2013-08-05

Free-space quantum network with trusted relay

Zhu Cao

Joint work with Wei-Yue Liu, Hai-Lin Yong, Ji-Gang Ren, Xiongfeng Ma, Cheng-Zhi Peng, and Jian-Wei Pan

Univ. of Sci. & Tech. of China
Tsinghua University

Outline

- Background
- Field tests
- Our scheme and key rate calculations
- Experiment Results
- Future Prospects

Commercial QKD Device

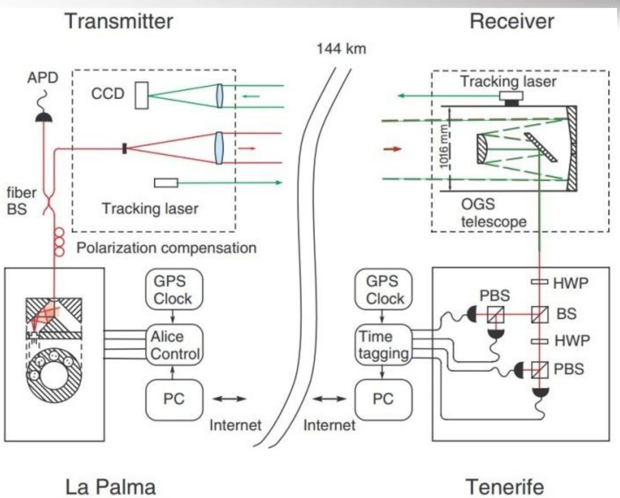
- MagiQ (Qbox)
- id Quantique (CERBERIS)
- Com Tech Co. Ltd., Anhui

www.magiqtech.com

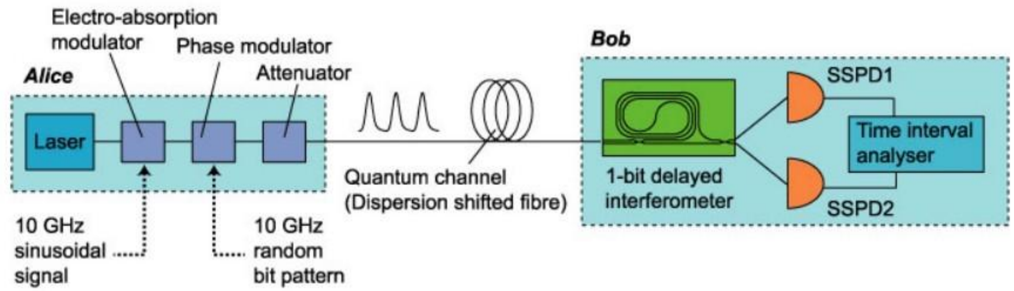
www.idquantique.com

www.quantum-info.com

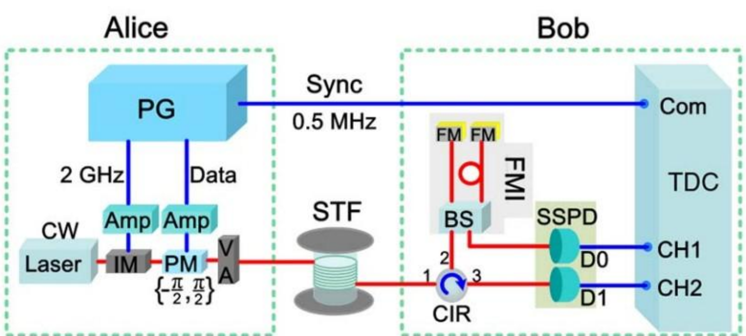
Long distance QKD experiments



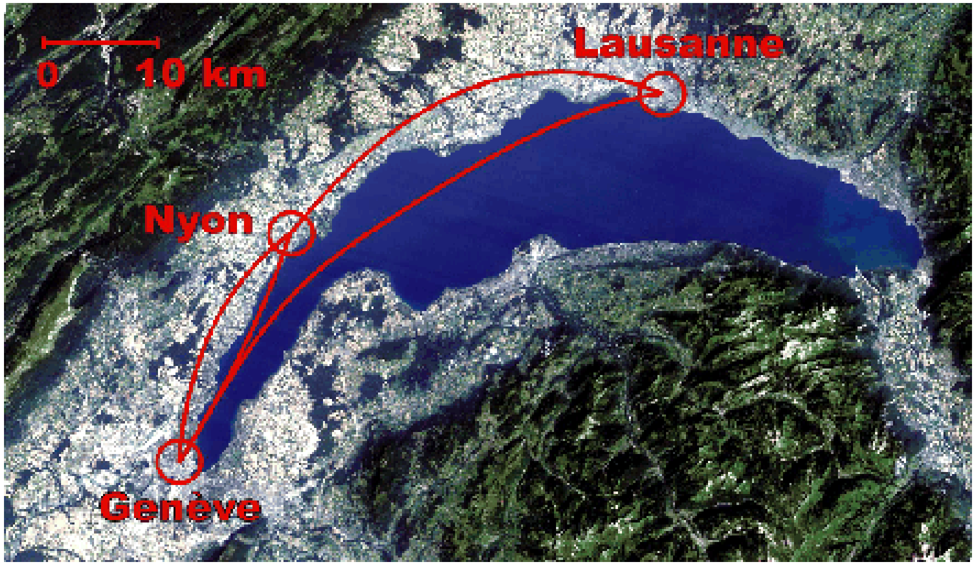
Schmitt-Manderbach, T. et al.
Phys. Rev. Lett. 98, 010504 (2007)



Takesue, H. et al. Nature Photonics 1, 343–348 (2007)



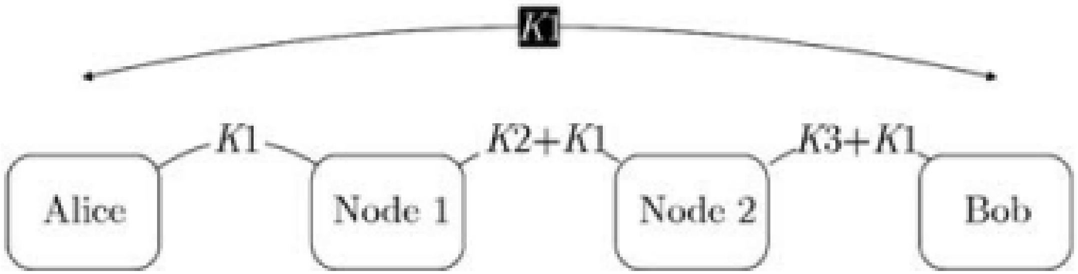
Wang, S. et al. Opt. Lett. 37, 1008–1010 (2012)



Stucki, D. et al. New J. of Phys. 4, 41 (2002)

Extend QKD distance

- 1. Combining multiple current QKD realizations as trusted relays



- 2. Use entanglement swapping as untrusted relays between users

Extend QKD distance (cont.)

- 3. Satellite-based QKD
  - By using satellite as relay which moves around the earth, transmission loss does not depend on key distribution distance.
  - Minimizes the effect of harsh geographical environment

Challenges

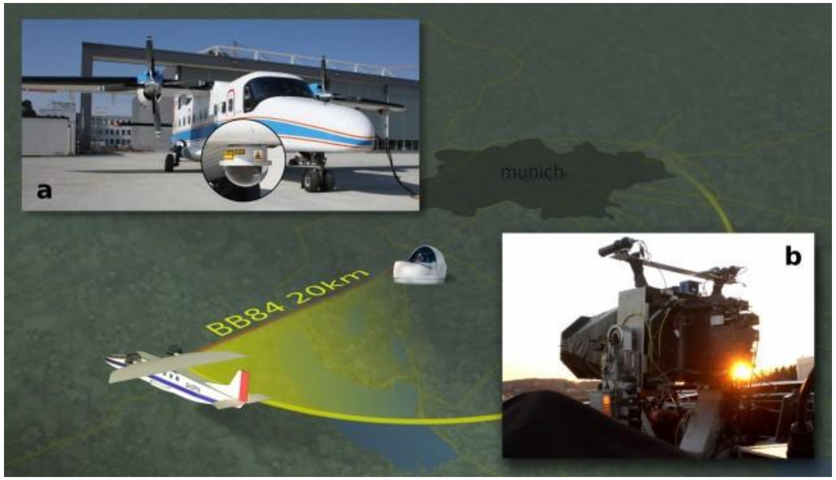
Comparable Channel Loss

Moving transmitter

Various locations

Limited computational power

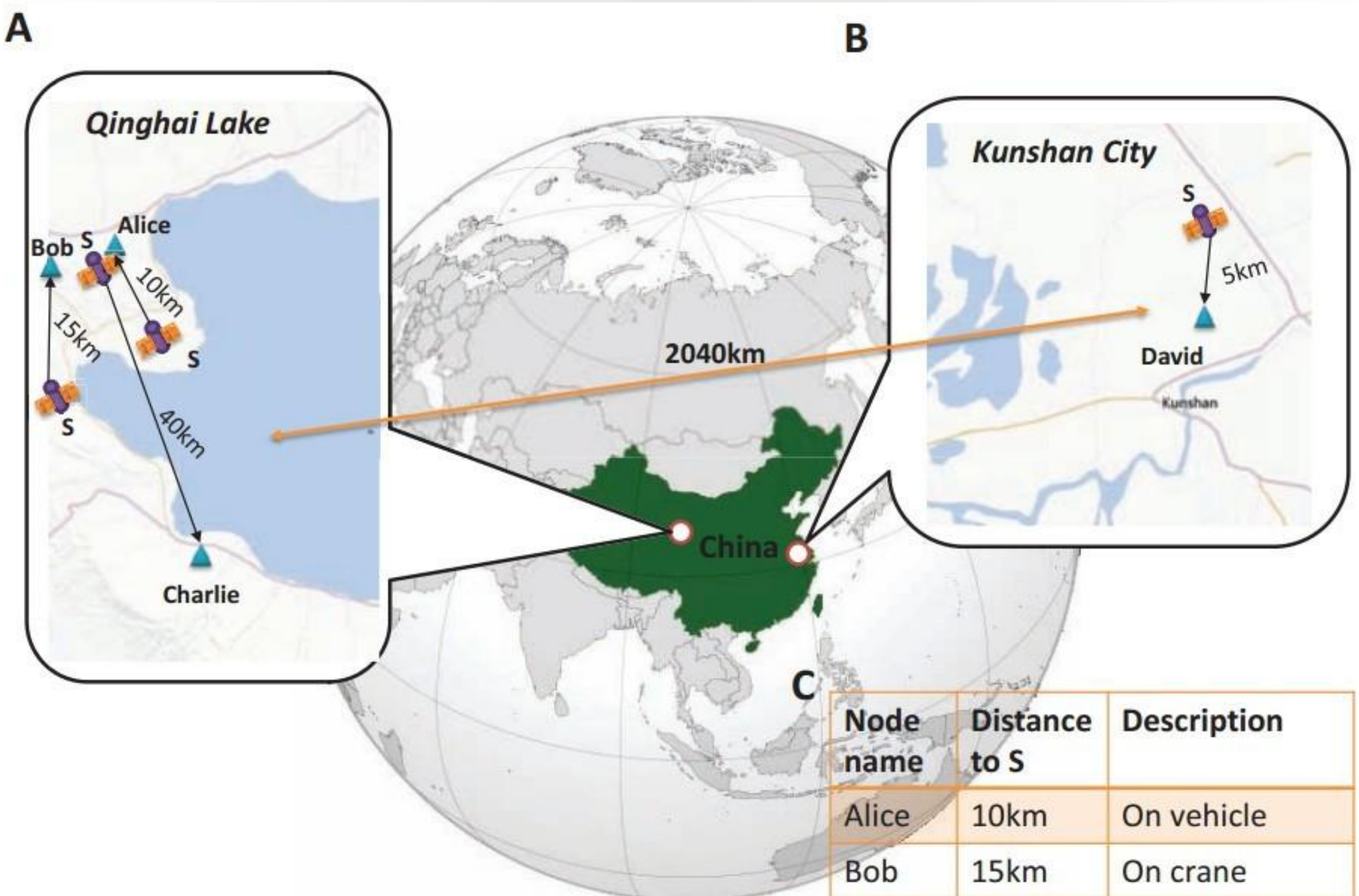
Communication cost



Nauerth,S. et al.. Nature Photonics 7, 382–386 (2013)

Wang et al., Nature Photon. 7, 387 (2013).

Experiment Demonstration



C

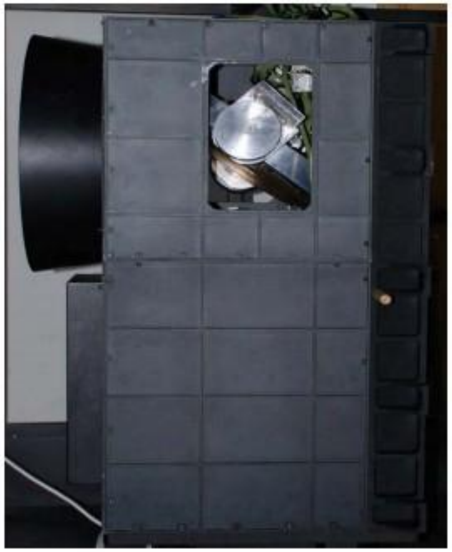
Node name	Distance to S	Description
Alice	10km	On vehicle
Bob	15km	On crane
Charlie	40km	Long distance
David	5km	High loss

Transmitter and Receiver

A

C

B



D

Secure BB84

- **(Prepare)** Alice creates $(4+\delta)n$ random bits, for each bit, she creates a qubit in the Z or X basis according a random **b**, Alice sends the resulting qubits to Bob, Alice chooses a random v_k in C_1,
- **(Measurement)** Bob receives and publicly announces it. He measures each qubit in random Z or X basis, Alice announces **b**,
- **(Sift)** Alice and Bob only keep the qubits measured and sent in the same basis. Alice randomly picks 2n of the remaining positions and picks n for testing, Alice and Bob publicly compared their check bits. If too many errors occurred then they abort. Alice is left with **|x>** and Bob with **|x+e>.**
- **(EC)** Alice announces $x-v_k$. Bob subtracts this from his result and corrects according C_1 to obtain v_k,
- **(PA)** Alice and Bob compute the coset v_k+C2 in C1 to obtain **k**.

Shor Preskill, Phys.Rev.Lett.85:441-444,2000

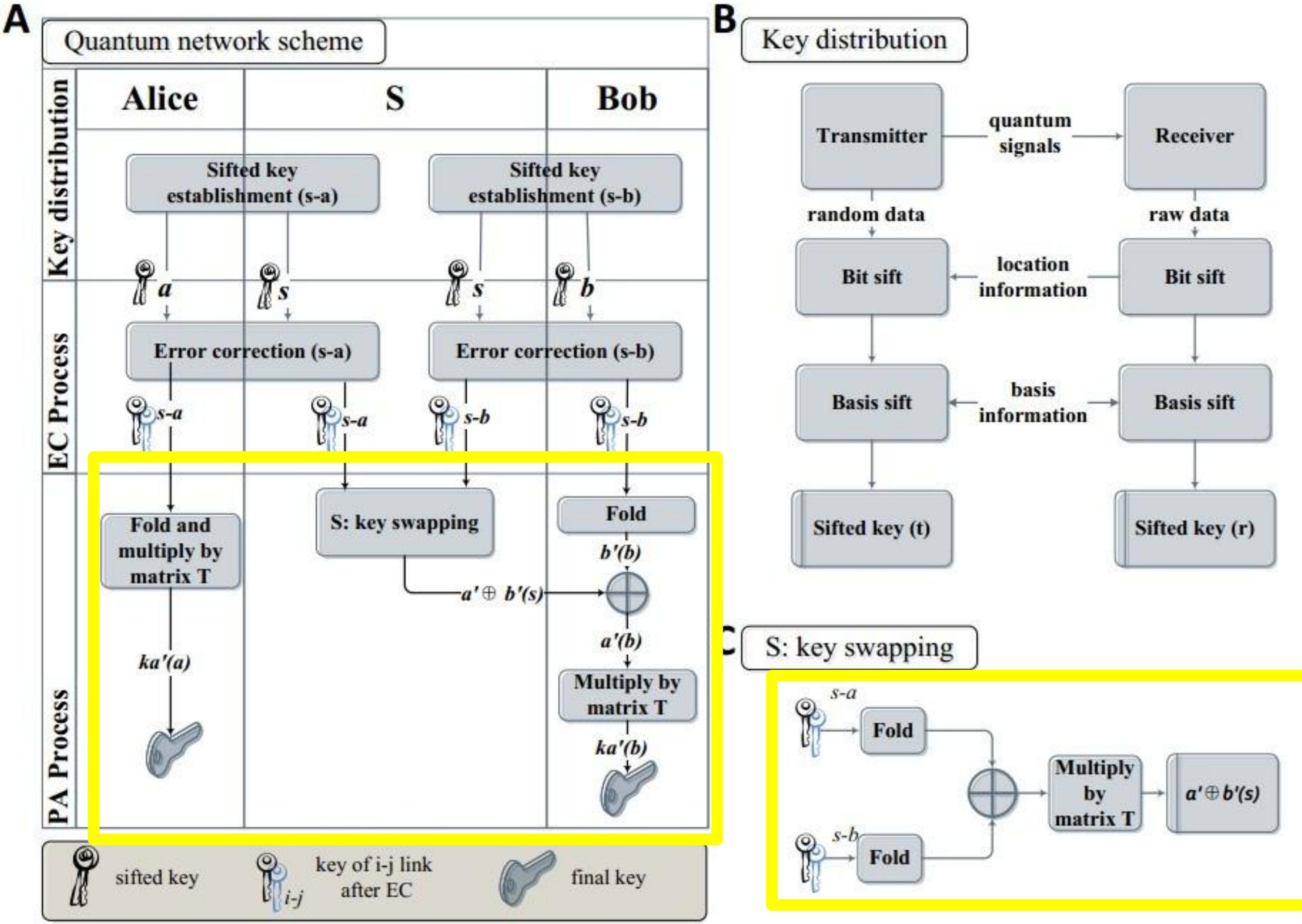
Original trusted relay scheme

1. Alice and Bob each performs QKD with the relay, S;
2. Alice and Bob each runs error correction with S;
3. Alice and Bob each runs privacy amplification with S;
4. S sends the parity of the two secure keys to one of the users, say, Bob.
5. Bob performs XOR of the parity with his key, thus shares a key with Alice.

Delayed Privacy Amplification Scheme

1. Alice and Bob each performs QKD with the relay, S,
2. Alice and Bob each runs error correction with S,
3. S sends the parity of the two partially secure identical keys to Bob.
4. Bob performs XOR of the parity with his key, thus shares a key with Alice.
5. Alice and Bob perform privacy amplification to extract a secure key.

Ma, X. & Lutkenhaus, N. US patent application (2011).
Fung, F., et al. Phys. Rev. A 85, 032308 (2012)


A
Quantum network scheme
Key distribution
EC Process
PA Process
Alice
S
Bob
Sifted key establishment (s-a)
Sifted key establishment (s-b)
a
s
s
b
Error correction (s-a)
Error correction (s-b)
s-a
s-a
s-b
s-b
Fold and multiply by matrix T
S: key swapping
Fold
b'(b)
a'⊕ b'(s)
a'(b)
ka'(a)
Multiply by matrix T
ka'(b)
sifted key
key of i-j link after EC
i-j
final key
B
Key distribution
Transmitter
quantum signals
Receiver
random data
raw data
Bit sift
location information
Bit sift
Basis sift
basis information
Basis sift
Sifted key (t)
Sifted key (r)
C
S: key swapping
s-a
Fold
s-b
Fold
Multiply by matrix T
a'⊕b'(s)

Folding

- Folding
  - Original string
    "010011100011100101001011"
  - Split in to two equal-length keys
    "010011100011"   "100101001011"
  - XOR them

$$
\begin{array}{r}
010011100011 \\
\oplus \quad \underline{100101001011} \\
110110101000
\end{array}
$$

Single channel QKD key rate

- Decoy state $R \geq \Omega_1[1 - H(e_1)] - I_{ec}$
  - Ω_1 the ratio of single-photon component, estimated by decoy-state method
  - e_1 the error rate of the single-photon component
  - I_{ec} the cost of error correction
  - R secure key bit per raw key bit
  - $H(x)$ the binary Shannon entropy of x

GLLP2004 Quantum Inf. Comput. 4, 325 arXiv:quant-ph/0212066

Key rate (combined channel)

- **Recall we cut the error-corrected into two parts and XOR them**
- **Single PA** $0.5 * (2\Omega - \Omega^2) * (1 - H(p^2))$
- **Combined PA**

$$I_{PA} = 0.5 * (2\Omega_1 - \Omega_1^2) * (2\Omega_2 - \Omega_2^2) *$$

$$(1 - H(p_a^2 * (1 - p_b^2) + p_b^2 * (1 - p_a^2)).$$

- **Final key rate is** $I_{PA} - I_{ec}$
  where $I_{ec} = H(e_\mu)$

Data for each single channel

	$S-Alice$	$S-Bob$	$S-Charlie$	$S-David$
$T(s)$	444	688	1468	1106
N_s	7095111	2247571	2067037	6888169
N_d	1413620	454105	447742	1523780
N_0	102779	57088	71909	95913
E_μ	0.035	0.029	0.034	0.041
E_v	0.058	0.058	0.071	0.062
Q_μ	$3.20 * 10^{-4}$	$6.53 * 10^{-5}$	$2.82 * 10^{-5}$	$1.25 * 10^{-4}$
Q_v	$1.27 * 10^{-4}$	$2.64 * 10^{-5}$	$1.22 * 10^{-5}$	$5.51 * 10^{-5}$
Y_0	$9.26 * 10^{-6}$	$3.32 * 10^{-6}$	$1.96 * 10^{-6}$	$3.47 * 10^{-6}$
Y_1	$4.34 * 10^{-4}$	$8.43 * 10^{-5}$	$3.97 * 10^{-5}$	$2.10 * 10^{-4}$
e_1	0.043	0.015	0.015	0.049
$R_0(bps)$	990.03	329.35	151.20	512.72
$Total\ key$	439573	226593	221974	567063

Key rate of each pair (bps)

	Alice	Bob	Charlie	David
Alice	/	27.71	23.27	87.7
Bob	27.71	/	22.74	36.16
Charlie	23.27	22.74	/	28.48
David	87.70	36.16	28.48	/

Future Prospects

- **Techniques**
  - **modified delayed privacy amplification**
  - **Acquisition Tracking Pointing (ATP)**
  - **High-precision time synchronization,**

- **Further reducing communication cost**
  - **bit and basis sift**
  - **error correction**
  - **privacy amplification.**
- **Build a ground-satellite network by sending satellite into space**
  - **Quantum Entanglement Distribution**
  - **Quantum Teleportation**
  - **QKD between East and West part of China**

Thank you!

Contact: Zhu Cao
Email: caozhu55@gmail.com