} \), and \( \eta^{1/2} \) for 1, 2, and 3 repeaters, respectively.
Very recent (and very promising) progress


See next talk (10:50 am) by Pei Zeng: “Global Phase Encoding QKD”
Twin-Field QKD Feasibility

Phase drift: \( \delta_b - \delta_a = \frac{2\pi}{s} (\Delta v L + v \Delta L) \)

fibre spools: up to 275 km each

\[ \text{With 6 rad/ms, a feedback every } \sim 50 \mu \text{s is necessary to make the optical error rate lower than 3%} \]

With 6 rad/ms, a feedback every \( \sim 50 \mu \text{s} \) is necessary to make the optical error rate lower than 3%.
Conclusions

- MDI-QKD is only 6 year-old, but we already have impressive results in terms of performance (key rate, distance) and functionalities (untrusted-node networks). This means the community is strong and responsive to innovations.

- The research on MDI-QKD has led to developments like
  - all-optical quantum repeaters
  - coherent-state HOM interference
  - optically-injected laser sources for quantum communications
  - refined control techniques for the in-field implementations.

- The (MDI) Twin-Field QKD allows us to overcome a bound considered unsurmountable without quantum repeaters. New techniques for quantum communications are likely to be imported from other fields.

The path to MDI Quantum Information has just started and we can expect many more surprising and exciting results along the way!
Thanks to…

**MDI-QKD team at TREL**

Mariella Minder  
Mirko Pittaluga  
George Roberts  
Zhiliang Yuan  
Andrew Shields  
James Dynes

…and to you for your attention!