

# A new quantum bit commitment protocol with correctness proof in ZX-calculus

Xin Sun

Sun Yat-sen University, China

The John Paul II Catholic University of Lublin, Poland

**Quanlong Wang**

University of Oxford, UK

CLAP Scotland, 20 November 2017

# Outline

Some background on quantum bit commitment

Our QBC protocol

Conclusion

# Bit commitment

- ▶ Bit commitment, used in a wide range of cryptographic protocols (e.g. zero-knowledge proof, multiparty secure computation, and oblivious transfer), consists of two phases, namely: commit and opening.

# Bit commitment

- ▶ Bit commitment, used in a wide range of cryptographic protocols (e.g. zero-knowledge proof, multiparty secure computation, and oblivious transfer), consists of two phases, namely: commit and opening.
- ▶ In the commit phase, the sender chooses a bit  $a$  ( $a = 0$  or  $1$ ) which he/she wishes to commit to the receiver, and thus presents the receiver some evidence about the bit. The committed bit cannot be known by the receiver prior to the opening phase.

# Bit commitment

- ▶ In the opening phase, the sender announces some information for reconstructing  $a$ . The receiver then reconstructs a bit  $a'$  using the sender's evidence and announcement. The commitment will be accepted by the receiver if, and only if,  $a' = a$ .

# Bit commitment

- ▶ In the opening phase, the sender announces some information for reconstructing  $a$ . The receiver then reconstructs a bit  $a'$  using the sender's evidence and announcement. The commitment will be accepted by the receiver if, and only if,  $a' = a$ .
- ▶ Bit commitment is also useful in access control in cloud computing because they can be used to protect privacy, by creating anonymous credential [2, 4] or hiding access control policy [3].

# Quantum Bit commitment

- ▶ The first quantum bit commitment (QBC) protocol is proposed by Bennett and Brassard in 1984 [1]. A QBC protocol is unconditionally secure if any cheating can be detected with a probability arbitrarily close to 1.

# Quantum Bit commitment

- ▶ The first quantum bit commitment (QBC) protocol is proposed by Bennett and Brassard in 1984 [1]. A QBC protocol is unconditionally secure if any cheating can be detected with a probability arbitrarily close to 1.
- ▶ Here, the sender's cheating means that the sender changes the committed bit after the commit phase, while the receiver's cheating means that the receiver learns the committed bit before the opening phase.



# Quantum Bit commitment

- ▶ A number of QBC protocols are designed to achieve unconditional security, such as those of [2, 3]. However, according to the Mayers-Lo-Chau (MLC) no-go theorem [2, 1], unconditionally secure QBC can never be achieved in principle, except for relativistic QBC [2, 3] and infinite-dimensional systems QBC.

# Quantum Bit commitment

- ▶ A number of QBC protocols are designed to achieve unconditional security, such as those of [2, 3]. However, according to the Mayers-Lo-Chau (MLC) no-go theorem [2, 1], unconditionally secure QBC can never be achieved in principle, except for relativistic QBC [2, 3] and infinite-dimensional systems QBC.
- ▶ Although unconditional secure QBC is impossible, several QBC protocols satisfy some other notions of security, such as cheat sensitive quantum bit commitment (CSQBC) protocols [3, 1, 2, 2].

# Quantum Bit commitment

- ▶ A number of QBC protocols are designed to achieve unconditional security, such as those of [2, 3]. However, according to the Mayers-Lo-Chau (MLC) no-go theorem [2, 1], unconditionally secure QBC can never be achieved in principle, except for relativistic QBC [2, 3] and infinite-dimensional systems QBC.
- ▶ Although unconditional secure QBC is impossible, several QBC protocols satisfy some other notions of security, such as cheat sensitive quantum bit commitment (CSQBC) protocols [3, 1, 2, 2].
- ▶ In CSQBC protocols, the probability for detecting cheating is merely required to be non-zero.

# Quantum Bit commitment

- ▶ More recently, Nagy [3, 1] proposed a QBC protocol in which cheating can be detected with a high probability.

# Quantum Bit commitment

- ▶ More recently, Nagy [3, 1] proposed a QBC protocol in which cheating can be detected with a high probability.
- ▶ Here we propose a QBC protocol which is more efficient and secure than Nagy's protocol. As far as we know, the security of our protocol is better than all the existing CSQBC protocols [3, 1, 2, 2].

# Quantum Bit commitment

- ▶ More recently, Nagy [3, 1] proposed a QBC protocol in which cheating can be detected with a high probability.
- ▶ Here we propose a QBC protocol which is more efficient and secure than Nagy's protocol. As far as we know, the security of our protocol is better than all the existing CSQBC protocols [3, 1, 2, 2].
- ▶ Moreover, no entanglement is used in our protocol, which makes it implementable by the current technology.

# The commit phase

The commit phase contains the following steps:

- ▶ 1. The receiver generates a sequence of  $n$  qubits, where  $n$  is a multiple of 4, such that the first  $\frac{n}{4}$  qubits are  $|0\rangle$ , the second  $\frac{n}{4}$  qubits are  $X(\frac{\pi}{2})|0\rangle = |i\rangle$ , the third  $\frac{n}{4}$  qubits are  $X(\pi)|0\rangle = |1\rangle$ , and the fourth  $\frac{n}{4}$  qubits are  $X(\frac{3\pi}{2})|0\rangle = |\bar{i}\rangle$ . Such a sequence is called a *uniform* sequence. The receiver permutes the sequence randomly and sends it to the sender. This step is repeated  $m$  times.

## The commit phase

- ▶ 2. The sender chooses  $m - 1$  sequences and ask the receiver to reveal, qubit by qubit, which state it was prepared. Then, the sender measures those qubits in the appropriate basis to verify whether the receiver has prepared those qubits in the required specification: the  $\{|0\rangle, |1\rangle\}$  basis for qubits  $|0\rangle$  and  $|1\rangle$  and the  $\{|i\rangle, |\bar{i}\rangle\}$  basis for qubits  $|i\rangle$  and  $|\bar{i}\rangle$ . If the sender detects that the receiver has prepared a sequence that is not uniform, then the sender has detected the receiver's cheating.



# The commit phase

- ▶ 3. The sender commits 2 bits by applying quantum operations on the only sequence left. If the sender decides to commit 00/01/10/11, then he/she applies  $X(0)/X(\frac{\pi}{2})/X(\pi)/X(\frac{3\pi}{2})$  to all qubits in the sequence, respectively. Then, the sender permutes the sequence and sends it to the receiver.
- ▶ 4. The receiver measures each received qubit either in the  $\{|0\rangle, |1\rangle\}$  basis or in the  $\{|i\rangle, |\bar{i}\rangle\}$  basis which is chosen uniformly at random.

# The opening phase

The opening phase contains the following steps:

- ▶ 1. The sender reveals which permutation he/she has applied to the sequence.
- ▶ 2. Based on the information of the sender's permutation, the receiver is able to determine for each qubit if it was measured in the correct basis: for a qubit that was originally in state  $|0\rangle$  or  $|1\rangle$ , the correct basis is the  $\{|0\rangle, |1\rangle\}$  basis, for other qubits the correct basis is the other basis.

# The opening phase

Now, the receiver can recover the bits committed by the sender as follows:

- ▶ (a). If the sender committed to 00, all the qubits measured in the correct basis must yield a state which is the same as the original one.
- ▶ (b). If the sender committed to 10, all the qubits measured in the correct basis must yield a state which can be recovered to the original one by applying a  $X(\pi)$  gate afterwards.

# The opening phase

- ▶ (c). If the sender committed to 01, all the qubits measured in the incorrect basis must yield a state which can be recovered to the original one by applying a  $X(\frac{3\pi}{2})$  gate afterwards.
- ▶ (d). If the sender committed to 11, all the qubits measured in the incorrect basis must yield a state which can be recovered to the original one by applying a  $X(\frac{\pi}{2})$  gate afterwards.

All other cases are classified as the sender's cheating.

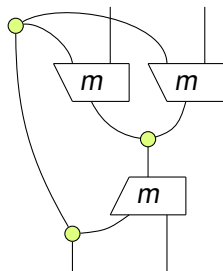
## Correctness

We show the correctness of our protocol only in the graphical language ZX-calculus which makes the demonstration pretty intuitive while still strict. Note that we ignore scalars in the graphical calculus.

## Correctness

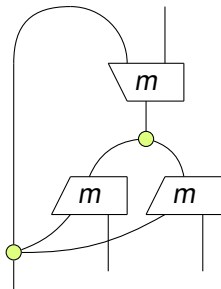
We show the correctness of our protocol only in the graphical language ZX-calculus which makes the demonstration pretty intuitive while still strict. Note that we ignore scalars in the graphical calculus.

Firstly, the bases involved in this protocol are a pair of complementary bases which can be represented by a controlled basis as follows ( $m$  is a controlled unitary):



# Correctness

A controlled measurement can be represented as follows:



## Correctness

Now specify the  $m$  box. Clearly,  $m$  is a controlled unitary which transforms the basis  $\{|0\rangle, |1\rangle\}$  into itself in the controlled state  $|0\rangle$  as well as sending the basis  $\{|i\rangle, |\bar{i}\rangle\}$  into  $\{|0\rangle, |1\rangle\}$  in the controlled state  $|1\rangle$ , thus in a matrix form  $m = \begin{pmatrix} I & U \end{pmatrix}$ , where

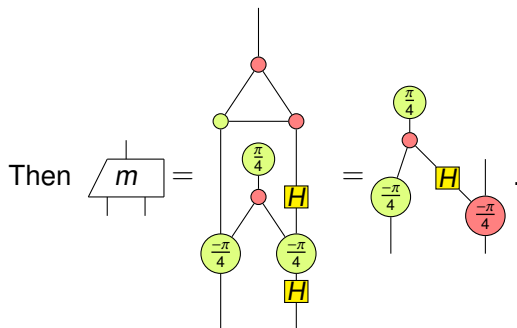
$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad U = |0\rangle\langle i| + |1\rangle\langle \bar{i}| = \frac{1}{2} \begin{pmatrix} 1-i & 1+i \\ 1+i & 1-i \end{pmatrix} = X\left(\frac{-\pi}{2}\right).$$



## Correctness

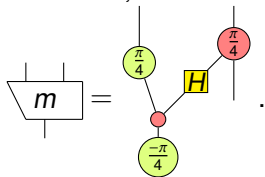
To represent  $m$  in a diagrammatic form, we decompose it into three components such that each component has a simple graphical representation:

$$(I \ U) = (I \ X(\pi)) \begin{pmatrix} I & \\ & X(\pi) \end{pmatrix} \begin{pmatrix} I & \\ & U \end{pmatrix}.$$



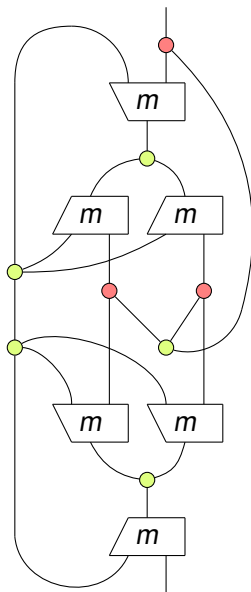
# Correctness

Therefore,



## Correctness

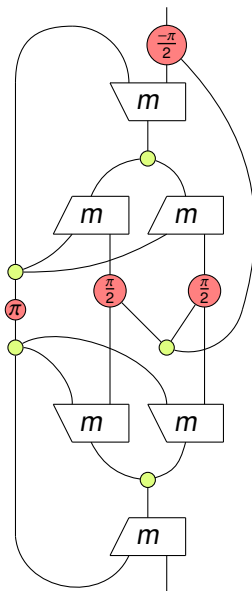
Now the the first two cases (a) and (b) of the opening phase is



(1)

## Correctness

The last two cases (c) and (d) of the opening phase is



(2)

# Correctness

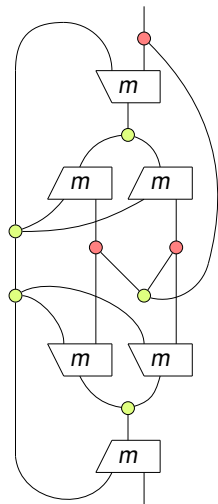
If the bits committed can be recovered, then both diagram (1) and (2) should be reduced to an identity (straight line). We prove this correctness by rewriting diagrams step by step.

# Correctness

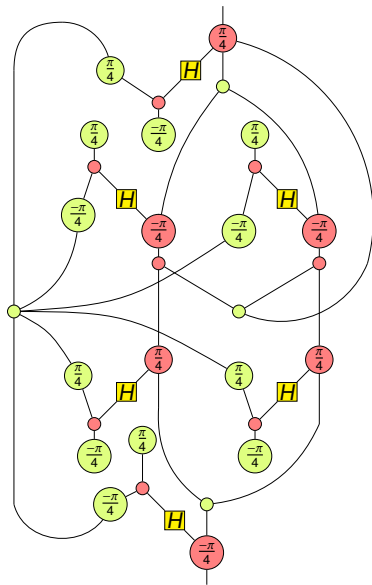
If the bits committed can be recovered, then both diagram (1) and (2) should be reduced to an identity (straight line). We prove this correctness by rewriting diagrams step by step.

For the first two cases (a) and (b) of the opening phase, we have

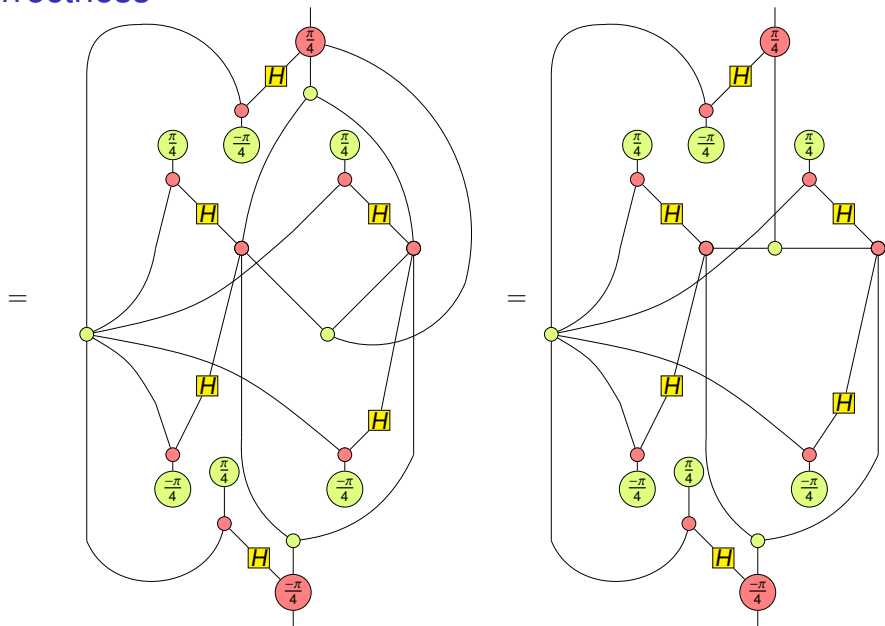
# Correctness



=

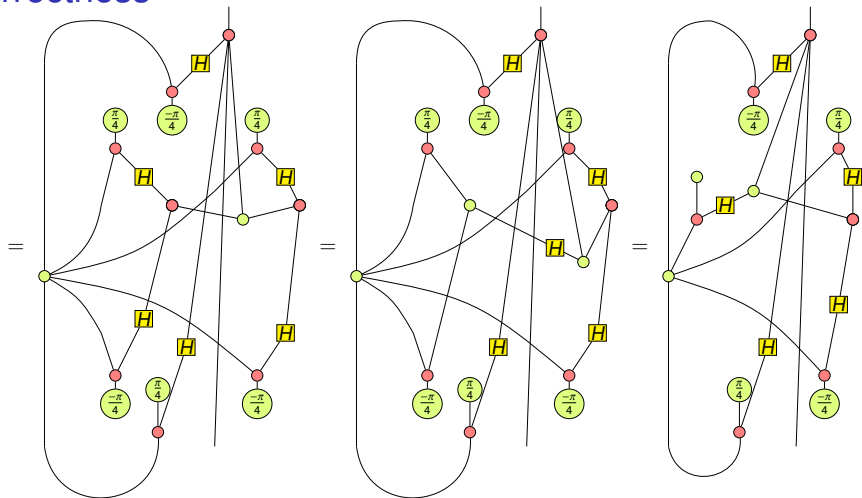


# Correctness

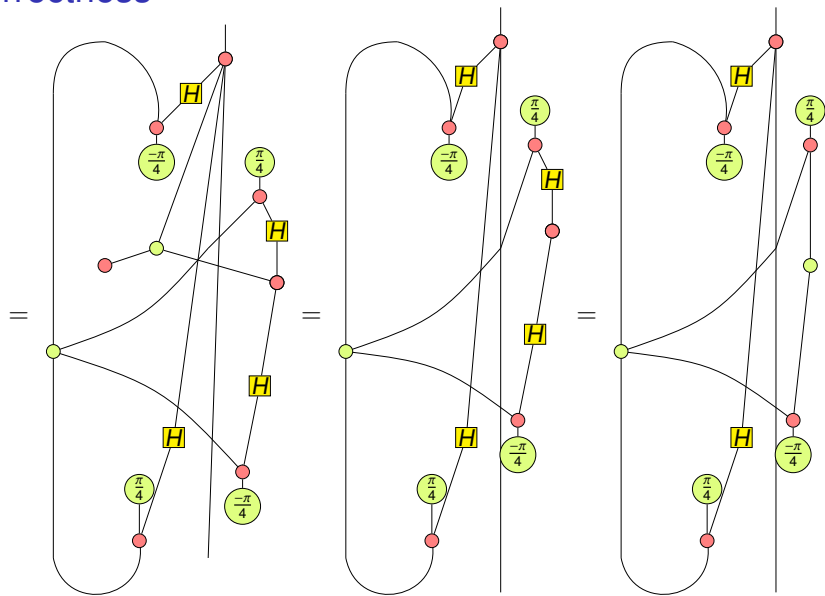




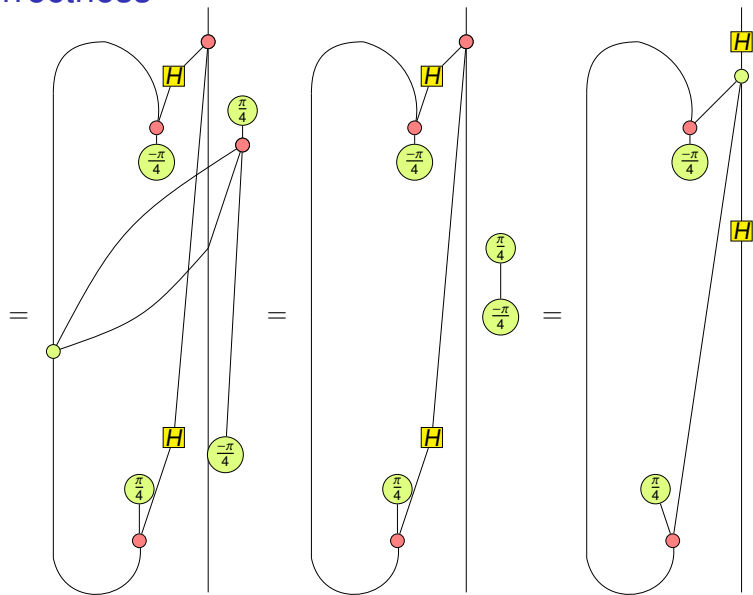
# Correctness



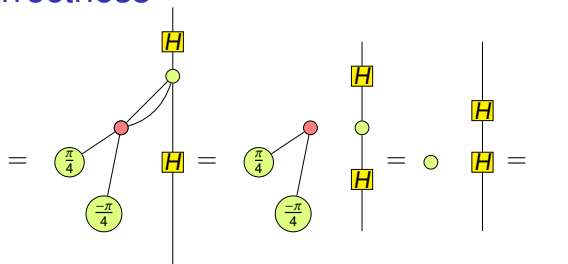
# Correctness



# Correctness

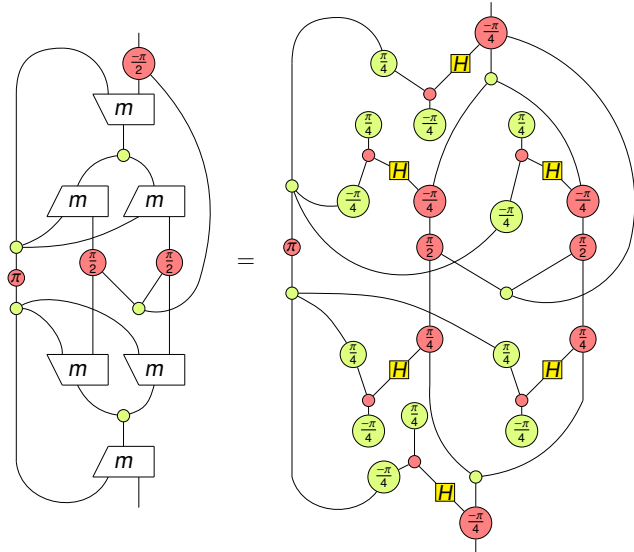


# Correctness

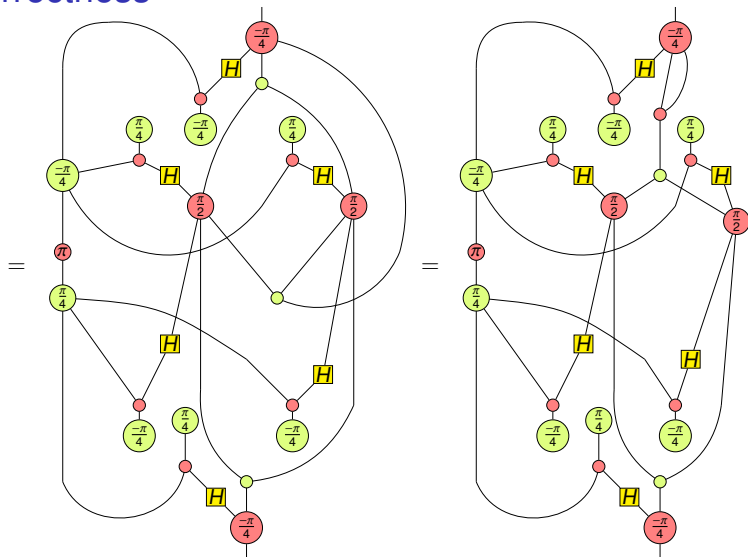


# Correctness

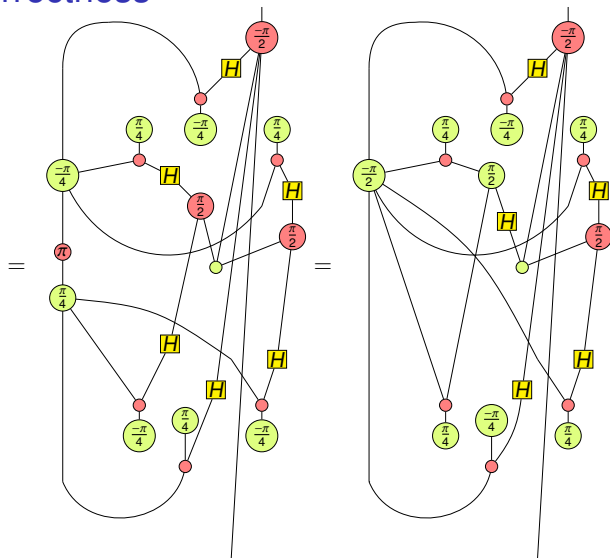
For the last two cases (c) and (d) of the opening phase, we have



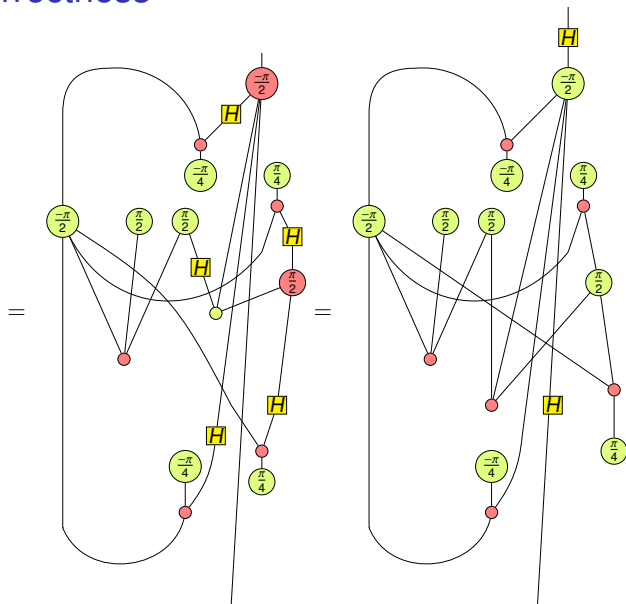
# Correctness



# Correctness

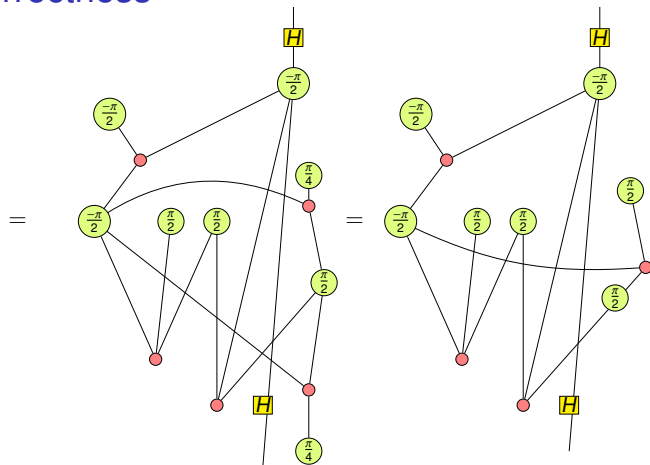


# Correctness

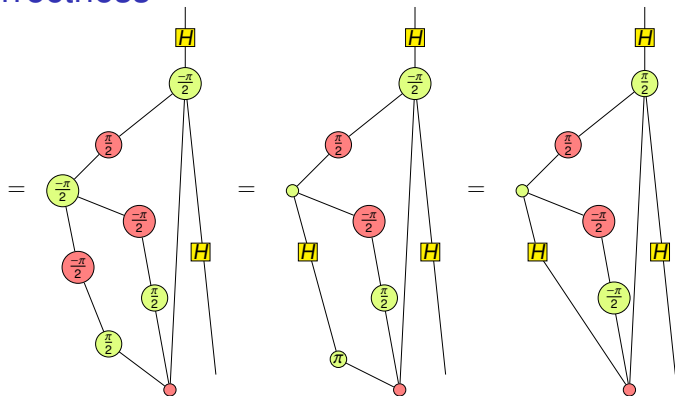




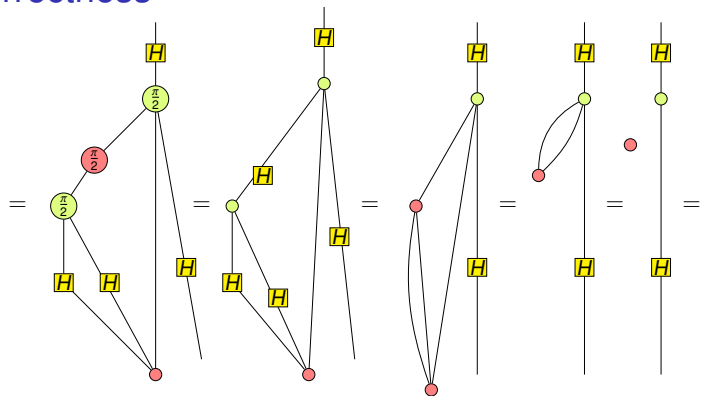
# Correctness



# Correctness



# Correctness



## Concealing property

To obtain some knowledge of the sender's commitment before the opening phase, the receiver may cheat by preparing a non-uniform sequence. For simplicity, let the length of each sequence to be 4. Assume the receiver prepares  $m$  sequence, of which one is a constant sequence  $|0000\rangle$  and the remaining are uniform sequences.

Suppose  $|0000\rangle$  is picked by the sender. The receiver measures 2 qubits in the  $\{|0\rangle, |1\rangle\}$  basis and 2 qubits in the  $\{|i\rangle, |\bar{i}\rangle\}$  basis once he/she receives the sequence from the sender. Then, the receiver will know what the sender has committed via the following procedure:

## Concealing property

1. If measuring the  $\{|0\rangle, |1\rangle\}$  basis returns two  $|0\rangle$  and measuring in the  $\{|i\rangle, |\bar{i}\rangle\}$  basis returns one  $|i\rangle$  and the other one  $|\bar{i}\rangle$ , then the bits committed by the sender is 00.
2. If measuring the  $\{|0\rangle, |1\rangle\}$  basis returns two  $|1\rangle$  and measuring in the  $\{|i\rangle, |\bar{i}\rangle\}$  basis returns one  $|i\rangle$  and the other one  $|\bar{i}\rangle$ , then the bits committed by the sender is 10.
3. If measuring in the  $\{|i\rangle, |\bar{i}\rangle\}$  basis returns two  $|i\rangle$  and measuring in the  $\{|0\rangle, |1\rangle\}$  basis returns one  $|0\rangle$  and one  $|1\rangle$ , then the bits committed by the sender is 01.
4. If measuring in the  $\{|i\rangle, |\bar{i}\rangle\}$  basis returns two  $|\bar{i}\rangle$  and measuring in the  $\{|0\rangle, |1\rangle\}$  basis returns one  $|0\rangle$  and one  $|1\rangle$ , then the bits committed by the sender is 11.
5. If measuring the  $\{|0\rangle, |1\rangle\}$  basis returns two  $|0\rangle$  or two  $|1\rangle$ , and measuring in the  $\{|i\rangle, |\bar{i}\rangle\}$  basis returns two  $|i\rangle$  or two  $|\bar{i}\rangle$ , then the receiver cannot reliably determine what bits the sender has committed.

## Concealing property

To sum up, the probability that the receiver cheats successfully is  $p_b < \frac{1}{m}$ . Note that  $p_b$  approximates to  $\frac{1}{m}$  when the length of the sequence is large. Indeed, suppose the  $m$  sequences the receiver prepared are of length  $n$ . One of them is a constant sequence  $|0 \dots 0\rangle$  and others are uniform sequences.

Suppose  $|0 \dots 0\rangle$  is picked by the sender. The receiver measures  $\frac{n}{2}$  qubits in the  $\{|0\rangle, |1\rangle\}$  basis and  $\frac{n}{2}$  qubits in the  $\{|i\rangle, |\bar{i}\rangle\}$  basis. Then, the receiver will know what the sender has committed via the following procedure:

## Concealing property

1. If measuring the  $\{|0\rangle, |1\rangle\}$  basis returns only  $|0\rangle$  or only  $|1\rangle$  and measuring in the  $\{|i\rangle, |\bar{i}\rangle\}$  basis returns some  $|i\rangle$  and some  $|\bar{i}\rangle$ , then the bits committed by the sender is either 00 or 10, depending on whether he/she gets is  $|0\rangle$ .
2. If measuring in the  $\{|i\rangle, |\bar{i}\rangle\}$  basis returns only  $|i\rangle$  or only  $|\bar{i}\rangle$  and measuring in the  $\{|0\rangle, |1\rangle\}$  basis returns some  $|0\rangle$  and some  $|1\rangle$ , then the bits committed by the sender is either 10 or 11, depending on whether he/she gets is  $|i\rangle$ .
3. If measuring the  $\{|0\rangle, |1\rangle\}$  basis returns only  $|0\rangle$  or only  $|1\rangle$ , and measuring in the  $\{|i\rangle, |\bar{i}\rangle\}$  basis returns only  $|i\rangle$  or only  $|\bar{i}\rangle$ , then it cannot reliably determined what bits the sender has committed.

Therefore,  $p_b = \frac{1}{m} \times (1 - (\frac{1}{2})^{\frac{n}{2}}) = \frac{1}{m} \times (1 - (\frac{1}{4})^n)$ . In other words,  $p_b$  approximates to  $\frac{1}{m}$  when  $n$  is large.

## Binding property

The binding property of our protocol is similar to the protocol of Nagy. If the sender wishes to postpone the commitment until the opening phase, then the sender has to know exactly the state of each qubit in the sequence received from the receiver. Only in that way can the sender pick a convenient index in the sequence corresponding to a qubit that matches the late commitment, when the receiver asks for the index.



## Binding property

Nevertheless, there is no reliable method to distinguish non-orthogonal quantum states. Without this knowledge, the sender can only cheat by randomly select a qubit from  $\{|0\rangle, |1\rangle, |i\rangle, |\bar{i}\rangle\}$ . Hence, there is always a probability of  $\frac{1}{4} \times 1 + \frac{1}{4} \times \frac{1}{2} + \frac{1}{4} \times \frac{1}{2} + \frac{1}{4} \times 0 = \frac{1}{2}$  for the sender to be detected as a cheater for each qubit verified by the receiver. Therefore, if the length of sequence is  $n$ , the probability of the sender cheating successfully is  $p_a = \left(\frac{1}{2}\right)^n$ . Here, our  $p_a$  is smaller than the  $p_a$  in the protocol of Nagy, which is  $\left(\frac{3}{4}\right)^n$ . Therefore, the security of our protocol is better than Nagy's.

Note that entanglement is of no use to the sender, since no entangled state will consistently collapse (when measured) to the outcome expected by the receiver.

# Conclusion




Our QBC protocol is correct, concealing and binding.

Protocol	resource	$p_a$	$p_b$	bits committed
CSQBC [3, 1, 2, 2]	–	–	$\geq 0.5$	1
Li et. al. [3]	$C(m, n)$	$(\frac{6+\sqrt{2}}{8})^{\frac{n}{2}}$	$\geq 0.5$	1
Nagy [3, 1]	$m \times n$	$(\frac{3}{4})^n$	$\frac{1}{m}$	1
Ours	$m \times n$	$(\frac{1}{2})^n$	$\frac{1}{m}$	2

Table: Comparison of security and efficiency

Thank you!

# References

-  Harry Buhrman, Matthias Christandl, Patrick Hayden, Hoi-Kwong Lo, and Stephanie Wehner.  
Possibility, impossibility, and cheat sensitivity of quantum-bit string commitment.  
*Physical Review A*, 78(022316):1–10, 2008.
-  Lucien Hardy and Adrian Kent.  
Cheat sensitive quantum bit commitment.  
*Physical Review Letters*, 92(15):1–4, 2004.
-  Yan-Bing Li, Qiaoyan Wen, Zi-Chen Li, Su-Juan Qin, and Ya-Tao Yang.  
Cheat sensitive quantum bit commitment via pre- and post-selected quantum states.  
*Quantum Information Processing*, 13(1):141–149, 2014.



Naya Nagy and Marius Nagy.

Unconditionally secure quantum bit commitment protocol based on incomplete information.

In Adrian-Horia Dediu, Manuel Lozano, and Carlos Martín-Vide, editors, *Theory and Practice of Natural Computing - Third International Conference*, pages 134–143. Springer, 2014.






Naya Nagy and Marius Nagy.




Quantum bit commitment - within an equivalence class.




*International Journal of Unconventional Computing*, 12(5-6):413–432, 2016.






ADLAM, EMILY, and ADRIAN KENT, 'Device-independent relativistic quantum bit commitment', *Physical Review A*, 92 (2015), 022315, 1–9.




-  BENNETTA, CHARLES, and GILLES BRASSARD, 'Quantum cryptography: Public key distribution and coin tossing', in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, 1984, pp. 175–179.
-  BRASSARD, GILLES, and CLAUDE CRÉPEAU, 'Quantum bit commitment and coin tossing protocols', in Alfred Menezes, and Scott A. Vanstone, (eds.), *Advances in Cryptology - CRYPTO '90, 10th Annual International Cryptology Conference*, Springer, 1990, pp. 49–61.
-  BRASSARD, GILLES, CLAUDE CRÉPEAU, RICHARD JOZSA, and DENIS LANGLOIS, 'A quantum bit commitment scheme provably unbreakable by both parties', in *34th Annual Symposium on Foundations of Computer Science, Palo Alto, California, USA, 3-5 November 1993*, IEEE Computer Society, 1993, pp. 362–371.





-  BUHRMAN, HARRY, MATTHIAS CHRISTANDL, PATRICK HAYDEN, HOI-KWONG LO, and STEPHANIE WEHNER, 'Possibility, impossibility, and cheat sensitivity of quantum-bit string commitment', *Physical Review A*, 78 (2008), 022316, 1–10.
-  CAMENISCH, JAN, and ANNA LYSYANSKAYA, 'A signature scheme with efficient protocols', in Stelvio Cimato, Clemente Galdi, and Giuseppe Persiano, (eds.), *Security in Communication Networks, Third International Conference, SCN 2002, Amalfi, Italy, September 11-13, 2002. Revised Papers*, vol. 2576 of *Lecture Notes in Computer Science*, Springer, 2002, pp. 268–289.
-  HARDY, LUCIEN, and ADRIAN KENT, 'Cheat sensitive quantum bit commitment', *Physical Review Letters*, 92 (2004), 15, 1–4.

-  HE, GUANGPING, ‘Security bound of cheat sensitive quantum bit commitment’, *Scientific Reports*, 9398 (2015), 5, 1–6.
-  KENT, ADRIAN, ‘Unconditionally secure bit commitment with flying qudits’, *New Journal of Physics*, 13 (2011), 113015, 1–16.
-  LI, JIANGTAO, and NINGHUI LI, ‘Policy-hiding access control in open environment’, in Marcos Kawazoe Aguilera, and James Aspnes, (eds.), *Proceedings of the Twenty-Fourth Annual ACM Symposium on Principles of Distributed Computing, PODC 2005, Las Vegas, NV, USA, July 17-20, 2005*, ACM, 2005, pp. 29–38.



-  LI, QIN, W. H. CHAN, and DONG-YANG LONG, 'Arbitrated quantum signature scheme using bell states', *Physical Review A*, 79 (2009), 054307.
-  LI, YAN-BING, QIAOYAN WEN, ZI-CHEN LI, SU-JUAN QIN, and YA-TAO YANG, 'Cheat sensitive quantum bit commitment via pre- and post-selected quantum states', *Quantum Information Processing*, 13 (2014), 1, 141–149.
-  LI, YAN-BING, SHENG-WEI XU, WEI HUANG, and ZONG-JIE WAN, 'Quantum bit commitment with cheat sensitive binding and approximate sealing', *Journal of Physics A: Mathematical and Theoretical*, 48 (2015), 135302, 1–10.

-  Lo, Hoi-Kwong, and H. F. Chau, 'Is quantum bit commitment really possible?', *Physical Review Letters*, 78 (1997), 17, 3410–3413.
-  MAYERS, DOMINIC, 'Unconditionally secure quantum bit commitment is impossible', *Physical Review Letters*, 78 (1997), 17, 3414–3417.
-  NAGY, NAYA, and MARIUS NAGY, 'Unconditionally secure quantum bit commitment protocol based on incomplete information', in Adrian-Horia Dediu, Manuel Lozano, and Carlos Martín-Vide, (eds.), *Theory and Practice of Natural Computing - Third International Conference*, Springer, 2014, pp. 134–143.

-  NAGY, NAYA, and MARIUS NAGY, 'Quantum bit commitment - within an equivalence class', *International Journal of Unconventional Computing*, 12 (2016), 5-6, 413–432.
-  SHIMIZU, KAORU, HIROYUKI FUKASAKA, KIYOSHI TAMAKI, and NOBUYUKI IMOTO, 'Cheat-sensitive commitment of a classical bit coded in a block of  $m \times n$  round-trip qubits', *Physical Review A*, 84 (2011), 022308, 1–14.
-  ZENG, GUIHUA, and CHRISTOPH KEITEL, 'Arbitrated quantum-signature scheme', *Physical Review A*, 65 (2002), 042312.
-  ZHANG, FANGGUO, XIAOFENG CHEN, YI MU, and WILLY SUSILO, 'A new and efficient signature on commitment values', *I. J. Network Security*, 7 (2008), 1, 100–105.