Quantum Cryptography and Network Applications

2014/3/10

Professor Han-Chieh Chao (趙涵捷)

Professor, Department of Electronic Engineering and CSIE

President, National Ilan University, I-Lan, Taiwan

Kaohsiung, Taiwan

March 7, 2014

Prof. Han-Chieh Chao

- Han-Chieh Chao
- TEL：+8863-9317000
- E-mail：hcc@niu.edu.tw

- PhD from Purdue University
- Current Position ： President of National Ilan University (NIU), Taiwan
- Jointly Appointed Professor of Department of CSIE and Electronic Engineering, NIU.
- Jointly Appointed Professor of National Dong Hwa University, Hualen, Chinese Taipei
- Honorary Professorship of
  - Beijing Jiaotong University, Yantai University, Xiamen University , Lanzhou University and HIT at SZ
- FIET (Fellow of IET)
- FBCS CITP (Fellow and Chartered IT Professional of British Computer Society)
- Editor-in-Chief: IET Communications, IET Networks, IJAHUC, JIT, IJIPT
- Associate Editor: IEEE Network, IEEE Systems Journal, Mobile Information Systems, WCMC, IJCS, … etc.

(http://www.twgrid.org)

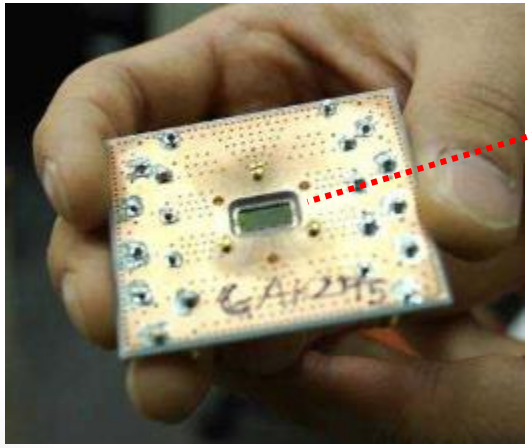
Outline

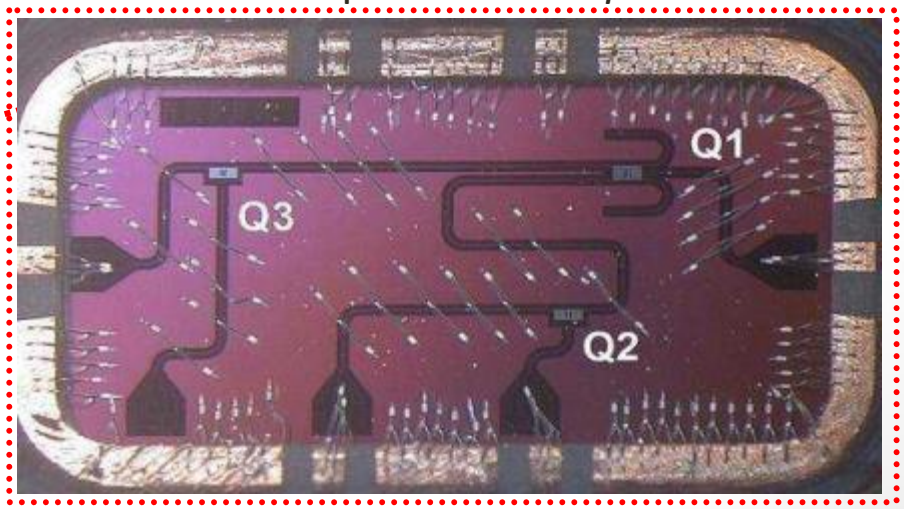
- **Quantum Computing**
- **Basic Properties of Quantum Mechanics**
- **Quantum Cryptography**
  - **Quantum Key Distribution (QKD)**
  - **Quantum Secure Direct Communication (QSDC)**
  - **Quantum Secret Sharing (QSS)**
- **Applications for Network Security**
  - **Multiparty Secure Computation**
  - **Quantum Cryptography for Future E-Commerce**
- **Conclusion**

Quantum Computing

- Extraordinary capabilities are expected:
  - factoring a 3,000 digit number 10^{40} faster than today
- Today's best multi-core processors can encrypt or decrypt a 150-digit number
- Decrypting a 1,000-digit number, it would take roughly all the computational resources in the world
- "On a quantum computer [in theory], it might take a few hours"

Silicon chip with three *qubits*

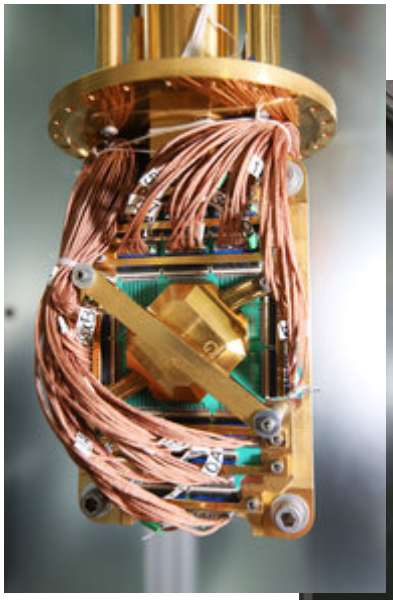




Source: IBM (2012)
Using a theory proposed 22 years ago by physicist Prof. Dr. Andreas Wieck of the Ruhr University Bochum (RUB)

Quantum Computing

- In this year, Google Buys a Quantum Computer developed by D-Wave Systems.
- Google declined to comment, aside from the blog post.
  - “For most problems, it was 11,000 times faster, but in the more difficult 50 percent, it was 33,000 times faster. In the top 25 percent, it was 50,000 times faster.”

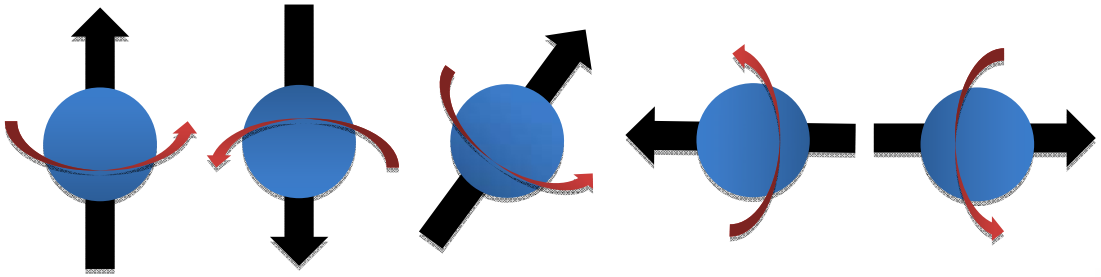


Source:
http://bits.blogs.nytimes.com/2013/05/16/google-buys-a-quantum-computer/?_r=0

Basic Properties of Quantum Mechanics

-Quantum bit (*qubit*)

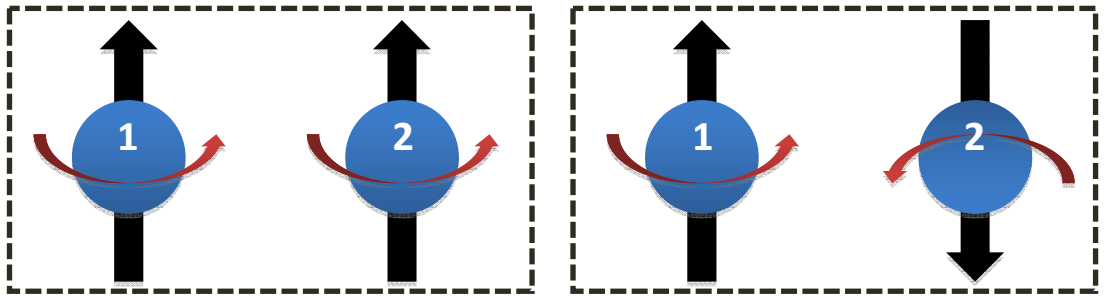
- In the quantum world, each particle is spinning in its own direction.
- *qubits* that spin up represent the classical bit “0” (a), and conversely the qubits that spin down represent “1” (b).
- But notice that before we measure qubits, we cannot assure their directions.
  - *qubit* can be 0 and 1 at the same time
  - Superposition (real parallel computing)



(a) (b) (c) (d) (e)

Basic Properties of Quantum Mechanics
-Quantum entanglement

- For two or more qubits their spinning directions are correlated to each other.
- There are two kinds of entanglement states
  - the same direction
  - opposite directions
- However far they are from each other, we can always correctly deduce one's direction from the other.



(f) (g)

Quantum Cryptography

- **Quantum Cryptography was invented in 1984 (29 years ago).**
- **Quantum Channel could not be**
  - **Tapped**
  - **Measured without disturbance**
  - **Faithfully copied**

QUANTUM CRYPTOGRAPHY: PUBLIC KEY DISTRIBUTION AND COIN TOSSING

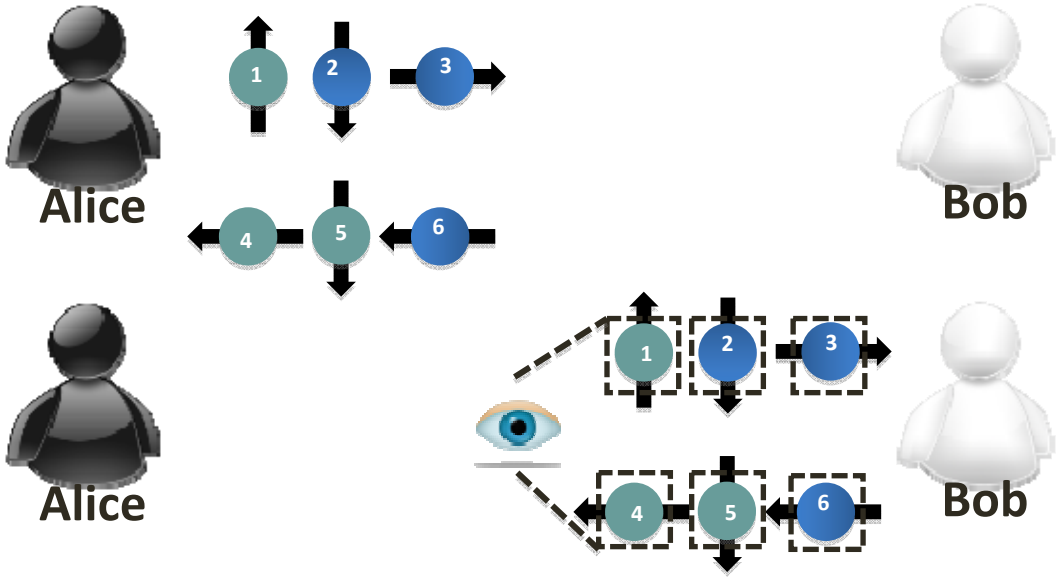
Charles H. Bennett (IBM Research, Yorktown Heights NY 10598 USA)
Gilles Brassard (dept. IRO, Univ. de Montreal, H3C 3J7 Canada)

International Conference on Computers, Systems & Signal Processing Bangalore, India December 10-12, 1984

Quantum Key Distribution (QKD)

- A famous protocol for creating a one-time pad is BB84
- Alice and Bob want to share a random key before they communicate
- They must first define the spinning type
  - left and right, to represent “0” and “1”
  - spinning up and down as key 1, left and right as key 2
- BB84 cannot only create the shared key but also detect eavesdroppers.
  - In order to get the shared key Eva may steal the sequence and measure them.
  - But the error rate will be higher than the safe one.

Quantum Key Distribution (QKD)



Measurement result

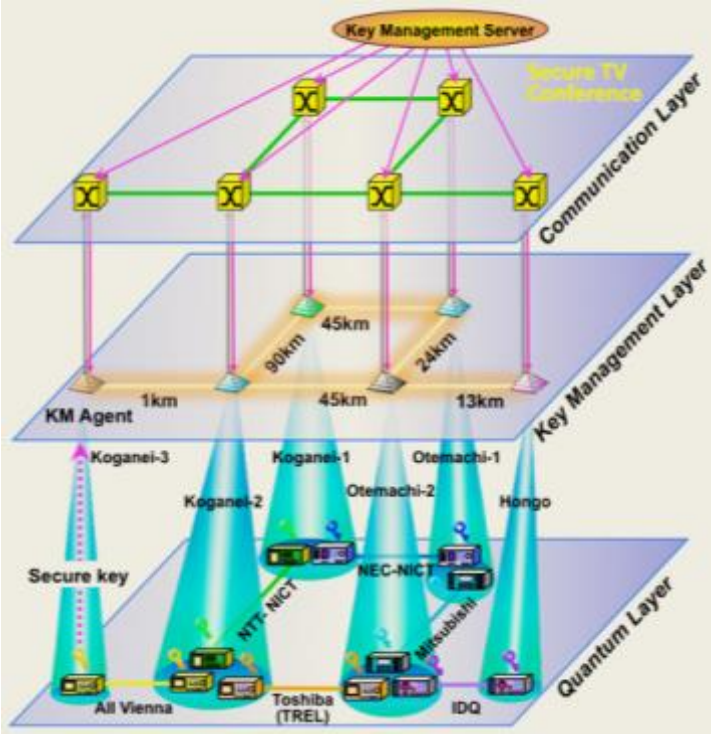
Qubit id	1	2	3	4	5	6
Key type (Alice)	1	1	2	2	1	2
Alice(bit)	0	1	1	0	1	0
Key type (Bob)	1	1	2	1	2	1
Bob	0	1	1	1	1	1

Measurement result with Eva

Qubit id	1	2	3	4	5	6
Key type (Alice)	1	1	2	2	1	2
Alice(bit)	0	1	1	0	1	0
Key type (Eva)	1	1	2	1	2	1
Eva	0	1	1	1	1	1
Key type (Bob)	2	2	1	2	1	2
Bob	1	1	0	1	0	0

Quantum Key Distribution (QKD)

- UQCC 2010 Tokyo QKD Network:
  - an eavesdropping attempt on the network and its detection,
  - demonstration of uncrackable one-time pad encryption of a live audio or video stream over a distance of 45 km with a line loss of some 13 dB



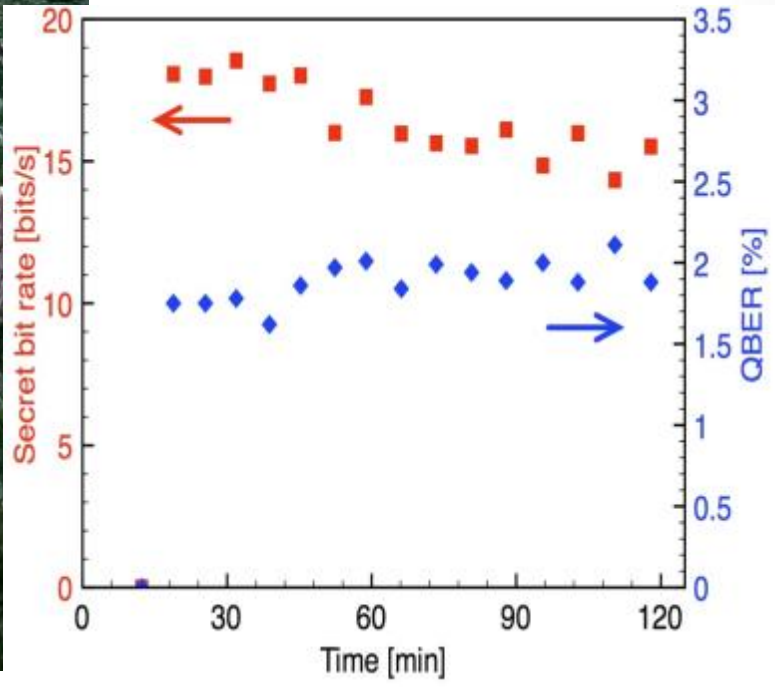
Source: http://www.uqcc2010.org/highlights/index.html

Long distance QKD (World records)

- **150 km of installed fibers**
  - **Optics Express 17, 13326 (2009)**

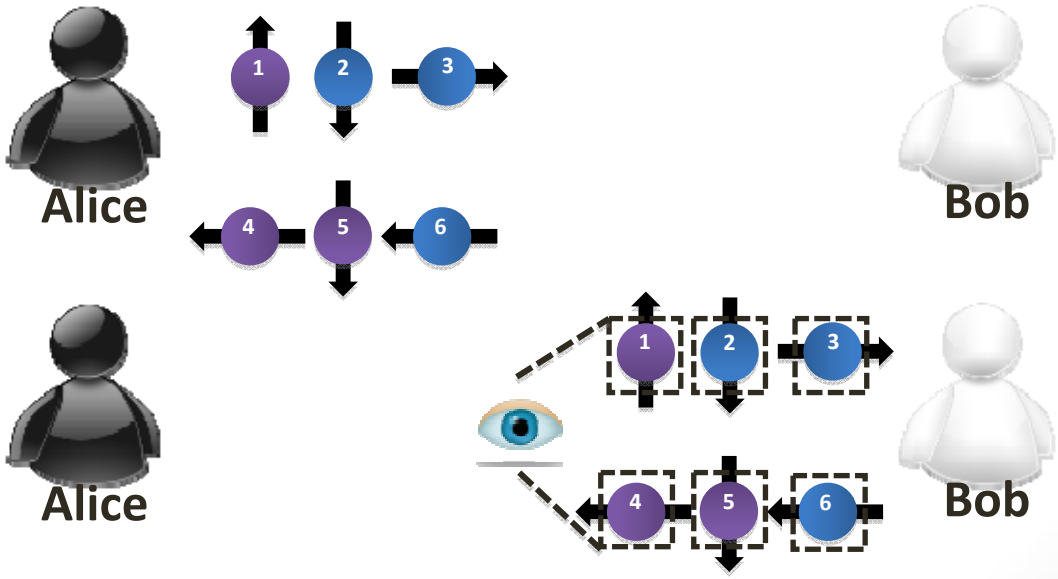
250 km (lab)

NJP 11, 075003 (2009)



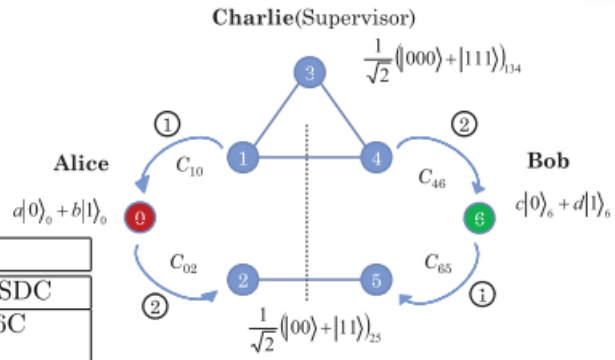
Quantum Secure Direct Communication (QSDC)

- QSDC combines the BB84 concept with direct communications.
- These qubits contain test qubits (darker ones) and message qubits (lighter ones).
- Measures the test qubits for eavesdropper detection.



Our Contributions (QSDC)

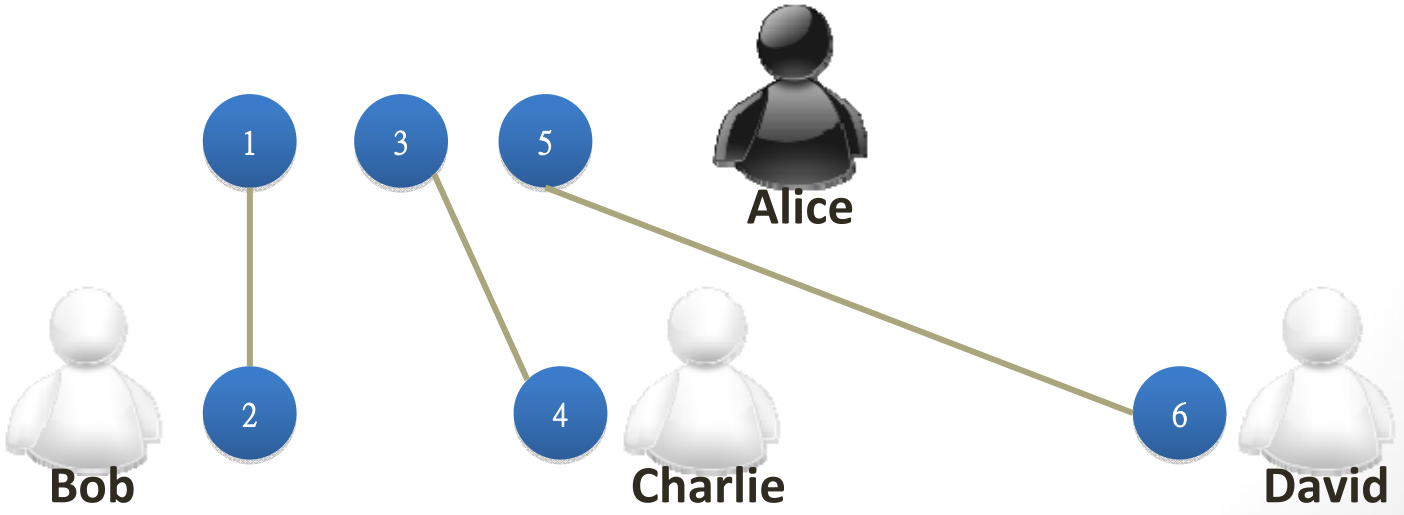
- Yao-Hsin Chou, Guo-Jyun Zeng, Fang-Jhu Lin, Chi-Yuan Chen and Han-Chieh Chao, "**Quantum Secure Communication Network Protocol with Entangled Photons for Mobile Communications**," ACM/Springer Mobile Networks and Applications (MONET), published online, 2013.
- Yao-Hsin Chou, Yu-Ting Lin, Chi-Yuan Chen, Fang-Jhu Lin, and Han-Chieh Chao, "**Controlled Bidirectional Quantum Secure Direct Communication**," under review.



Scheme	Gao2005	Dong2011	Man2006	Dong2008	Ours
Protocol type	CQSDC	CQSDC	CBQSDC	CBQSDC	CBQSDC
Resource cost of two directional transmission	6Q&6C	6Q&6C	6Q&6C	6Q&6C	5Q&6C
Secret message type	C/Q	C/Q	C	C	C/Q
Received classical bits	1C	1C	2C	2C	1C
Received quantum bits	1Q	1Q	0	0	1Q
Controller	Yes	Yes	Yes	Yes	Yes
Classical message exchange	Yes	Yes	Yes	Yes	Yes
Quantum information exchange	Yes	Yes	No	No	Yes
No transmission	Yes	Yes	No	Yes	Yes
Honest condition between legitimate users	No	No	No	No	Yes

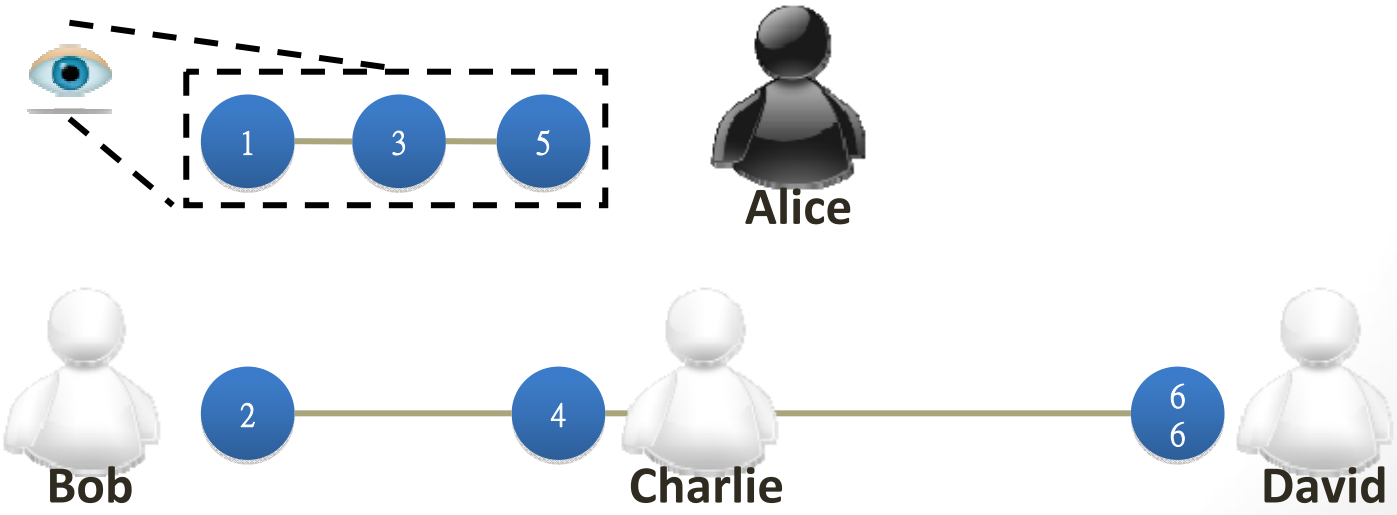
Quantum Secret Sharing (QSS)

- A sender divides a secret message into *n* components and sends them to *n* agents.
- It means that the *n* agents will have to cooperate with each other to decode the secret message.
- Step 1: Alice prepares three pairs of two entangled qubits, ordered by (1, 2), (3, 4) and (5, 6). She then sends one qubit of each pair to each receiver.



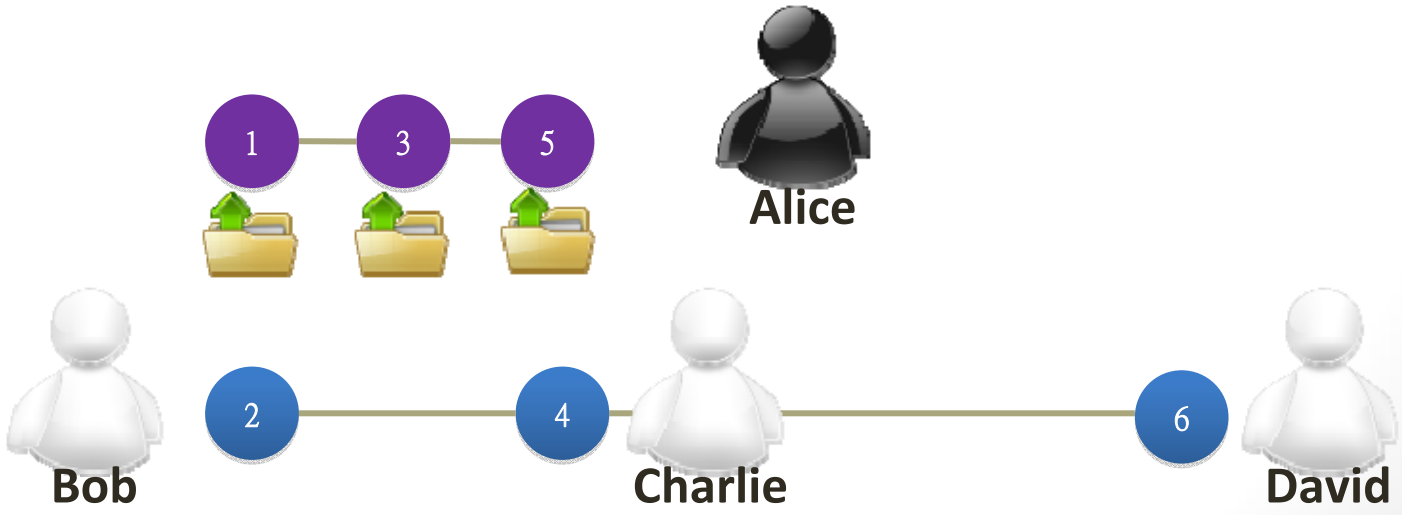
Quantum Secret Sharing (QSS)

- Step 2: Alice measures all of the qubits that she holds.
- The three qubits that Alice holds are now entangled with each other. The other qubits are also mutually entangled.
- This interesting feature of quantum mechanics is called entanglement swapping.



Quantum Secret Sharing (QSS)

- Step 3: After the entanglement swapping process Alice encodes her secret message by performing one of four operations on each *qubit*.
- Step 4: Bob, Charlie and David cooperate to decode Alice' message using the *qubits* they have and the classical bits that Alice published.



Our Contributions (QSS)

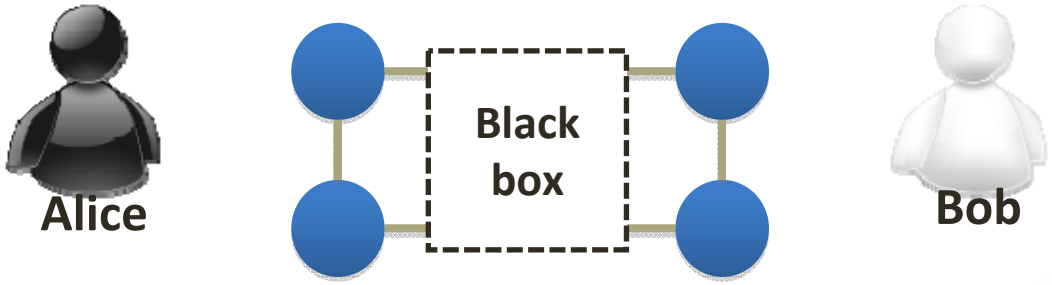
- Yao-Hsin Chou, Chi-Yuan Chen, Rui-Kai Fan, Han-Chieh Chao, and Fang-Jhu Lin, "**Enhanced Multiparty Quantum Secret Sharing of Classical Messages by using Entanglement Swapping**," IET Information Security, Vol. 6, No. 2, pp. 84-92, June 2012.
- Yao-Hsin Chou, Shuo-Mao Chen, Yu-Ting Lin, Chi-Yuan Chen, and Han-Chieh Chao, "**Using GHZ-state for Multiparty Quantum Secret Sharing without Code Table**," The Computer Journal, Vol. 56, No. 10, pp. 1167-1175, 2013.
  - Not only using less qubits but also carrying more information
  - Does not have to pre-share the code table

	The cost of each scheme and the performance comparison		
Schemes	Cost of qubits	Cost of bits	Rounds
Deng *et al.* [10]	$(A+1)*\frac{C}{4}$	0	$\frac{C}{4}$
Sun *et al.* [11]	$2(A+1)*\frac{C}{4}$	0	$\frac{C}{4}$
→ Chou *et al.* [22]	$2(A+1)*\frac{C}{4}$	$\frac{C}{2}$	$\frac{C}{4}$
→ Our schemes	$2(A+1)*\frac{C}{6}$	$\frac{C}{3}$	$\frac{C}{2A}$

1. A: The total number of agents.
2. C: The classical bits of secret messages.

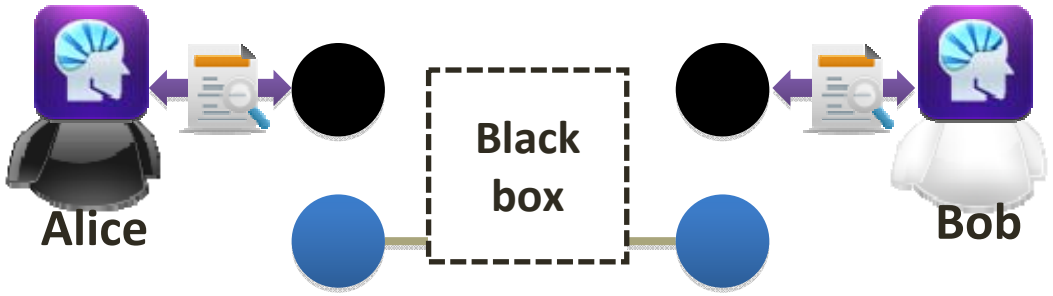
Multiparty Secure Computation

- Secure computation involves obtaining the final decryption result without exposing the required details.
- There is a related secure computation problem called the “dating problem”.
- we simply think of the quantum machine as a black box. Imagined a black box exists between Alice and Bob.
- Inside the box are four entangled *qubits*. Alice and Bob each have two *qubits* in their possession



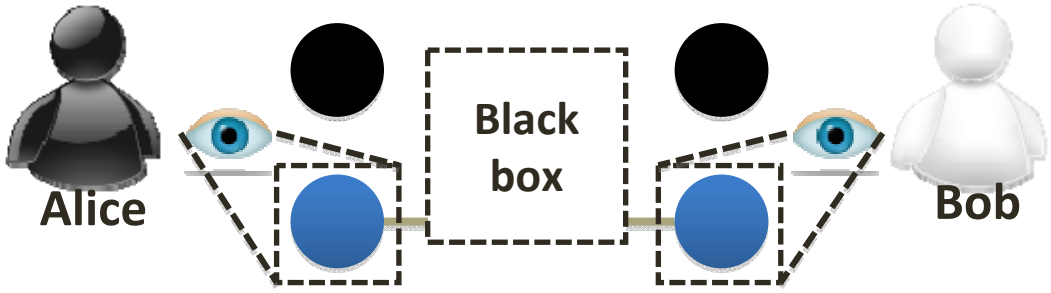
Multiparty Secure Computation

- Alice and Bob first measure one of their *qubits*.
- If the outcome is in accord with their intention, the process continues, or otherwise they restart the process.



Multiparty Secure Computation

- If the process goes on, they measure the remaining qubits and publish their second outcome.
- They can now obtain the final result by computing the published outcomes.
- This secure computation concept can also be used for cloud computing.
- Moreover, the cloud data center knows nothing about the encoded data because any measurement cannot avoid disturbing the *qubit* states.

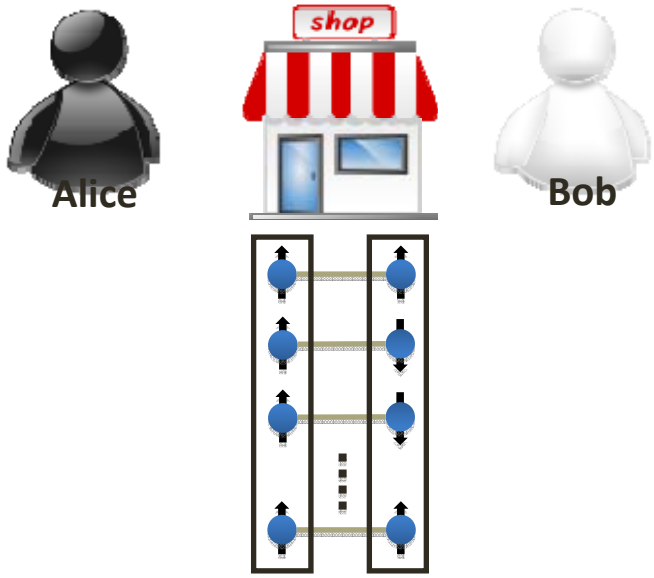


Quantum Cryptography for Future E-Commerce

- The E-Commerce application uses the QKD and QSDC concepts.
- Suppose Alice and Bob are a customer and seller, respectively, and they have a deal through an online shopping mall.
- There are some constraints as follows.
  - First, the business platform is provided by an online shopping mall.
  - Second, the process the customers use to find and buy goods must be through the online shopping mall.
  - Third, sellers provide their services through the online shopping mall.

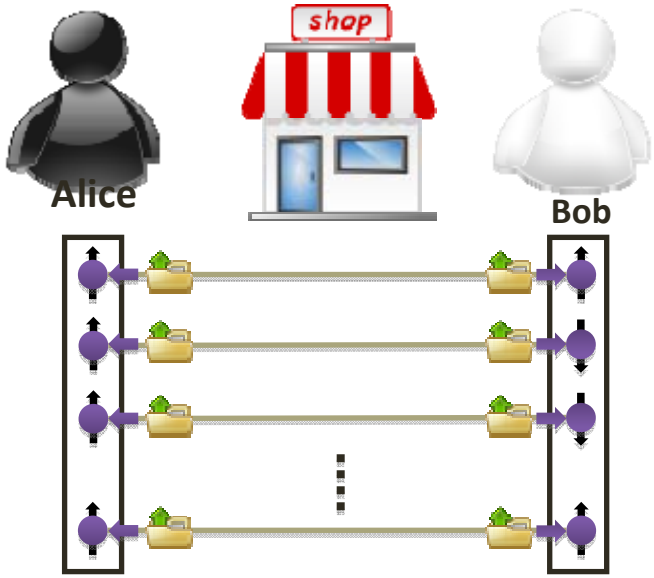
Quantum Cryptography for Future E-Commerce

- The protocol is composed of three steps
- Step1: The online shop first prepares a sequence of *qubits* in entanglement to provide service for Alice and Bob.



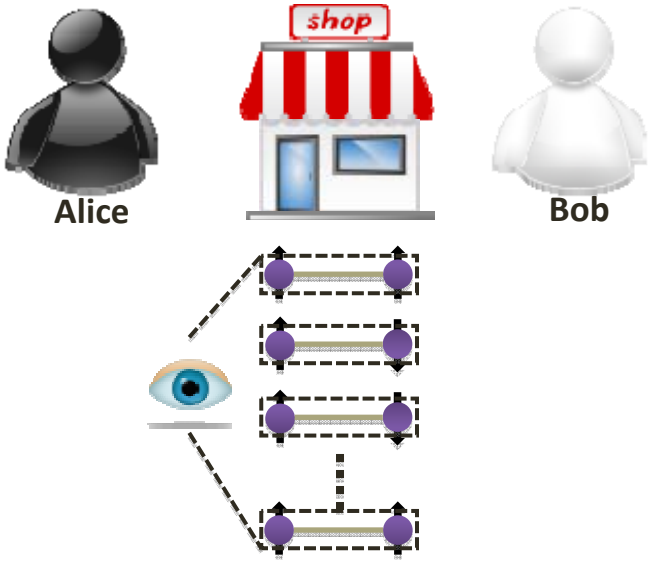
Quantum Cryptography for Future E-Commerce

- Step2: It then sends these sequences to them.
- Alice and Bob next encode their messages by performing quantum operations and send the encoded *qubits* back to the online shop.



Quantum Cryptography for Future E-Commerce

- Step3: The online shop then performs measurements on each entangled *qubits* pair and publishes the measurement outcomes.
- Alice and Bob now have accomplished their deal.
- By comparing the original entangled quibits prepared by the online shop and the measurement outcomes, they can know decipher messages from each other



Our Contributions (Secure Computation)

- Yao-Hsin Chou, Chi-Yuan Chen, Han-Chieh Chao, Jong Hyuk Park, and Rui-Kai Fan, "**Quantum Entanglement and Non-Locality based Secure Computation for Future Communication**," IET Information Security, Vol. 5, No. 1, pp. 69-79, March 2011.
- Chi-Yuan Chen, Yao-Hsin Chou, and Han-Chieh Chao, "**Distributed quantum entanglement sharing model for high-performance real-time system**," Soft Computing, Vol. 16, No. 3, pp. 427-435, 2012.

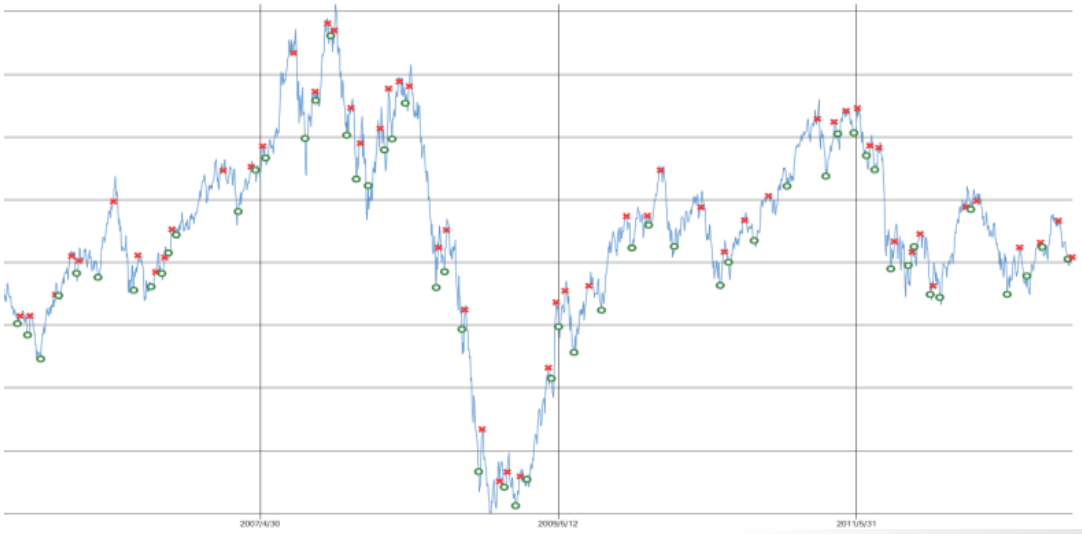
  - We proposed the Distributed Quantum Entanglement Sharing (DQES) model to share quantum entanglement with processors
  - Some possible applications such like
    - Database consistency,
    - Job scheduling,
    - System dependability, and
    - Reliable communication protocols

Our Contributions (furthermore …)

- Yao-Hsin Chou, Chi-Yuan Chen, Chia-Hui Chiu, and Han-Chieh Chao, "**Classical and Quantum-Inspired Electromagnetism-like Mechanism and its applications**," IET Control Theory & Applications, Vol. 6, No. 10, pp. 1424-1433, July 2012.
- Yao-Hsin Chou, Shu-Yu Kuo, Chi-Yuan Chen, and Han-Chieh Chao, "**A Rule-based Dynamic Decision-making Stock Trading System based on Quantum-Inspired Tabu Search algorithm**," under review.

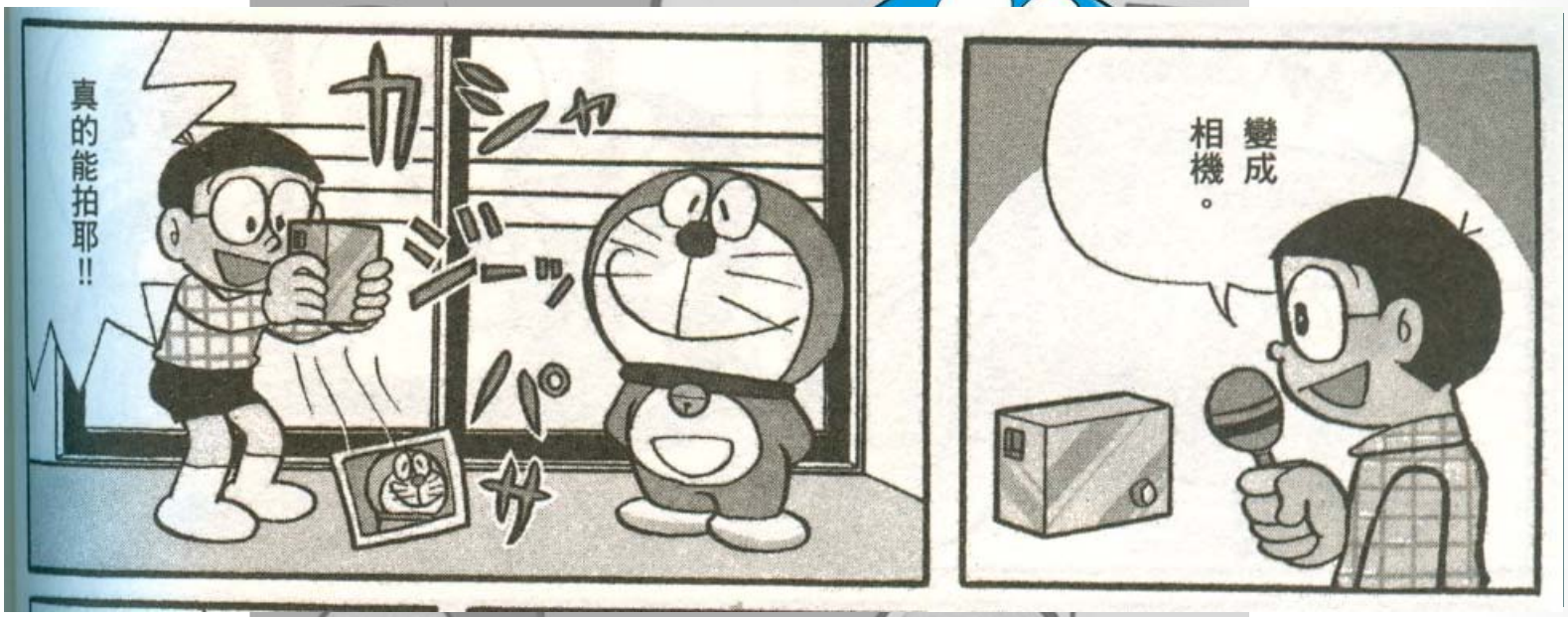
EXPERIMENTAL RESULTS OF THE 0-1 KNAPSACK PROBLEM

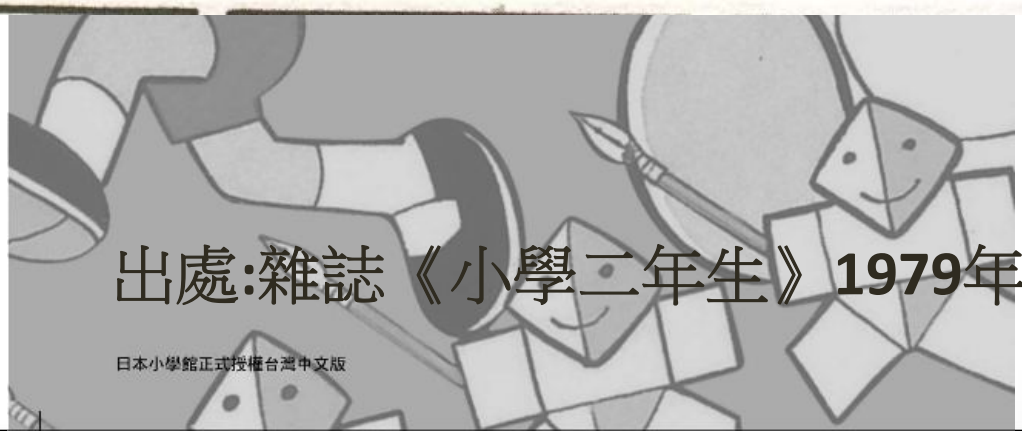
Number of items	Profit	GA	TS	QEA	QTS
100	*b.*	580.98	606.20	617.35	619.66
	m.	577.43	603.44	604.19	613.45
	w.	543.03	536.37	543.15	544.93
t(sec/run)		0.6407	0.5256	0.5821	0.4429
250	*b.*	1400.97	1494.03	1532.33	1546.55
	m.	1394.19	1485.69	1476.07	1514.88
	w.	1336.31	1324.33	1336.21	1338.55
t(sec/run)		0.7449	0.5353	0.9266	0.6739
500	*b.*	2766.55	2981.94	3030.37	3098.40
	m.	2754.88	2960.74	2906.63	3003.84
	w.	2666.85	2635.97	2667.84	2673.02
t(sec/run)		0.9712	0.5654	1.5083	1.0064



Quantum Teleportation

The original object is scanned in such a way as to extract all the information from it, then this information is transmitted to the receiving location and used to construct the replica, not necessarily from the actual material of the original, but perhaps from atoms of the same kinds, arranged in exactly the same pattern as the original.





出處:雜誌《小學二年生》1979年1月號

Conclusion

- When integrated circuits become smaller down to the nano level, quantum mechanics characteristics are revealed presenting greater computing performance possibilities.
- Quantum cryptography can be used in secret sharing, secure computation and secure direct communications as well.

- The future research …
  - Quantum networks
    - DWDM, Satellite, Quantum Internet …
  - Classical protocols based on quantum primitives

References

- [1] Lov K. Grover, “A fast quantum mechanical algorithm for database search,” *Proceedings of 28th Annual ACM Symposium on Theory of Computing (STOC)*, 1996, pp. 212-219.
- [2] P. W. Shor, “Algorithms for quantum computation: discrete logarithms and factoring,” *Proc. 35nd Annual Symposium on Foundations of Computer Science*, 1994, pp. 124-134.
- [3] C. H. Bennett and G. Brassard, “Quantum cryptography: public key distribution and coin tossing,” Proc. IEEE Int. Conf. on Computers, Systems & Signal processing Bangalore, India, 1984, pp.175-179.
- [4] Y. H. Chou, S. M. Chen, Y. T. Lin, C. Y. Chen and H. C. Chao, “Using GHZ-state for multiparty quantum secret sharing without code table,” *The Computer Journal*, 2012.
- [5] Y. H. Chou, C. Y. Chen, R. K. Fan, H. C. Chao and F. J. Lin, “Enhanced multiparty quantum secret sharing of classical messages by using entanglement swapping,” *IET Information Security*, vol. 6, Iss. 2, 2012, pp. 84-92.
- [6] Y. H. Chou, C. Y. Chen, H. C. Chao, J. H. Park R. K. Fan, “Quantum entanglement and non-locality based secure computation for future communication,” *IET Information Security*, 2011, pp. 69-79.
- [7] Y. H. Chou, F. J. Lin, and G. J. Zeng, “An Efficient Novel Online Shopping Mechanism based on Quantum Communication,” submitted for publication.
- [8] C. Y. Chen, Y. H. Chou and H. C. Chao, “Distributed quantum entanglement sharing model for high-performance real-time system,” *Soft Computing*, Vol. 16, No. 3, 2012, pp.427-435.
- [9] Y. H. Chou, I M. Tsai and S. Y. Kuo, “Quantum Boolean Circuits are 1-Testable”, *IEEE Transactions on Nanotechnology (TNANO)*, Vol. 7, Iss. 4, 2008, pp. 484-493.
- [10] C. Y. Chen, C. H. Chiu, H. C. Chao, “Classical and quantum-inspired electromagnetism-like mechanism and its applications,” *IET Control Theory & Applications*, Vol. 6, Iss. 10, 2012, pp. 1424-1433.

Thanks for your attention.
Q&A