

Continuous Quantum Secure Dialogue (CQSD)

Zichuan Wang
Shaokai Lin

Motivation

- Secure transmission of digital information more important than ever
- Many classical cryptography techniques no longer works in the quantum era
- Thus new protocol that are safe against quantum computer based attack are needed



Problem Definition

How do two parties communicate with each other easily, effectively, and securely?



Background

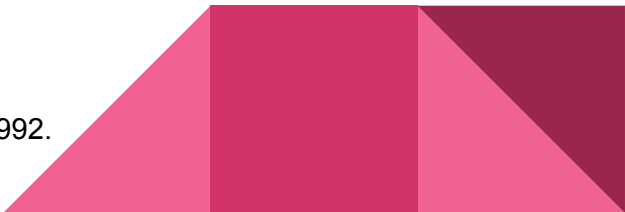
- Superdense Coding
- Qudits in High dimensional Hilbert space
- Quantum Cryptography



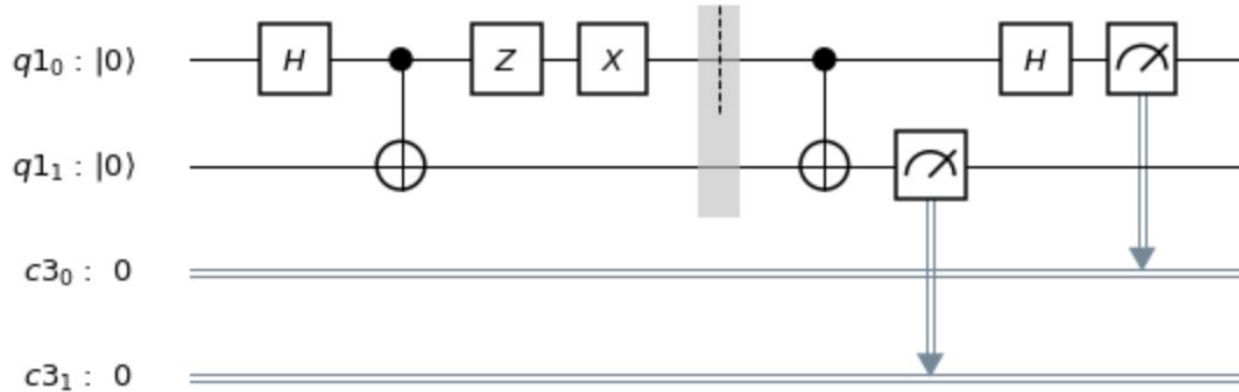
Background - Superdense Coding

- Two bits of classical information transmitted through one qubit
- Requires sharing EPR pair in advance
- Secure*

C. H. Bennett and S. J. Wiesner, "Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states," *Phys. Rev. Lett.*, vol. 69, no. 20, pp. 2881–2884, Nov. 1992.



Background - Superdense Coding



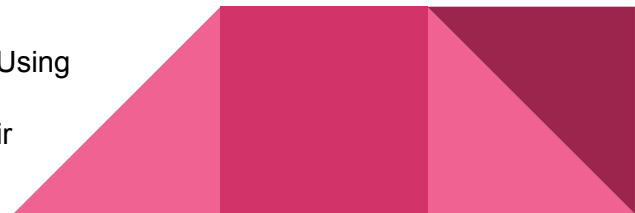
From Qiskit

Background - Qudits

- Qudits can be seen as a generalized qubit, which can be measured into $(1\dots n)$
- Higher-dimensional Hilbert space is involved
- Each particle carries more information
- Technically feasible

N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, "Security of Quantum Key Distribution Using d -Level Systems," *Phys. Rev. Lett.*, vol. 88, no. 12, p. 127902, Mar. 2002.

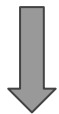
C. Reimer *et al.*, "Integrated generation of high-dimensional entangled photon states and their coherent control," in *Frontiers in Optics 2017 (2017)*, paper FTh3E.2, 2017, p. FTh3E.2.



Background - Quantum Cryptography

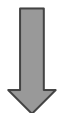
Quantum Key Distribution(QKD)

BB84, E91



Quantum Direct Secure Communication(QSDC)

EPR based QSDC



Quantum Direct Secure Dialogue(QSDD)

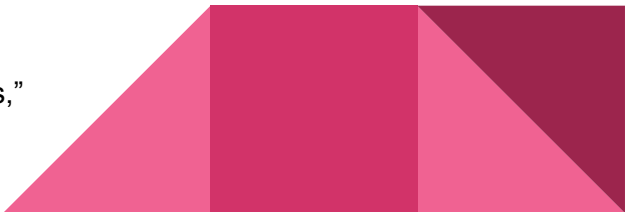
EPR based QSDD

C. Zheng and G. Long, "Quantum secure direct dialogue using Einstein-Podolsky-Rosen pairs,"
Sci. China Phys. Mech. Astron., vol. 57, no. 7, pp. 1238–1243, Jul. 2014.

Background - QSDD

- Secure
- Unnecessary security check overhead in multi-round communication
- Not flexible

C. Zheng and G. Long, “Quantum secure direct dialogue using Einstein-Podolsky-Rosen pairs,”
Sci. China Phys. Mech. Astron., vol. 57, no. 7, pp. 1238–1243, Jul. 2014.



How QSDD works

Alice

Bob



White: ground state

Grey: EPR pair

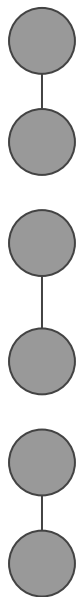
Color: message encoded

Preparation

Alice

Bob

(Prepares 3 EPR pairs in Ψ^- basis)



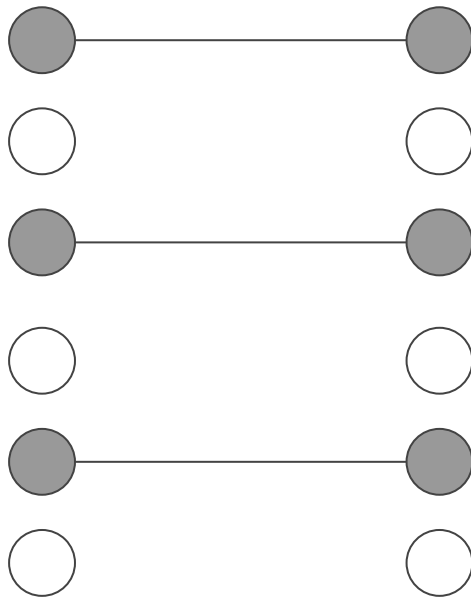
White: ground state
Grey: EPR pair
Color: message encoded

Preparation

Alice

Bob

(Alice sends half of the EPR pairs to Bob)



Transparent: ground state

Grey: EPR pair

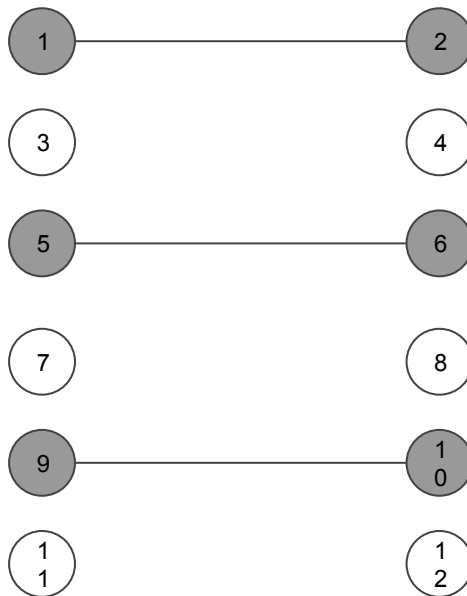
Color: message encoded

Initial Eavesdropping Check

Alice

Bob

"Let's measure state 5 & 6 to check if there is an Eve."



Transparent: ground state

Grey: EPR pair

Color: message encoded

Initial Eavesdropping Check

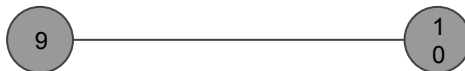
Alice Bob

"I got 0."
"There is an Eve!"

"Me too."
"Oh no!"

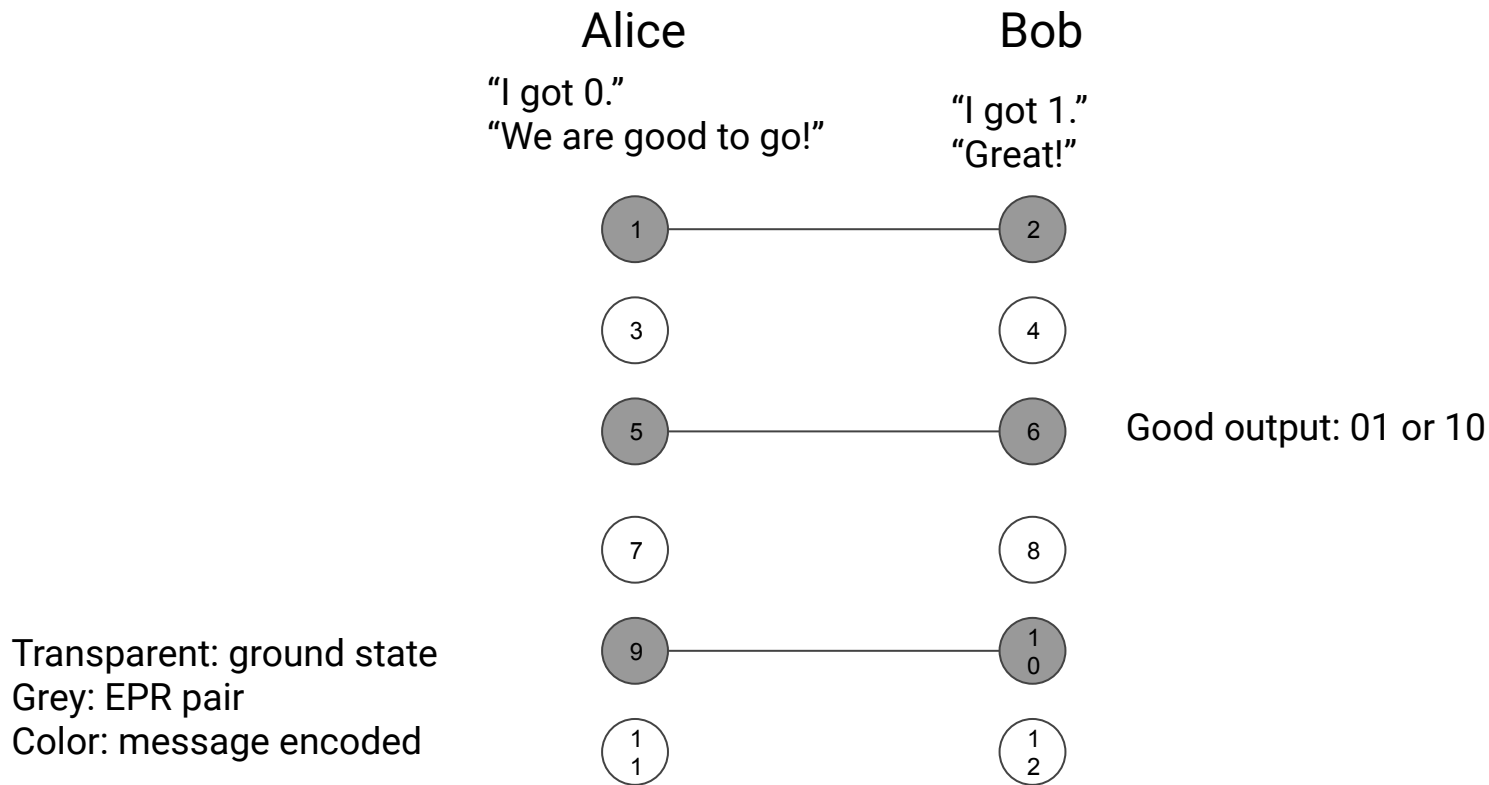


Bad output: 00 or 11



Transparent: ground state
Grey: EPR pair
Color: message encoded

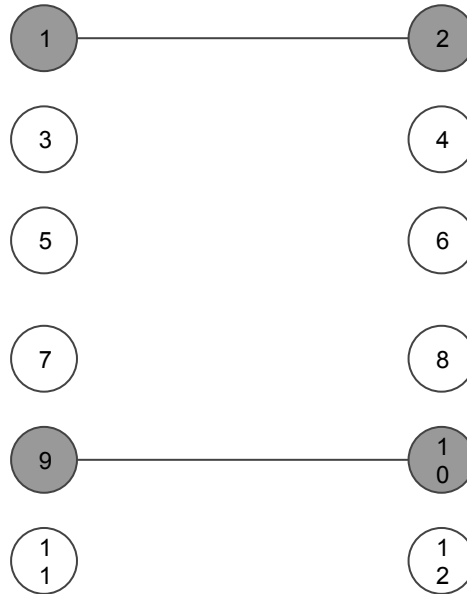
Initial Eavesdropping Check



Alice Speaks to Bob

Alice

Bob



Transparent: ground state

Grey: EPR pair

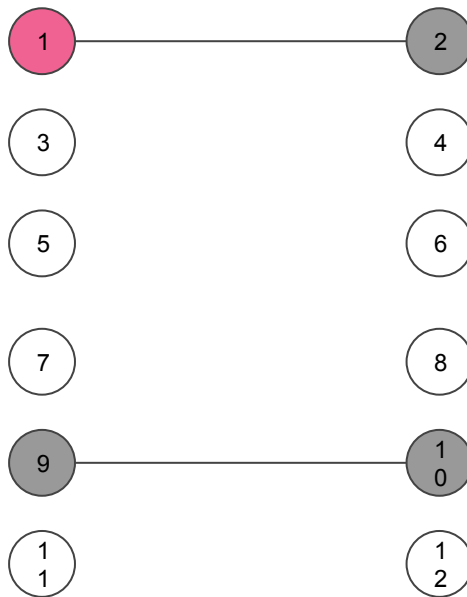
Color: message encoded

Alice Speaks to Bob

Alice

Bob

(Alice encodes 10)



Transparent: ground state

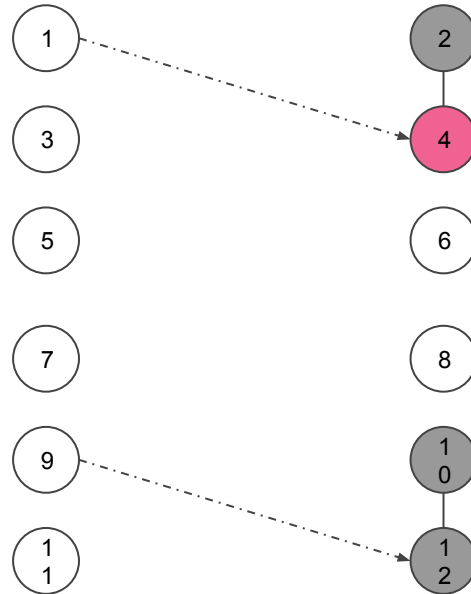
Grey: EPR pair

Color: message encoded

Alice Speaks to Bob

Alice

Bob



Transparent: ground state
Grey: EPR pair
Color: message encoded

Alice Speaks to Bob

Alice

Bob

"Eavesdropping check is passed!"

1

3

5

7

9

1
1

2

4

6

8

1
0

1
2

Transparent: ground state
Grey: EPR pair
Color: message encoded

Output: 10 or 01

Alice Speaks to Bob

Alice

Bob

"I got 10!"

1

3

5

7

9

1
1

2

4

6

8

1
0

1
2

Output: 10

Transparent: ground state

Grey: EPR pair

Color: message encoded

Alice Speaks to Bob

Alice

Bob

(If Bob has remaining EPR pair left, he can send back message in the same fashion. If all EPR pairs have been used, Alice and Bob will repeat from step 1 to continue conversation.)

1

2

3

4

5

6

7

8

9

1
0

1
1

1
2

Transparent: ground state

Grey: EPR pair

Color: message encoded

Advantages of QSDD over its predecessors

- No need for classical communication channel to read out message (unlike QKD, DQKC)
- High capacity. One qubit carries two bits of information
- Efficient. Every EPR pair is used for communication and checking.
- Secure. QSDD is based on DQKC, which is proven secure.



Problems with QSDD

- EPR pairs constantly run out. Dialogue has to halt.
- No regulation on message size. More classical communication is required to coordinate qubit transmission.



Continuous Quantum Secure Dialogue (CQSD)

How CQSD works

Alice

Bob



White: ground state

Grey: EPR pair

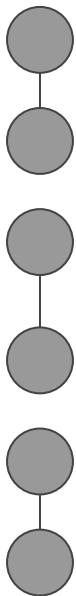
Color: message encoded

Preparation

Alice

Bob

(Prepares 3 EPR pairs in Ψ^- basis)



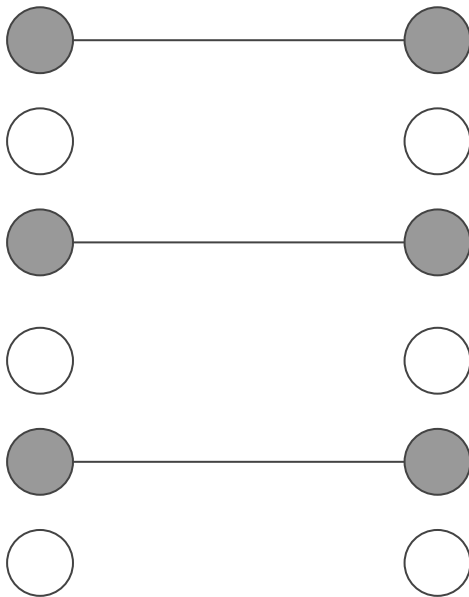
White: ground state
Grey: EPR pair
Color: message encoded

Preparation

Alice

Bob

(Alice sends half of the EPR pairs to Bob)



Transparent: ground state

Grey: EPR pair

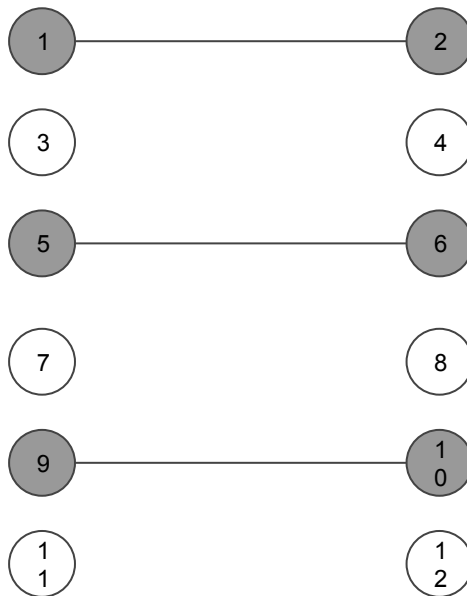
Color: message encoded

Initial Eavesdropping Check

Alice

Bob

"Let's measure state 5 & 6 to check if there is an Eve."



Transparent: ground state

Grey: EPR pair

Color: message encoded

Initial Eavesdropping Check

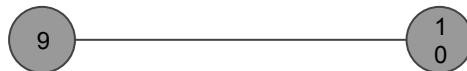
Alice Bob

"I got 0."

"There is an Eve!"

"Me too."

"Oh no!"



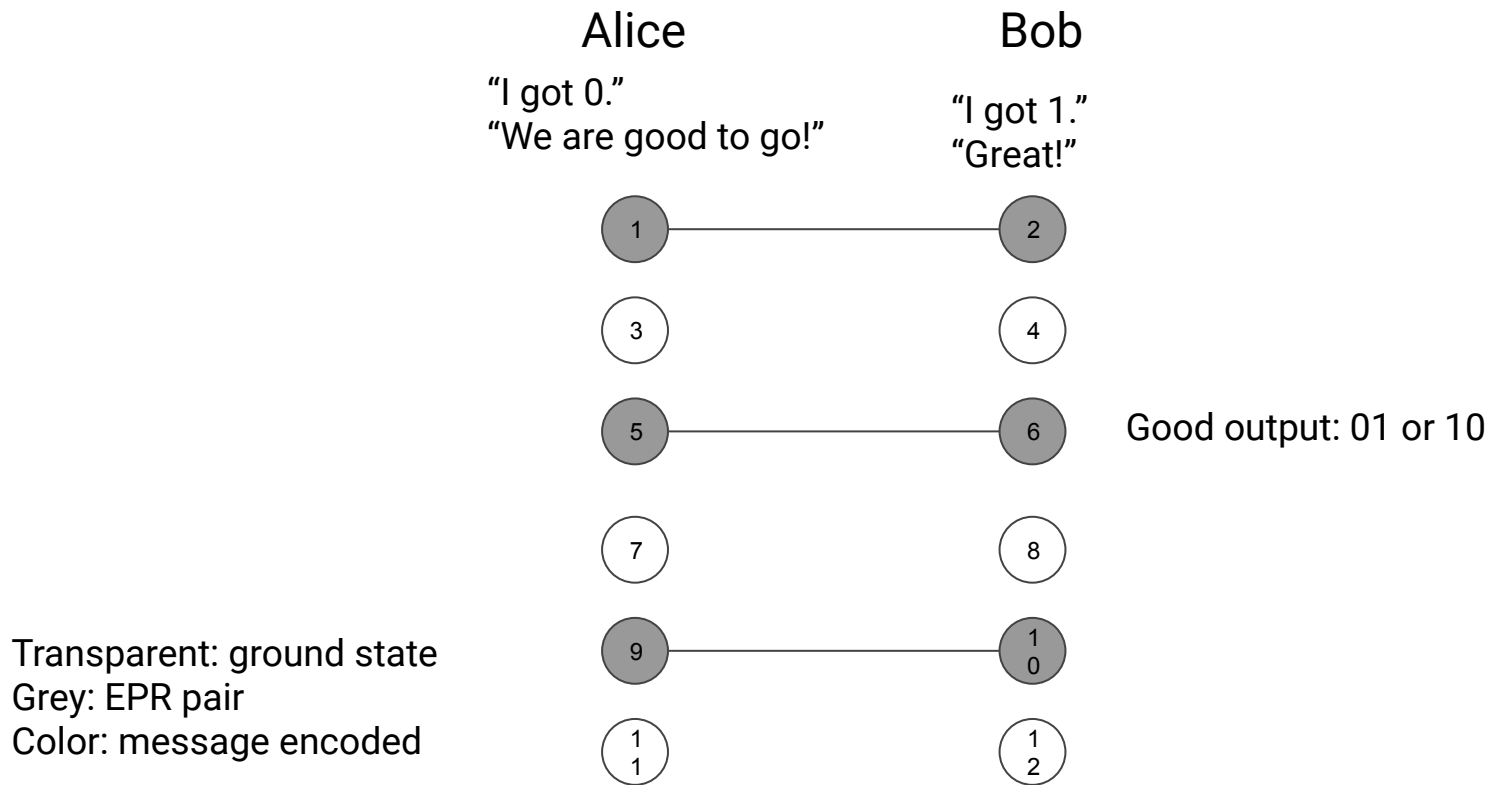
Bad output: 00 or 11

Transparent: ground state

Grey: EPR pair

Color: message encoded

Initial Eavesdropping Check



Alice Speaks to Bob

Alice

Bob



All qubits used for
messaging



All qubits used for
eavesdropping check



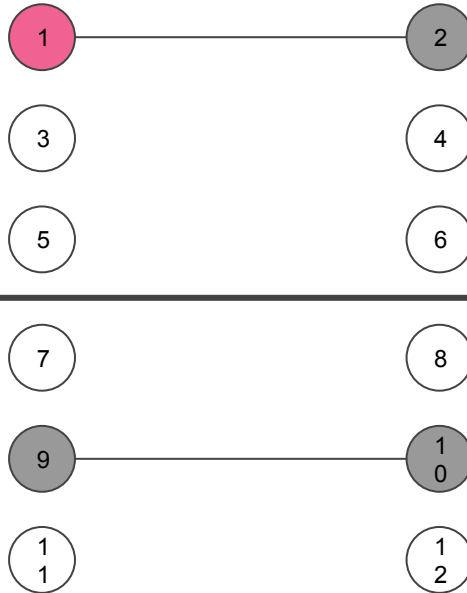
Transparent: ground state
Grey: EPR pair
Color: message encoded

Alice Speaks to Bob

Alice

Bob

(Encodes a message, say "10")



Transparent: ground state

Grey: EPR pair

Color: message encoded

Alice Speaks to Bob

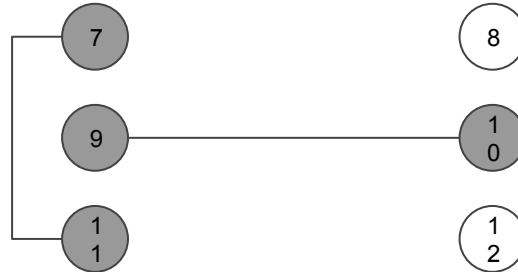
Alice

Bob

(Prepares two new EPR pairs)



Transparent: ground state
Grey: EPR pair
Color: message encoded

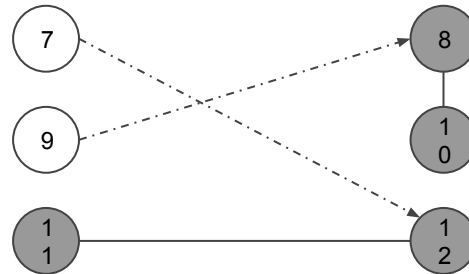
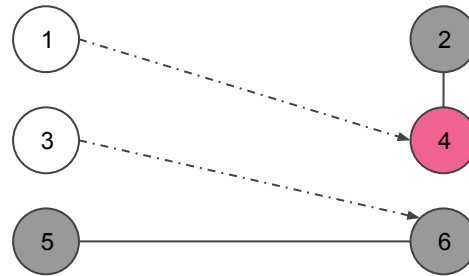


Alice Speaks to Bob

Alice

Bob

(sends four states to Bob)



Transparent: ground state
Grey: EPR pair
Color: message encoded

Alice Speaks to Bob

Alice

Bob

(sends four states to Bob)

1

2

3

4

5

6

7

8

9

1
0

1
1

1
2

Transparent: ground state
Grey: EPR pair
Color: message encoded

Alice Speaks to Bob

Alice

Bob

"The eavesdropping check failed. There is an Eve!"

1

2

3

4

5

6

7

8

9

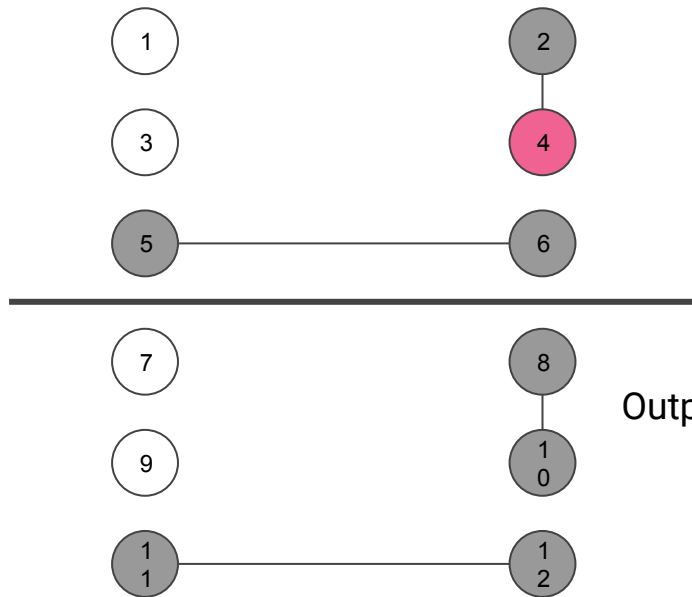
1
0

1
1

1
2

Output: 11 or 00

Transparent: ground state
Grey: EPR pair
Color: message encoded



Alice Speaks to Bob

Alice

Bob

"The eavesdropping
check is passed!"

1

2

3

4

5

6

7

8

9

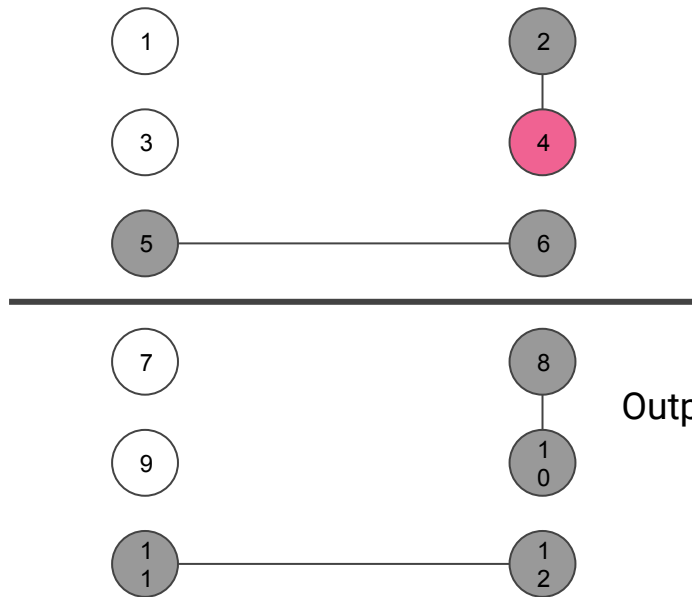
1
0

1
1

1
2

Output: 10 or 01

Transparent: ground state
Grey: EPR pair
Color: message encoded



Alice Speaks to Bob

Alice

Bob

"I get 10!"

Output: 10

1

2

3

4

5

6

7

8

9

1
0

1
1

1
2

Transparent: ground state
Grey: EPR pair
Color: message encoded

Alice Speaks to Bob

Alice

Bob

1

2

3

4

5

6

7

8

9

1
0

1
1

1
2

Transparent: ground state
Grey: EPR pair
Color: message encoded

Recap: Before Alice Speaks to Bob

Alice

Bob



All qubits used for
messaging



All qubits used for
eavesdropping check



Transparent: ground state
Grey: EPR pair
Color: message encoded

Bob Speaks to Alice

Alice

Bob

“I can talk to you right back, without halting the communication to prepare EPR pairs. And I don’t need to redo the initial handshake, since the quantum channel is proven safe during initial check. ”

1

2

3

4

5

6

7

8

9

1
0

1
1

1
2

Transparent: ground state
Grey: EPR pair
Color: message encoded

Bob Speaks to Alice

Alice

Bob

1

3

5

7

9

1
1

2

4

6

8

1
0

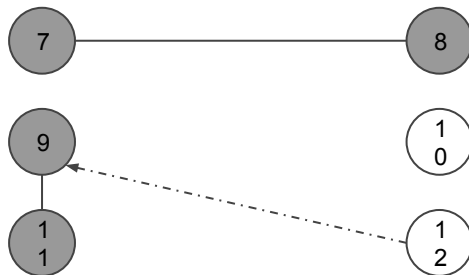
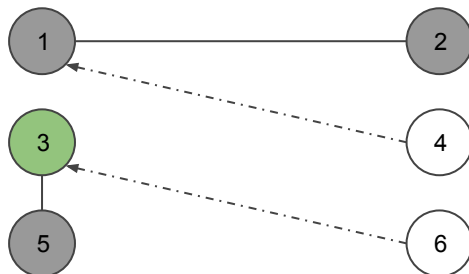
1
2

Transparent: ground state
Grey: EPR pair
Color: message encoded



Bob Speaks to Alice

Alice Bob



Transparent: ground state
Grey: EPR pair
Color: message encoded

Bob Speaks to Alice

Alice

Bob



Transparent: ground state

Grey: EPR pair

Color: message encoded

Advantages over QSDD

1. Continuous message flow. This can mean faster communication, since many handshakes via classical communications from QSDD are eliminated.
2. Fixed-size message. No longer deals with the communication overhead generated from the dynamic size of a message.
3. A protocol that can be realistically implemented.
CQSD can run on a minimum 6-qubit device and can scale according to the capability of a device.




Implementation



Generalization to Higher Dimensions

- Recall Qudits can be seen as a generalized qubit
- Generalized Bell-basis states takes the place of regular Bell states
- Measurement done in conjugate measuring basis
- Each particle carries more information: $\log_2 d^2$

C. Wang, F.-G. Deng, Y.-S. Li, X.-S. Liu, and G. L. Long, "Quantum secure direct communication with high-dimension quantum superdense coding," *Phys. Rev. A*, vol. 71, no. 4, p. 044305, Apr. 2005.



Questions?



Reference

- [1] P. W. Shor, “Algorithms for quantum computation: discrete logarithms and factoring,” in *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 1994, pp. 124–134.
- [2] A. Ekert and R. Jozsa, “Quantum computation and Shor’s factoring algorithm,” *Rev. Mod. Phys.*, vol. 68, no. 3, pp. 733–753, Jul. 1996.
- [3] C. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” presented at the International Conference on Computers, Systems & Signal Processing, Bangalore, India, 1984, pp. 175–179.
- [4] A. K. Ekert, “Quantum cryptography based on Bell’s theorem,” *Phys. Rev. Lett.*, vol. 67, no. 6, pp. 661–663, Aug. 1991.
- [5] K. Boström and T. Felbinger, “Deterministic Secure Direct Communication Using Entanglement,” *Phys. Rev. Lett.*, vol. 89, no. 18, p. 187902, Oct. 2002.
- [6] W. Chuan, L. Yan-Song, and L. Gui-Lu, “Secure Direct Communication Using Ensembles with the Same Compressed Density Matrix,” *Commun. Theor. Phys.*, vol. 46, no. 3, pp. 440–442, Sep. 2006.
- [7] F.-G. Deng and G. L. Long, “Secure direct communication with a quantum one-time pad,” *Phys. Rev. A*, vol. 69, no. 5, p. 052319, May 2004.
- [8] L. Dong, H.-K. Dong, X.-M. Xiu, Y.-J. Gao, and F. Chi, “Quantum secure direct communication using a six-qubit maximally entangled state with dense coding,” *Int. J. Quantum Inf.*, vol. 07, no. 03, pp. 645–651, Apr. 2009.
- [9] F.-G. Deng, G. L. Long, and X.-S. Liu, “Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block,” *Phys. Rev. A*, vol. 68, no. 4, p. 042317, Oct. 2003.
- [10] C. Wang, F.-G. Deng, Y.-S. Li, X.-S. Liu, and G. L. Long, “Quantum secure direct communication with high-dimension quantum superdense coding,” *Phys. Rev. A*, vol. 71, no. 4, p. 044305, Apr. 2005.

Reference

- [11] X. Yin, W. Ma, D. Shen, and C. Hao, “Efficient Three-Party Quantum Secure Direct Communication with EPR Pairs,” 2013.
- [12] M.-Y. Wang and F.-L. Yan, “Three-party simultaneous quantum secure direct communication scheme with EPR pairs,” *Chin. Phys. Lett.*, vol. 24, no. 9, pp. 2486–2488, 2007.
- [13] T. Gao, F.-L. Yan, and Z.-X. Wang, “Quantum secure direct communication by Einstein-Podolsky-Rosen pairs and entanglement swapping,” *Il Nuovo Cimento B*, vol. 119, no. 3, pp. 313–318, Sep. 2004.
- [14] A. Einstein, B. Podolsky, and N. Rosen, “Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?,” *Phys. Rev.*, vol. 47, no. 10, pp. 777–780, May 1935.
- [15] C. H. Bennett and S. J. Wiesner, “Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states,” *Phys. Rev. Lett.*, vol. 69, no. 20, pp. 2881–2884, Nov. 1992.
- [16] C. Zheng and G. Long, “Quantum secure direct dialogue using Einstein-Podolsky-Rosen pairs,” *Sci. China Phys. Mech. Astron.*, vol. 57, no. 7, pp. 1238–1243, Jul. 2014.
- [17] T.-Y. Ye, “Quantum secure direct dialogue over collective noise channels based on logical Bell states,” *Quantum Inf. Process.*, vol. 14, no. 4, pp. 1487–1499, Apr. 2015.
- [18] L. He, T. Wang, and C. Wang, “High-Dimensional Bell State Analysis for Photon-Atoms Hybrid System,” *Int. J. Theor. Phys.*, vol. 58, no. 2, pp. 451–462, Feb. 2019.
- [19] H. Zhang *et al.*, “An arbitrary two-particle high-dimensional Bell state measurement by auxiliary entanglement,” *ArXiv190101373 Quant-Ph*, Jan. 2019.
- [20] D. Sych and G. Leuchs, “A complete basis of generalized Bell states,” *New J. Phys.*, vol. 11, no. 1, p. 013006, Jan. 2009.

Reference

- [21] H. Bechmann-Pasquinucci and A. Peres, “Quantum Cryptography with 3-State Systems,” *Phys. Rev. Lett.*, vol. 85, no. 15, pp. 3313–3316, Oct. 2000.
- [22] M. Bourennane, A. Karlsson, and G. Björk, “Quantum key distribution using multilevel encoding,” *Phys. Rev. A*, vol. 64, no. 1, p. 012306, Jun. 2001.
- [23] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, “Security of Quantum Key Distribution Using d -Level Systems,” *Phys. Rev. Lett.*, vol. 88, no. 12, p. 127902, Mar. 2002.
- [24] Z. You-Bang, Z. Ling-Ling, W. Yu-Wu, and Z. Qun-Yong, “Quantum Dialogue by Using Non-Symmetric Quantum Channel,” *Commun. Theor. Phys.*, vol. 53, no. 4, pp. 648–652, Apr. 2010.
- [25] C. Reimer *et al.*, “Integrated generation of high-dimensional entangled photon states and their coherent control,” in *Frontiers in Optics 2017 (2017)*, paper FTh3E.2, 2017, p. FTh3E.2.





Thank you!