Long distance and high rate quantum key distribution.

Hugo Zbinden
GAP – Quantum Technologies
Is the quantum computer a threat for information security?

IBM, 20 qubits
Classical Cryptography

A) Based on Complexity
   DES, AES (secret key)
   RSA (public key)
   Security unproven

B) Based on Information Theory
   one time pad (Vernam)

plaintext: 001010010011101010001101001
key: +101011011100110101001111010101
cyphertext: 100001001001010111110110111100

security proven

problem: key distribution
Quantum Key Distribution

- Quantum Cryptography is not a new coding method
- Send key with individual photons (quantum states)
- The eavesdropper may not measure without perturbation (Heisenberg's uncertainty principle)
- Eavesdropping can be detected by Alice and Bob!

QKD is proven information theoretically secure!
Quantum Key Distribution

Assumption: secure perimeters for Alice and Bob
BB84 protocol (Bennett, Brassard, 1984)

Alice's Bit Sequence
0     1     0     -     0     1     1     1     1     -      1     0
-      1     -     -      0    1      -      -     1     -      1     0

Bob's Bases

Bob's Results

Key
Eavesdropping (intercept-resend)

Error with 25 % probability

\[ I_{AE} = 2 \text{ QBER} \] (quantum bit error rate)
Eve attacks: information curves

\[ I_{AB} = 1 - H(QBER) \]

Secret key rate

\[ I_{AE} = 2 \times QBER \]

Probabilistic I-R

Binary Entropy function

\[ H_b(p) = -p \log_2 p - (1 - p) \log_2 (1 - p) \]
The steps to a secret key

Transmission

Quantum channel
(losses)

Public channel

Reconciliation

Basis

Sifted key

QBER estimate

Error correction

Privacy amplification

Key

+ Authentication!!!
Smolin and Bennett
IBM 1989
Swiss QCRIPT project (2013)
Secure Quantum Key Distribution over 421 km of Optical Fiber

Alberto Boaron,1,* Gianluca Boso,1 Davide Rusca,1 Cédric Vulliez,1 Claire Autebert,1 Misael Caloz,1 Matthieu Perrenoud,1 Gaëtan Gras,1,2 Félix Bussières,1 Ming-Jun Li,3 Daniel Nolan,3 Anthony Martin,1 and Hugo Zbinden1

1Group of Applied Physics, University of Geneva, Chemin de Pinchat 22, 1211 Geneva 4, Switzerland
2ID Quantique SA, Chemin de la Marbrerie 3, 1227 Carouge, Switzerland
3Corning Incorporated, Corning, New York 14831, USA

(Received 10 July 2018; published 5 November 2018)

New simple and efficient QKD protocol

2.5 GHz repetition rate transmitter

Ultralow-loss fibers

Superconducting detectors developed in Geneva
# Time-bin encoding BB84

<table>
<thead>
<tr>
<th>Alice’s state preparation</th>
<th>Bob’s detection apparatus</th>
</tr>
</thead>
</table>
| **Z, 0** | $|0\rangle$ | ![Z detection times](image)
| **Z, 1** | $|1\rangle$ | ![2 detection times](image)
| **X, 0** | $|+\rangle$ | ![2 detectors](image)
| **X, 1** | $|-\rangle$ | ![2 detectors](image)
a) Protocol

- Time-bin encoding
- Decoy-state method

<table>
<thead>
<tr>
<th>basis, bit</th>
<th>state</th>
<th>$\mu_1$</th>
<th>$\mu_2$</th>
<th>$\mu_3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Z, 0</td>
<td>$</td>
<td>0\rangle$</td>
<td>___</td>
<td>___</td>
</tr>
<tr>
<td>Z, 1</td>
<td>$</td>
<td>1\rangle$</td>
<td>___</td>
<td>___</td>
</tr>
<tr>
<td>X, 0</td>
<td>$</td>
<td>+\rangle$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>X, 1</td>
<td>$</td>
<td>-\rangle$</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

a) Protocol

- Time-bin encoding
- Decoy-state method

<table>
<thead>
<tr>
<th>basis, bit</th>
<th>state</th>
<th>$\mu_1$</th>
<th>$\mu_2$</th>
<th>$\mu_3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Z, 0</td>
<td>$</td>
<td>0\rangle$</td>
<td><img src="image" alt="Graph" /></td>
<td><img src="image" alt="Graph" /></td>
</tr>
<tr>
<td>Z, 1</td>
<td>$</td>
<td>1\rangle$</td>
<td><img src="image" alt="Graph" /></td>
<td><img src="image" alt="Graph" /></td>
</tr>
<tr>
<td>X, 0</td>
<td>$</td>
<td>+\rangle$</td>
<td><img src="image" alt="Graph" /></td>
<td><img src="image" alt="Graph" /></td>
</tr>
<tr>
<td>X, 1</td>
<td>$</td>
<td>-\rangle$</td>
<td><img src="image" alt="Graph" /></td>
<td><img src="image" alt="Graph" /></td>
</tr>
</tbody>
</table>

Finite key analysis:
For limited block size, using only two different average energies is advantageous!

$\epsilon = 10^{-9}$
a) Protocol

- Time-bin encoding
- Decoy-state method

4 states, 4 outcomes → 3 states, 3 outcomes

μ₁ ≈ 0.5

Simple Setup (with a single intensity modulator)
b) all fibre, high repetition rate source

Alice and Bob are FPGA controlled:

- Synchronization
  real-time adjustment of:
  - interferometer phase
  - detector timing

- Generate random bits
  QRNG + expansion

- High-speed integrated intensity modulator: 5 GHz

- Sifting
- Error correction
- Privacy amplification
- Authentication
c) quantum channel: ultra low-loss fibres

Corning ULL-28® ultralow-loss fibre: 0.16 dB/km
Attenuation including connectors and splices: 0.17 dB/km
d) detectors

Superconducting nanowire single-photon detectors
Amorphous molybdenum silicide
Temperature: 0.8 K

Performance of our SNSPD
Detector contributions to QBER

- Timing jitter
- darkcounts
Dark counts: dominated by black-body radiation

- No filtering
- + Fiber spool (cold)
- + WDM filter
- < 1 cts/s
- ~50% efficiency
**Results: SKR vs distance**

![Graph showing secret key rate vs distance and attenuation in dB.](image)

**Ideal system**
- BB84 with decoy state
- 2.5 GHz repetition rate
- No detector noise
- 100% detection efficiency
- Same block size than exp. points

(1) **BB84**, Fröhlich et al., Optica 4, 163 (2017), (2) **COW**, Korzh et al., Nat. Phot. 9, 163 (2015)
Secret Key rate vs distance

10 Mbit/s
≈ 1/t_{dead}

D_{\text{max}} = f(d_{\text{cr}}, \text{block size})

- 1 day acquisition time
- BB84 with decoy state
- 40 GHz repetition rate
- 0 Hz dark counts
- 100% detection efficiency
- \( \varepsilon = 10^{-9} \)
- 8600 bits/24h @ 600km

Other approach: twin-field QKD
Twin field QKD

In fact, it’s a huge interferometer!
- Stabilisation!
- Synchronisation!

- Recent feasibility experiment: 500 km
Quantum repeater

Create remote entanglement independently for each link. Extend by swapping

Direct transmission \( T \sim \left( \frac{1}{\eta_t} \right)^n \)
Repeater \( T \sim \frac{1}{\eta_t} \)

Requires heralded entanglement creation, storage and swapping of entanglement

Talk de Mikael Afzelius demain!
Satellite-based entanglement distribution over 1200 kilometers

Juan Yin,1,2 Yuan Cao,1,2 Yu-Huai Li,1,2 Sheng-Kai Xiao,1,2 Liang Zhang,2,2
Ji-Gang Ren,1,2 Wen-Qi Cai,1,2 Wei-Yue Liu,1,2 Bo Li,1,2 Hui Dai,1,2 Guang-Bing Li,1,2
Qi-Ming Lu,1,2 Yan-Hong Gong,1,2 Yu Xu,1,2 Shuang-Lin Li,1,2 Peng Zhi Li,1,2
Yu-Yun Yin,1,2 Zi-Qing Jiang,3 Ming Li,3 Jian-Jun Jia,3 Ge Ren,4 Dong He,4
Yi-Lin Zhou,5 Xiao-Xiang Zhang,6 Na Wang,7 Xiang Chang,6 Zhen-Cal Zhu,3
Nai-Le Liu,1,2 Yu-Ao Chen,1,2 Chao-Yang Lu,1,2 Rong Shu,2,3 Cheng-Zhi Peng,1,2
Jian-Yu Wang,2,5,6 Jian-Wei Pan1,2,5

http://science.sciencemag.org/content/356/6343/1140
SPDC source: 810 nm
6 MHz pair generation rate

Total loss: ~65dB

**Average coincidence count rate:** 1Hz

**275s coverage time**

\[ S = 2.37 \pm 0.09 \]

Finite key analysis: Impossible to extract a key with small \( \varepsilon \)
Satellite to ground QKD

- just one downlink with decoy-state faint laser pulses (polarisation BB84)
Results

1-10 kb/s during 250s per passage
Conclusions

• QKD over 400 - 500 km
• Bit rates over 10Mbit/s @ < 50km

Outlook:
• Make it smaller, make it cheaper (integrated optics)
• Integrate it in telecom network
• Find many applications!