Topics 11-13: Quantum cryptography in the presence of noise and adversaries

1. Quantum money
2. Quantum bit commitment (M 6.3)
3. Quantum key distribution (NC 12.6, M 6.2)
   - Encryption
   - Classical one-time pad
   - Key distribution problem
   - QKD through a noiseless insecure channel (BB84, E92, and their relation)
   - QKD through noisy insecure channels

Encryption:

Reasons for communication with privacy:
- national secret, wartime commands
- internet finance
- human right not to be watched

PS different from transparency and accountability citizens expect from their governments ...

Encryption:

Reasons for communication with privacy:
- national secret, wartime commands
- internet finance
- human right not to be watched

PS different from transparency and accountability citizens expect from their governments ...

Our wish to maintain privacy, and the wish to hack those schemes, have given rise some of the best mathematics (e.g., Turing, Tutte ...)

Encryption:

Reasons for communication with privacy:
- national secret, wartime commands
- internet finance
- human right not to be watched

PS different from transparency and accountability citizens expect from their governments ...

Our wish to maintain privacy, and the wish to hack those schemes, have given rise some of the best mathematics (e.g., Turing, Tutte ...)

Many public key cryptosystems (RSA, Diffe-Hellman, elliptic curves) are NOT quantum safe.

Encryption:

Reasons for communication with privacy:
- national secret, wartime commands
- internet finance
- human right not to be watched

PS different from transparency and accountability citizens expect from their governments ...

Our wish to maintain privacy, and the wish to hack those schemes, have given rise some of the best mathematics (e.g., Turing, Tutte ...)

Many public key cryptosystems (RSA, Diffe-Hellman, elliptic curves) are NOT quantum safe.

The new proposals that may be quantum safe still relies on computational assumptions (e.g. $P \neq PSPACE$).

Are there encryption schemes that do not rely on computational assumptions?

These schemes are said to have "information theoretic security", something that can be proved.

Are there encryption schemes that do not rely on computational assumptions?

These schemes are said to have "information theoretic security", something that can be proved.

The public key cryptosystem like RSA allows a sender and a receiver who have never met to communicate with some privacy.

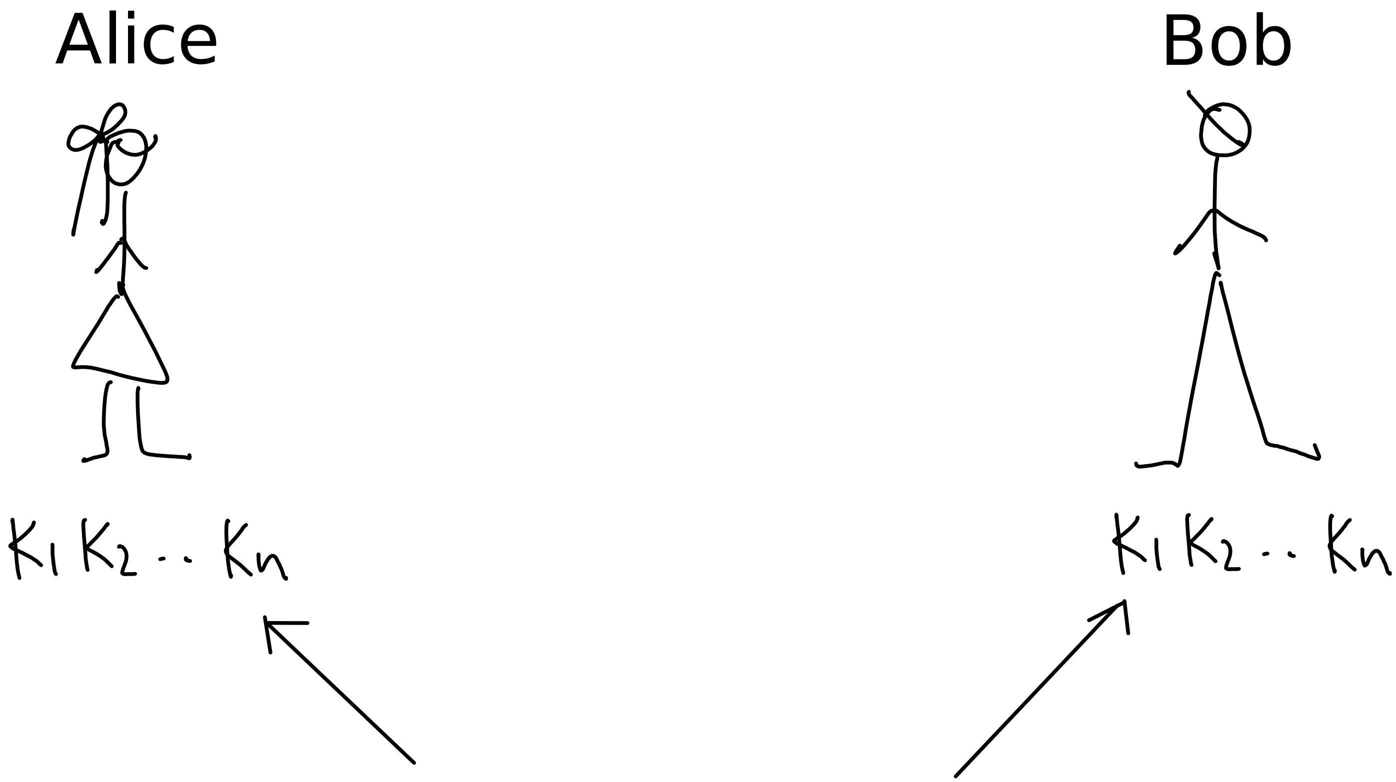
Are there encryption schemes that do not rely on computational assumptions?

These schemes are said to have "information theoretic security", something that can be proved.

The public key cryptosystem like RSA allows a sender and a receiver who have never met to communicate with some privacy.

It turns out, if the sender and the receiver have prior contact and share a secret key, they can instead use private key cryptosystem, some has information theoretic security.

The one-time pad:

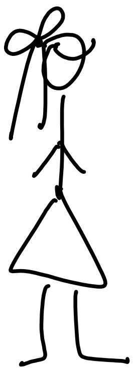


0. n-bit key shared
before the communication

The one-time pad:

1. Alice wants to communicate n bits to Bob $m_1 m_2 \dots m_n$

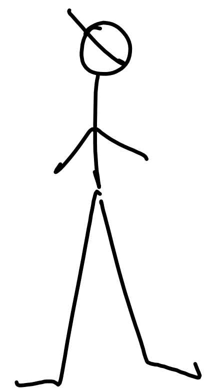
Alice



2. she sends to Bob the ciphertext:

$k_1 \oplus m_1, k_2 \oplus m_2, \dots, k_n \oplus m_n$

Bob



$k_1 k_2 \dots k_n$

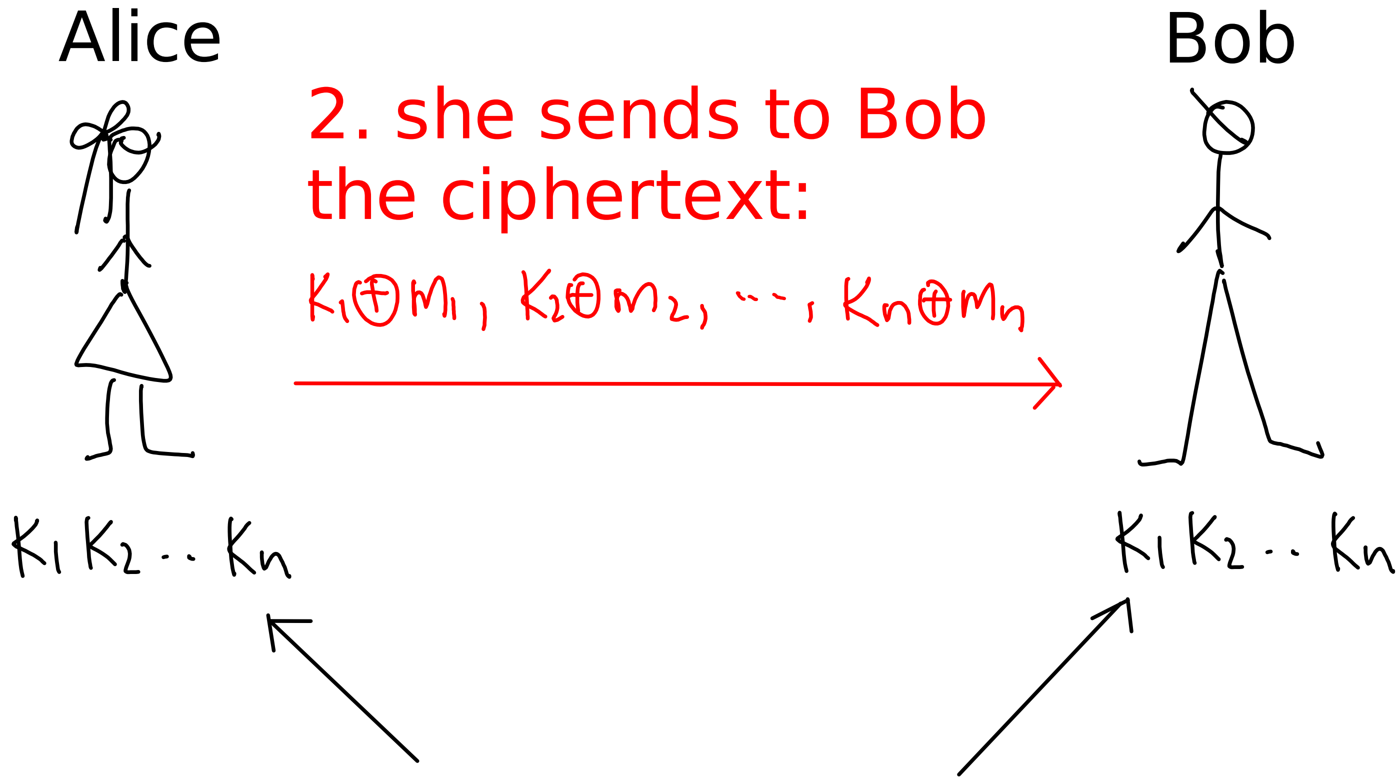
$k_1 k_2 \dots k_n$

0. n-bit key shared before the communication

The one-time pad:

1. Alice wants to communicate n bits to Bob $m_1 m_2 \cdots m_n$

3. Bob decrypts the ciphertext with his key to get the message



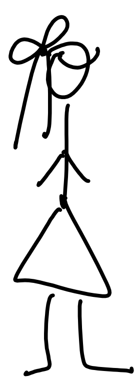
0. n-bit key shared before the communication

The one-time pad:

1. Alice wants to communicate n bits to Bob $m_1 m_2 \ldots m_n$

3. Bob decrypts the ciphertext with his key to get the message

Alice

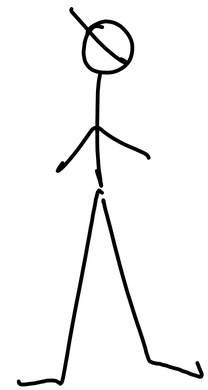


$K_1 K_2 \ldots K_n$

2. she sends to Bob the ciphertext:

$K_1 \oplus m_1, K_2 \oplus m_2, \ldots, K_n \oplus m_n$

Bob



$K_1 K_2 \ldots K_n$

Any eavesdropper Eve, without info on the key, and only seeing the ciphertext, will have no information on the message (Shannon 49)!

The one-time pad is named as such because the key that "pads" the message should not be reused!

The one-time pad is named as such because the key that "pads" the message should not be reused!

e.g., if Alice encrypts a second message x1 x2 ... xn with the same key, Eve can in principle record both of:

$$K_1 \oplus m_1 , \; K_2 \oplus m_2 , \; \ldots , \; K_n \oplus m_n$$

$$K_1 \oplus x_1 , \; K_2 \oplus x_2 , \; \ldots , \; K_n \oplus x_n$$

The one-time pad is named as such because the key that "pads" the message should not be reused!

e.g., if Alice encrypts a second message x1 x2 ... xn with the same key, Eve can in principle record both of:

$$k_1 \oplus m_1, \; k_2 \oplus m_2, \; \ldots, \; k_n \oplus m_n$$

$$k_1 \oplus x_1, \; k_2 \oplus x_2, \; \ldots, \; k_n \oplus x_n$$

If Eve takes the xor bitwise of the two ciphertexts, the unknown ki cancel out in the xor and she gets

$$x_1 \oplus m_1, \; x_2 \oplus m_2, \; \ldots, \; x_n \oplus m_n$$

which are n bits of information on the two messages.

The one-time pad is named as such because the key that "pads" the message should not be reused!

e.g., if Alice encrypts a second message x1 x2 ... xn with the same key, Eve can in principle record both of:

$$k_1 \oplus m_1 ,\ k_2 \oplus m_2 ,\ \ldots ,\ k_n \oplus m_n$$

$$k_1 \oplus x_1 ,\ k_2 \oplus x_2 ,\ \ldots ,\ k_n \oplus x_n$$

If Eve takes the xor bitwise of the two ciphertexts, the unknown ki cancel out in the xor and she gets

$$x_1 \oplus m_1 ,\ x_2 \oplus m_2 ,\ \ldots ,\ x_n \oplus m_n$$

which are n bits of information on the two messages.

Problem: how do Alice and Bob share this key?

Quantum key distribution:

Assumptions:

1. A quantum channel from Alice to Bob, insecure in that Eve can do to the transmission anything allowed by quantum mechanics

Quantum key distribution:

Assumptions:

1. A quantum channel from Alice to Bob, insecure in that Eve can do to the transmission anything allowed by quantum mechanics

2. An authenticated classical channel, where Eve can read the messages but cannot alter them. This also allows Alice & Bob to identify each other.

Quantum key distribution:

Assumptions:

1. A quantum channel from Alice to Bob, insecure in that Eve can do to the transmission anything allowed by quantum mechanics

2. An authenticated classical channel, where Eve can read the messages but cannot alter them. This also allows Alice & Bob to identify each other.

The second requirement is often met with a classical message authentication scheme that in turns requires a key. Goal: use a small authentication key and QKD to obtain a larger key -- QKD achieves key EXPANSION.

QKD schemes that are secure given an insecure noiseless channel --

In other words, without an eavesdropping the channel should be noiseless.

BB84' (Bennett and Brassard) (cf A4)

1. Alice picks 2n random bits: $c_1 c_2 \cdots c_n,\ b_1 b_2 \cdots b_n$

2. Alice sends n qubits (A1 A2 ... An) to Bob:

$$H^{b_1}|c_1\rangle \otimes H^{b_2}|c_2\rangle \otimes \cdots \otimes H^{b_n}|c_n\rangle$$

as in Q$

BB84' (Bennett and Brassard) (cf A4)

1. Alice picks 2n random bits: $c_1 c_2 \cdots c_n$, $b_1 b_2 \ldots b_n$

2. Alice sends n qubits (A1 A2 ... An) to Bob:

$$H^{b_1}|c_1\rangle \otimes H^{b_2}|c_2\rangle \otimes \cdots \otimes H^{b_n}|c_n\rangle$$

3. Eve applies an arbitrary quantum operation on A1 A2 ... An, and forwards the output B1 B2 ... Bn to Bob. The identity operation corresponds to a secure transmission.

BB84' (Bennett and Brassard) (cf A4)

1. Alice picks 2n random bits: $c_1 c_2 \cdots c_n,\ b_1 b_2 \ldots b_n$
2. Alice sends n qubits (A1 A2 ... An) to Bob:

$$H^{b_1}|c_1\rangle \otimes H^{b_2}|c_2\rangle \otimes \cdots \otimes H^{b_n}|c_n\rangle$$

3. Eve applies an arbitrary quantum operation on A1 A2 ... An, and forwards the output B1 B2 ... Bn to Bob. The identity operation corresponds to a secure transmission.

4. Bob acknowledges to Alice he has received B1 ... Bn.

VERY CRUCIAL STEP !!
(WITHOUT THIS THE PROTOCOL IS INSECURE)

BB84' (Bennett and Brassard) (cf A4)

1. Alice picks 2n random bits: $c_1 c_2 \cdots c_n, \; b_1 b_2 \cdots b_n$

2. Alice sends n qubits (A1 A2 ... An) to Bob:

$$H^{b_1}|c_1\rangle \otimes H^{b_2}|c_2\rangle \otimes \cdots \otimes H^{b_n}|c_n\rangle$$

3. Eve applies an arbitrary quantum operation on A1 A2 ... An, and forwards the output B1 B2 ... Bn to Bob. The identity operation corresponds to a secure transmission.

4. Bob acknowledges to Alice he has received B1 ... Bn.

5. Alice picks another n random bits r1 r2 ... rn.

BB84' (Bennett and Brassard) (cf A4)

1. Alice picks 2n random bits: $c_1 c_2 \cdots c_n, \; b_1 b_2 \ldots b_n$

2. Alice sends n qubits (A1 A2 ... An) to Bob:

$$H^{b_1}|c_1\rangle \otimes H^{b_2}|c_2\rangle \otimes \cdots \otimes H^{b_n}|c_n\rangle$$

3. Eve applies an arbitrary quantum operation on A1 A2 ... An, and forwards the output B1 B2 ... Bn to Bob. The identity operation corresponds to a secure transmission.

4. Bob acknowledges to Alice he has received B1 ... Bn.

5. Alice picks another n random bits r1 r2 ... rn.

6. She tells Bob the values of b1 b2 ... bn, r1 r2 ... rn, and the ci's for which ri = 1.

BB84' (Bennett and Brassard) (cf A4)

1. Alice picks 2n random bits: $c_1 c_2 \cdots c_n, \; b_1 b_2 \ldots b_n$

2. Alice sends n qubits (A1 A2 ... An) to Bob:

$$H^{b_1}|c_1\rangle \otimes H^{b_2}|c_2\rangle \otimes \cdots \otimes H^{b_n}|c_n\rangle$$

3. Eve applies an arbitrary quantum operation on A1 A2 ... An, and forwards the output B1 B2 ... Bn to Bob. The identity operation corresponds to a secure transmission.

4. Bob acknowledges to Alice he has received B1 ... Bn.

5. Alice picks another n random bits r1 r2 ... rn.

6. She tells Bob the values of b1 b2 ... bn, r1 r2 ... rn, and the ci's for which ri = 1.

$\approx$

Alice tells Bob all basis info & discloses a random half of the ci's.

7. Bob measures Bi in the {|0>,|1>} basis if bi = 0, in the {|+>,|->} basis if bi = 1. Let the outcomes be d1 d2 ... dn.

For each i, if ri = 1, he checks whether ci = di.

7. Bob measures Bi in the {|0>,|1>} basis if bi = 0, in the {|+>,|->} basis if bi = 1. Let the outcomes be d1 d2 ... dn.

For each i, if ri = 1, he checks whether ci = di.

If they are not always the same, he concludes that someone is eavesdropping. He tells Alice they should abort the protocol.

7. Bob measures Bi in the {|0>,|1>} basis if bi = 0, in the {|+>,|->} basis if bi = 1. Let the outcomes be d1 d2 ... dn.

For each i, if ri = 1, he checks whether ci = di.

If they are not always the same, he concludes that someone is eavesdropping. He tells Alice they should abort the protocol.

If they are always the same, he concludes that the channel is secure. He tells Alice the protocol is successful. Alice take the ci's for which ri = 0 as the key; Bob takes the di's.

Example: n=10

1. Alice picks c1 c2 ... cn = 1011001010

b1 b2 ... bn = 1001100010

Example: n=10

1. Alice picks c1 c2 ... cn = 1011001010

b1 b2 ... bn = 1001100010

2. Alice sends to Bob $|-\rangle\ |0\rangle\ |1\rangle\ |-\rangle\ |+\rangle\ |0\rangle\ |1\rangle\ |0\rangle\ |-\rangle\ |0\rangle$

Example: n=10

1. Alice picks c1 c2 ... cn = 1011001010

   b1 b2 ... bn = 1001100010

2. Alice sends to Bob $|-\rangle\,|0\rangle\,|1\rangle\,|-\rangle\,|+\rangle\,|0\rangle\,|1\rangle\,|0\rangle\,|-\rangle\,|0\rangle$

3. Without eavesdropping, Bob receives

$$|-\rangle\,|0\rangle\,|1\rangle\,|-\rangle\,|+\rangle\,|0\rangle\,|1\rangle\,|0\rangle\,|-\rangle\,|0\rangle$$

Example: n=10

1. Alice picks c1 c2 ... cn = 1011001010

   b1 b2 ... bn = 1001100010

2. Alice sends to Bob $|-\rangle |0\rangle |1\rangle |-\rangle |+\rangle |0\rangle |1\rangle |0\rangle |-\rangle |0\rangle$

3. Without eavesdropping, Bob receives

$$|-\rangle |0\rangle |1\rangle |-\rangle |+\rangle |0\rangle |1\rangle |0\rangle |-\rangle |0\rangle$$

4. He tells Alice he receives the state.

Example: n=10

1. Alice picks c1 c2 ... cn = 1011001010

b1 b2 ... bn = 1001100010

2. Alice sends to Bob $|-\rangle\,|0\rangle\,|1\rangle\,|-\rangle\,|+\rangle\,|0\rangle\,|1\rangle\,|0\rangle\,|-\rangle\,|0\rangle$

3. Without eavesdropping, Bob receives

$$|-\rangle\,|0\rangle\,|1\rangle\,|-\rangle\,|+\rangle\,|0\rangle\,|1\rangle\,|0\rangle\,|-\rangle\,|0\rangle$$

4. He tells Alice he receives the state.

5-6. Alice picks r1 r2 ... r10 = 0010110010

3 5 6 9

Example: n=10

1. Alice picks c1 c2 ... cn = 1011001010

   b1 b2 ... bn = 1001100010

2. Alice sends to Bob $|-\rangle|0\rangle|1\rangle|-\rangle|+\rangle|0\rangle|1\rangle|0\rangle|-\rangle|0\rangle$

3. Without eavesdropping, Bob receives

$$|-\rangle|0\rangle|1\rangle|-\rangle|+\rangle|0\rangle|1\rangle|0\rangle|-\rangle|0\rangle$$

4. He tells Alice he receives the state.

5-6. Alice picks r1 r2 ... r10 = 0010110010

3 5 6 9

She sends b1 b2 ... b10 = 1001100010

r1 r2 ... r10 = 0010110010

c3 = 1, c5 = 0, c6 = 0, c9 = 1 to Bob.

7. Bob uses b1 b2 ... b10 = 1001100010 to meas

$|-\rangle\ |0\rangle\ |1\rangle\ |-\rangle\ |+\rangle\ |0\rangle\ |1\rangle\ |0\rangle\ |-\rangle\ |0\rangle$

He gets $-\quad 0\quad 1\quad -\quad +\quad 0\quad 1\quad 0\quad -\quad 0$

7. Bob uses b1 b2 ... b10 = 1001100010 to meas

$$|-\rangle\, |0\rangle\, |1\rangle\, |-\rangle\, |+\rangle\, |0\rangle\, |1\rangle\, |0\rangle\, |-\rangle\, |0\rangle$$

He gets $-\ 0\ 1\ -\ +\ 0\ 1\ 0\ -\ 0$

Converting the +/- to 0/1, his outcomes are

d1 d2 ... d10 = 1011001010 (= c1 ... c10)

7. Bob uses b1 b2 ... b10 = 1001100010 to meas

$|-\rangle\, |0\rangle\, |1\rangle\, |-\rangle\, |+\rangle\, |0\rangle\, |1\rangle\, |0\rangle\, |-\rangle\, |0\rangle$

He gets $-\ 0\ 1\ -\ +\ 0\ 1\ 0\ -\ 0$

Converting the +/- to 0/1, his outcomes are

d1 d2 ... d10 = 1011001010 (= c1 ... c10)

Since r1 r2 ... r10 = 0010110010

he checks if c3 = d3, c5 = d5, c6 = d6, c9 = d9

and they all agree, so, he tells Alice QKD passes.

7. Bob uses b1 b2 ... b10 = 1001100010 to meas

$$|-\rangle |0\rangle |1\rangle |-\rangle |+\rangle |0\rangle |1\rangle |0\rangle |-\rangle |0\rangle$$

He gets $-\ 0\ 1\ -\ +\ 0\ 1\ 0\ -\ 0$

Converting the +/- to 0/1, his outcomes are

d1 d2 ... d10 = 1011001010 (= c1 ... c10)

Since r1 r2 ... r10 = 0010110010

he checks if c3 = d3, c5 = d5, c6 = d6, c9 = d9

and they all agree, so, he tells Alice QKD passes.

Alice outputs c1 c2 c4 c7 c8 c10 = 101100,
Bob outputs d1 d2 d4 d7 d8 d10 = 101100.

3. With eavesdropping, Bob no longer receives

$$|-\rangle\,|0\rangle\,|1\rangle\,|-\rangle\,|+\rangle\,|0\rangle\,|1\rangle\,|0\rangle\,|-\rangle\,|0\rangle$$

3. With eavesdropping, Bob no longer receives

$$|-\rangle|0\rangle|1\rangle|-\rangle|+\rangle|0\rangle|1\rangle|0\rangle|-\rangle|0\rangle$$

Recall A4, if Eve makes the optimal measurement on each qubit, the resulting state is independent of the basis.

$|+\rangle, |0\rangle \rightarrow +1$ eigenstate of H

$|-\rangle, |1\rangle \rightarrow -1$ "

3. With eavesdropping, Bob no longer receives

$$|-\rangle|0\rangle|1\rangle|-\rangle|+\rangle|0\rangle|1\rangle|0\rangle|-\rangle|0\rangle$$

Recall A4, if Eve makes the optimal measurement on each qubit, the resulting state is independent of the basis. $|+\rangle, |0\rangle \rightarrow +1$ eigenstate of H

$|-\rangle, |1\rangle \rightarrow -1$ " "

Most generally, Eve applies a quantum operation jointly on all n qubits. She keeps the environment output system of the Stinespring dilation (what she gains from eavesdropping) and gives the output (n qubits) to Bob. By discretization of errors (writing the Kraus operations as a linear combination of Pauli errors) we can focus on Pauli errors. QKD is a Pauli error detecting code.

For each qubit, if Pauli X/Z happens with prob 1/2:

(a) wp 1/4: state is |0> or |1> and the error is X

For each qubit, if Pauli X/Z happens with prob 1/2:

(a) wp 1/4: state is |0> or |1> and the error is X
(b) wp 1/4: state is |+> or |-> and the error is Z
(c) wp 1/2: the error does not change the state

For each qubit, if Pauli X/Z happens with prob 1/2:

(a) wp 1/4: state is |0> or |1> and the error is X
(b) wp 1/4: state is |+> or |-> and the error is Z
(c) wp 1/2: the error does not change the state

in each case,
wp 1/2, ri = 1; Alice & Bob will check if ci = di.

For each qubit, if Pauli X/Z happens with prob 1/2:

(a) wp 1/4: state is |0> or |1> and the error is X
(b) wp 1/4: state is |+> or |-> and the error is Z
(c) wp 1/2: the error does not change the state

in each case,
wp 1/2, ri = 1; Alice & Bob will check if ci = di.

wp 1/4 = prob([(a)or(b)] & ri=1) , ci ≠ di.

For each qubit, if Pauli X/Z happens with prob 1/2:

(a) wp 1/4: state is |0> or |1> and the error is X
(b) wp 1/4: state is |+> or |-> and the error is Z
(c) wp 1/2: the error does not change the state

in each case,
wp 1/2, ri = 1; Alice & Bob will check if ci = di.

wp 1/4 = prob([(a)or(b)] & ri=1) , ci ≠ di.

If instead, for each qubit, there's an X/Z wp pe,
& there are n qubits, Pr(undetected error) = $(3/4)^{n*pe}$

exponentially decreasing with n.

For each qubit, if Pauli X/Z happens with prob 1/2:

(a) wp 1/4: state is |0> or |1> and the error is X
(b) wp 1/4: state is |+> or |-> and the error is Z
(c) wp 1/2: the error does not change the state

in each case,
wp 1/2, ri = 1; Alice & Bob will check if ci = di.

wp 1/4 = prob([(a)or(b)] & ri=1) , ci ≠ di.

If instead, for each qubit, there's an X/Z wp pe,
& there are n qubits, Pr(undetected error) = $(3/4)^{n*pe}$

exponentially decreasing with n.

QKD is insecure only if Alice and Bob generate a compromised key. (OK if they abort the protocol ...)

Real BB84: Bob measures B1 ... Bn in step 4 AS THE QUBITS ARRIVE. He does not know b1 ... bn, so, he uses RANDOM computational or conjugate basis!

Real BB84: Bob measures B1 ... Bn in step 4 AS THE QUBITS ARRIVE. He does not know b1 ... bn, so, he uses RANDOM computational or conjugate basis!

The price:

* Qubits measured with incorrect bases give random outcomes and are "wasted." Everything else is same as before. They tolerate the loss (1/2) in key rate.

Real BB84: Bob measures B1 ... Bn in step 4 AS THE QUBITS ARRIVE. He does not know b1 ... bn, so, he uses RANDOM computational or conjugate basis!

The price:

* Qubits measured with incorrect bases give random outcomes and are "wasted." Everything else is same as before. They tolerate the loss (1/2) in key rate.

* Bob also needs to tell Alice which qubits are right; so, more back communication is needed.

Real BB84: Bob measures B1 ... Bn in step 4 AS THE QUBITS ARRIVE. He does not know b1 ... bn, so, he uses RANDOM computational or conjugate basis!

The price:

* Qubits measured with incorrect bases give random outcomes and are "wasted." Everything else is same as before. They tolerate the loss (1/2) in key rate.

* Bob also needs to tell Alice which qubits are right; so, more back communication is needed.

The benefit:

Bob does not need quantum storage (really hard for photons which is widely used). BB84 is called a "prepare-measure" scheme.

Additional improvements:

With better analysis, can use conjugation basis a small fraction f of the time (for both Alice and Bob) which eliminates the 1/2 loss in key rate.

Additional improvements:

With better analysis, can use conjugation basis a small fraction f of the time (for both Alice and Bob) which eliminates the 1/2 loss in key rate.

BB84 requires 2 bases to detect both X and Z errors.

If n is very large, and Alice prepares in and Bob measures in computational basis (1-f) fraction of the qubits, and Alice releases a fraction g of the ci's

Additional improvements:

With better analysis, can use conjugation basis a small fraction f of the time (for both Alice and Bob) which eliminates the 1/2 loss in key rate.

BB84 requires 2 bases to detect both X and Z errors.

If n is very large, and Alice prepares in and Bob measures in computational basis (1-f) fraction of the qubits, and Alice releases a fraction g of the ci's, on average they can detect:

$(1-f)^2 * g * n * pe/2$ X errors

$f^2 * g * n * pe/2$ Z errors

Additional improvements:

With better analysis, can use conjugation basis a small fraction f of the time (for both Alice and Bob) which eliminates the 1/2 loss in key rate.

BB84 requires 2 bases to detect both X and Z errors.

If n is very large, and Alice prepares in and Bob measures in computational basis (1-f) fraction of the qubits, and Alice releases a fraction g of the ci's, on average they can detect:

$(1-f)^2 * g * n * pe/2$ X errors

$f^2 * g * n * pe/2$ Z errors

f,g can be quite small (e.g., 1%) if n is very large (e.g., 10^9) while maintaining security.
(Small pe can be handled by methods to be described.)

Now comes the real, big, problem ...

What about noise in the channel?

1. This can cause Alice and Bob to output different keys
   If they try to use error correction (for classical data)
   information on the key "may leak" in the syndrome
   measurements

What about noise in the channel?

1. This can cause Alice and Bob to output different keys
   If they try to use error correction (for classical data) information on the key "may leak" in the syndrome measurements

2. Classical privacy amplification addresses inefficient detection of error.
   e.g., even if Eve has partial info on e1, e2, e3, she may have less info on e1+e2+e3 mod 2, or on f(e1, e2, e3) for some pseudorandom function f.

What about noise in the channel?

1. This can cause Alice and Bob to output different keys
   If they try to use error correction (for classical data) information on the key "may leak" in the syndrome measurements

2. Classical privacy amplification addresses inefficient detection of error.
   e.g., even if Eve has partial info on e1, e2, e3, she may have less info on e1+e2+e3 mod 2, or on f(e1, e2, e3) for some pseudorandom function f.

But a convincing security proof was elusive (84-96).
e.g., can Eve mask the error she induces as noise?
e.g., what if Eve does not find the key, but keep the quantum state from tampering with BB84 and use it for future attack when Alice and Bob use their key?

Mayers 96: first proof of security of BB84+ without restriction on the adversary and with noise
(NB his proof was very hard to understand ...)

Mayers 96: first proof of security of BB84+ without restriction on the adversary and with noise
(NB his proof was very hard to understand ...)

Lo & Chau 97: easy security proof of E91
(based on BDSW96 -- Bennett, DiVincenzo, Smolin, Wootters on entanglement purification and QECC)

Mayers 96: first proof of security of BB84+ without restriction on the adversary and with noise
(NB his proof was very hard to understand ...)

Lo & Chau 97: easy security proof of E91
(based on BDSW96 -- Bennett, DiVincenzo, Smolin, Wootters on entanglement purification and QECC)

Shor & Preskill 00: show Lo-Chau proof of security of E91 can be turned into the Mayers proof of BB84!

Mayers 96: first proof of security of BB84+ without restriction on the adversary and with noise
(NB his proof was very hard to understand ...)

Lo & Chau 97: easy security proof of E91
(based on BDSW96 -- Bennett, DiVincenzo, Smolin, Wootters on entanglement purification and QECC)

Shor & Preskill 00: show Lo-Chau proof of security of E91 can be turned into the Mayers proof of BB84!

E91 is hard to implement experimentally but easy to analyse, BB84 is opposite. Relating the two gives the best of the 2 worlds ...

Plan:

1. Ekert's QKD scheme E91
2. Lo-Chau security proof for E91
   General Eve, noiseless channel, then add noise.
3. Relate E91 and BB84 (noiseless case)
4. Relating security of E91 to BB84 (Shor-Preskill)
   (brief ideas)

E91 (Ekert 91) (version 1)

If Alice and Bob share: $|\Phi_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

both measuring in the computational basis gives equal and secret outcomes, i.e., 1 key bit.

E91 (Ekert 91) (version 1)

If Alice and Bob share: $|\Phi_{00}\rangle = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)$

both measuring in the computational basis gives equal and secret outcomes, i.e., 1 key bit.

Catch: how do they get many copies of $|\Phi_{00}\rangle$?

E91 (Ekert 91) (version 1)

If Alice and Bob share: $|\Phi_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

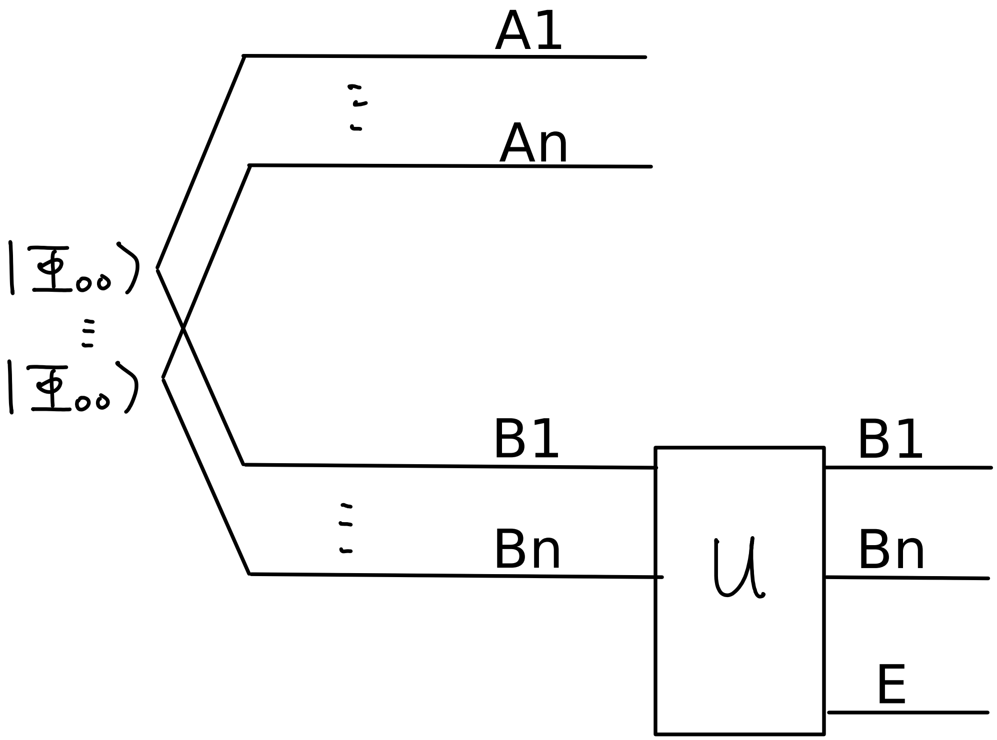
both measuring in the computational basis gives equal and secret outcomes, i.e., 1 key bit.

Catch: how do they get many copies of $|\Phi_{00}\rangle$?

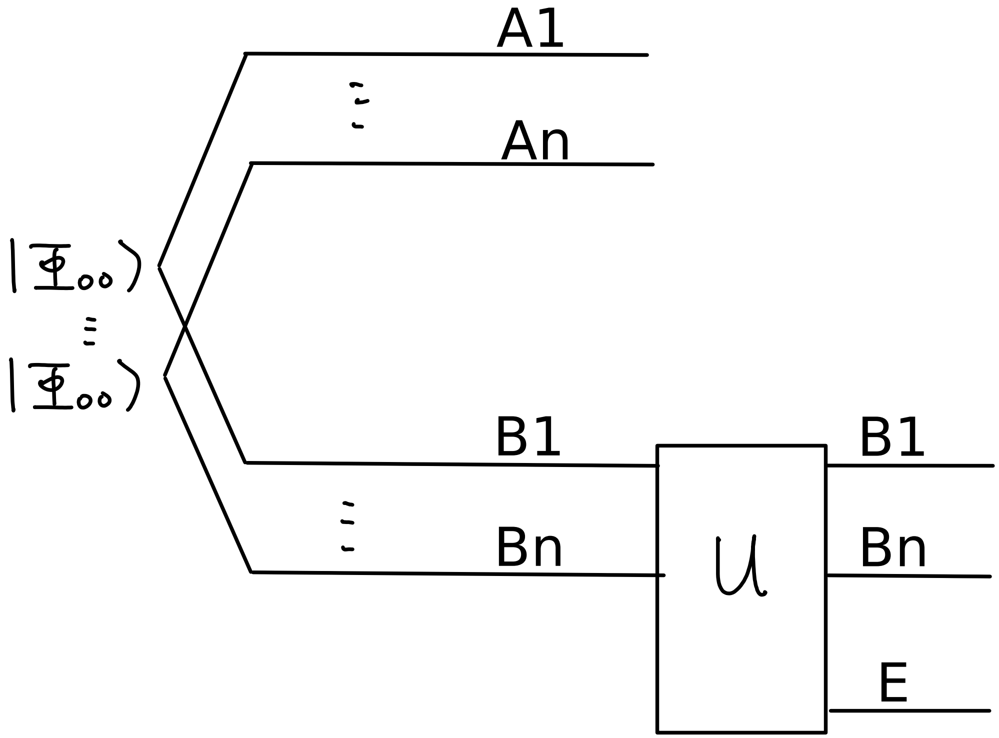
Solution: Alice prepare many copies of $|\Phi_{00}\rangle$.

Let the i-th copy live on systems Ai Bi. Alice sends B1 ... Bn to Bob via the insecure quantum channel .

Security of E91 via insecure noisy channel:



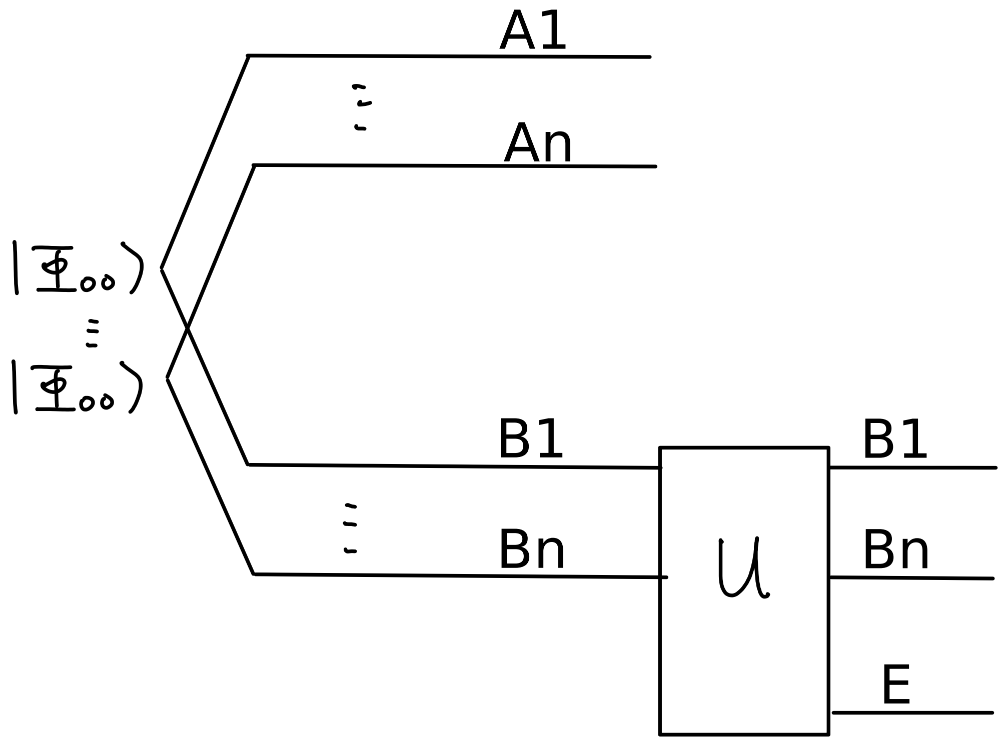
Security of E91 via insecure noisy channel:



Claim 1: the most general error reduces to Pauli errors !

(based on discretization of error for sharing $|\Phi_{00}\rangle$)

Security of E91 via insecure noisy channel:



Claim 1: the most general error reduces to Pauli errors !

(based on discretization of error for sharing $|\Phi_{00}\rangle$)

Claim 2: it is possible to identify & correct Pauli errors
if there are not too many of them ...

Detecting and identifying Pauli error on Bell states:

Label each of the 4 Bell states with 2 bits

$$|\Phi_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = I \otimes I\,|\Phi_{00}\rangle \quad \longleftrightarrow \quad 00$$

$$|\Phi_{10}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) = I \otimes X\,|\Phi_{00}\rangle \quad \longleftrightarrow \quad 10$$

$$|\Phi_{01}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) = I \otimes Z\,|\Phi_{00}\rangle \quad \longleftrightarrow \quad 01$$

$$|\Phi_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = I \otimes Y\,|\Phi_{00}\rangle \quad \longleftrightarrow \quad 11$$

↑ up to an overall phase

$$|\Phi_{ab}\rangle = I \otimes X^a Z^b\,|\Phi_{00}\rangle \quad \longleftrightarrow \quad ab$$

Detecting and identifying Pauli error on Bell states:

Label each of the 4 Bell states with 2 bits

$$|\Phi_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = I \otimes I\, |\Phi_{00}\rangle \longleftrightarrow 00$$

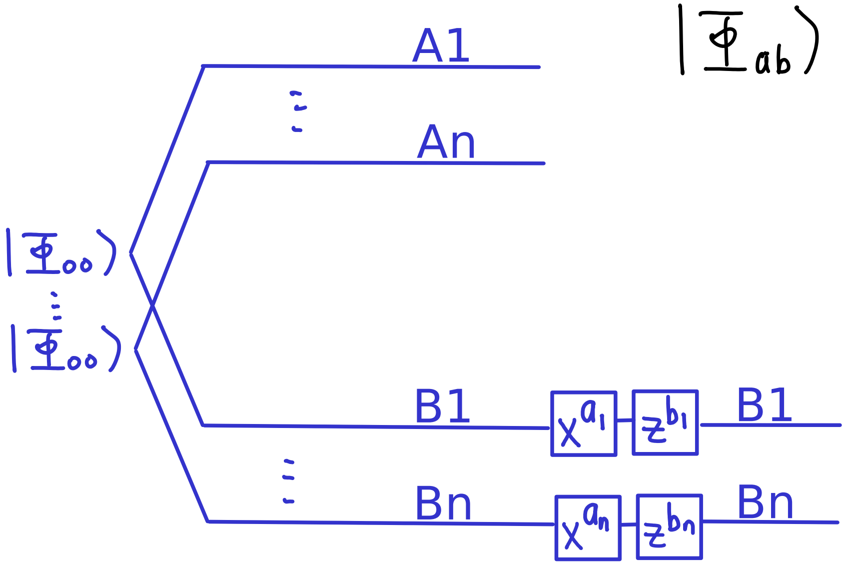
$$|\Phi_{10}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) = I \otimes X\, |\Phi_{00}\rangle \longleftrightarrow 10$$

$$|\Phi_{01}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) = I \otimes Z\, |\Phi_{00}\rangle \longleftrightarrow 01$$

$$|\Phi_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = I \otimes Y\, |\Phi_{00}\rangle \longleftrightarrow 11$$

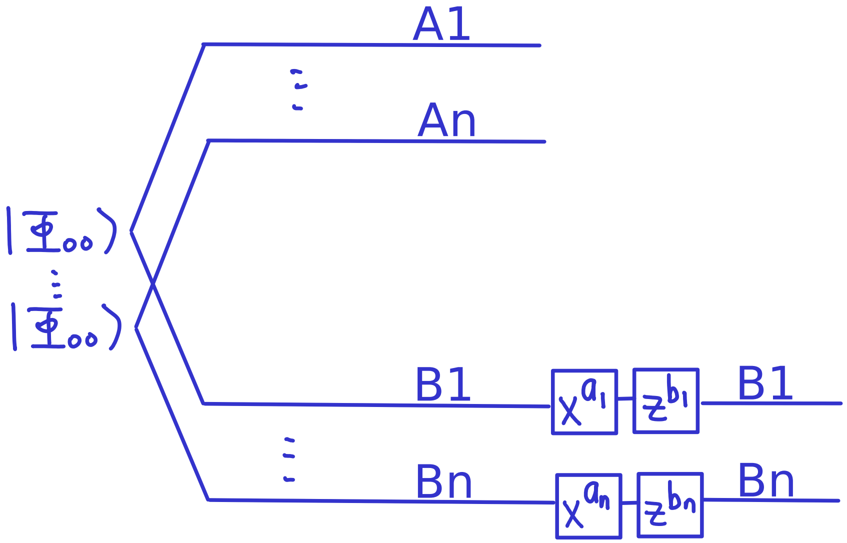
↑ up to an overall phase

$$|\Phi_{ab}\rangle = I \otimes X^a Z^b\, |\Phi_{00}\rangle \longleftrightarrow ab$$



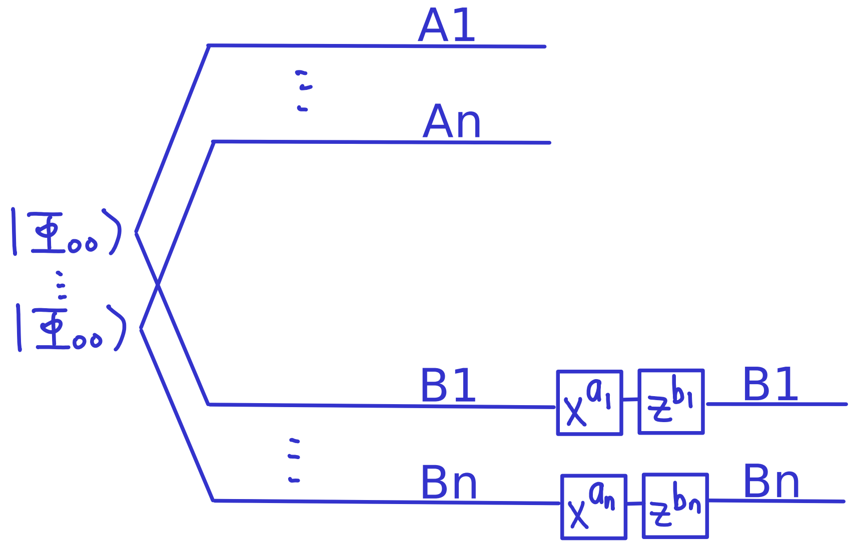
$$\longleftrightarrow \quad a_1 b_1 a_2 b_2 \dots a_n b_n$$

Theorem: suppose Alice and Bob share the following:



$$\longleftrightarrow \quad a_1 b_1 a_2 b_2 \ldots a_n b_n$$

Theorem: suppose Alice and Bob share the following:



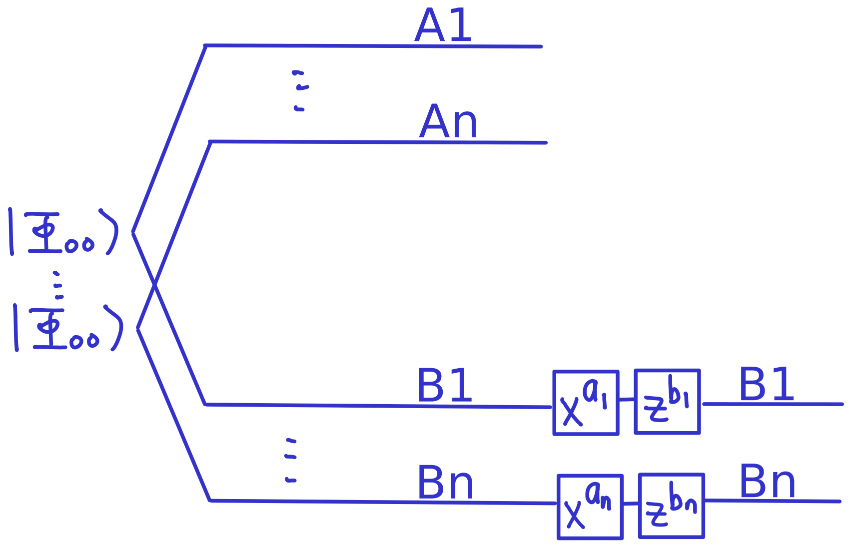
$\longleftrightarrow \quad a_1 b_1 a_2 b_2 \cdots a_n b_n$

There is a test that consumes k copies of $|\Phi_{00}\rangle$ uses classical communication (CC), without changing the above state, such that

$$\Pr\left(a_1 b_1 \cdots a_n b_n \neq 00 \cdots 00 \text{ and test passes}\right) \leq \frac{1}{2^k}$$

noiseless, perfect copies

Theorem: suppose Alice and Bob share the following:



$\longleftrightarrow \quad a_1 b_1 a_2 b_2 \cdots a_n b_n$

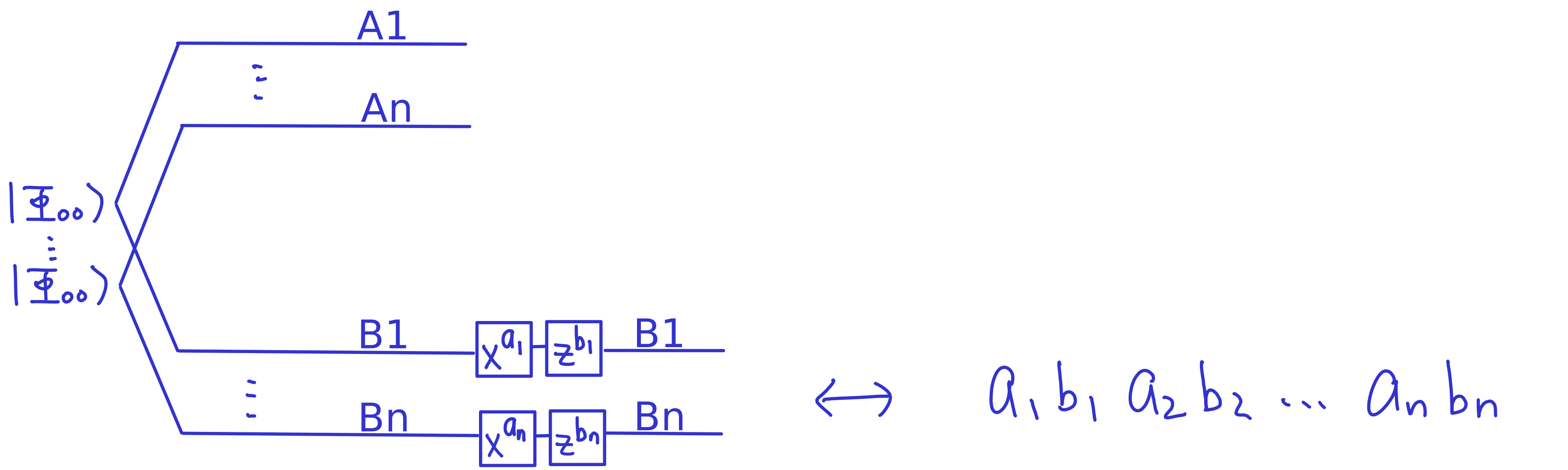
There is a test that consumes k copies of $|\Phi_{00}\rangle$ uses classical communication (CC), without changing the above state, such that

$$\Pr(a_1 b_1 \cdots a_n b_n \neq 00 \cdots 00 \text{ and test passes}) \leq \frac{1}{2^k}$$

noiseless, perfect copies

not a chicken-n-egg problem, if k < n and can be borrowed and return (more later)

Theorem: suppose Alice and Bob share the following:



There is a test that consumes k copies of $|\Phi_{00}\rangle$ uses classical communication (CC), without changing the above state, such that

$$\Pr(a_1 b_1 \cdots a_n b_n \neq 00 \cdots 00 \text{ and test passes}) \leq \frac{1}{2^k}$$

Lemma: with 1 copy of $|\Phi_{00}\rangle$ & CC, Alice and Bob can learn the parity of any subset in $a_1 b_1 a_2 b_2 \cdots a_n b_n$.

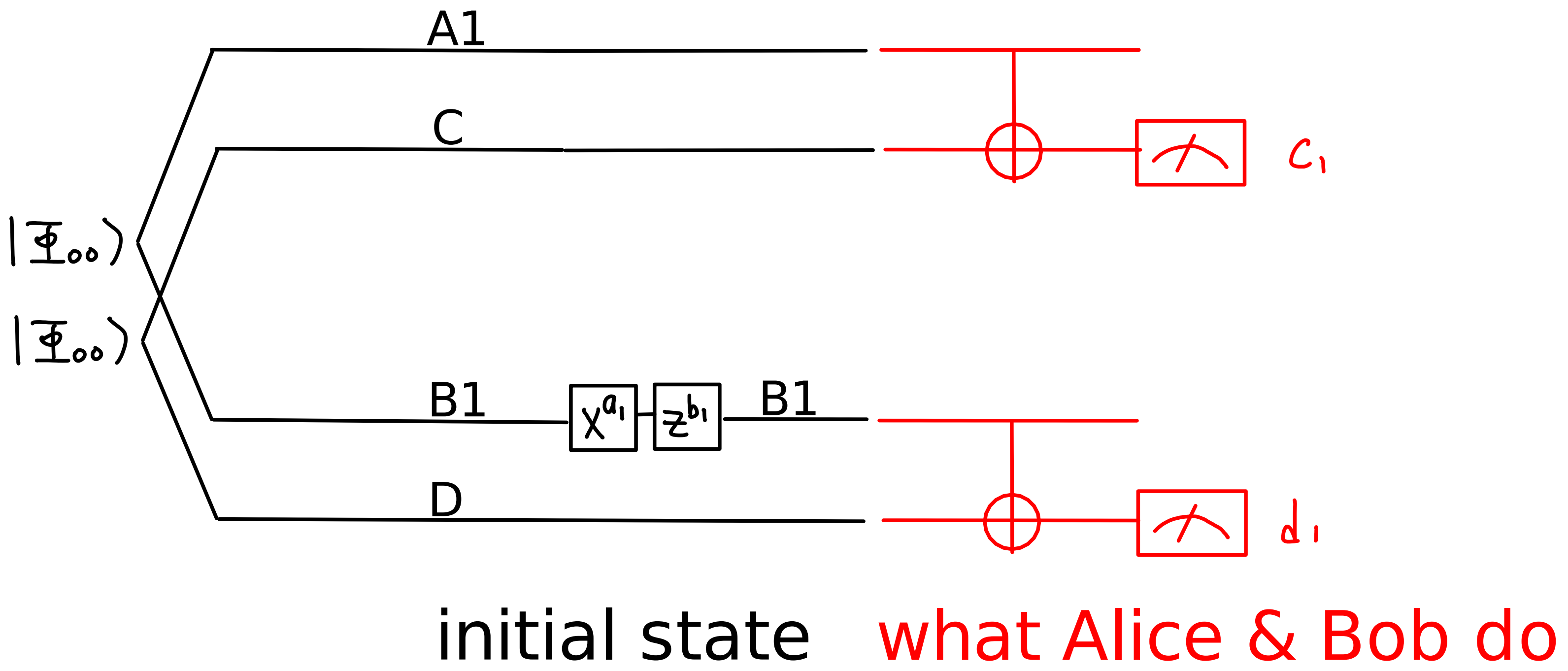
NB The parity of a subset of bits is called a "hash".

Switch to continuous view ...

Why lemma holds (via examples):

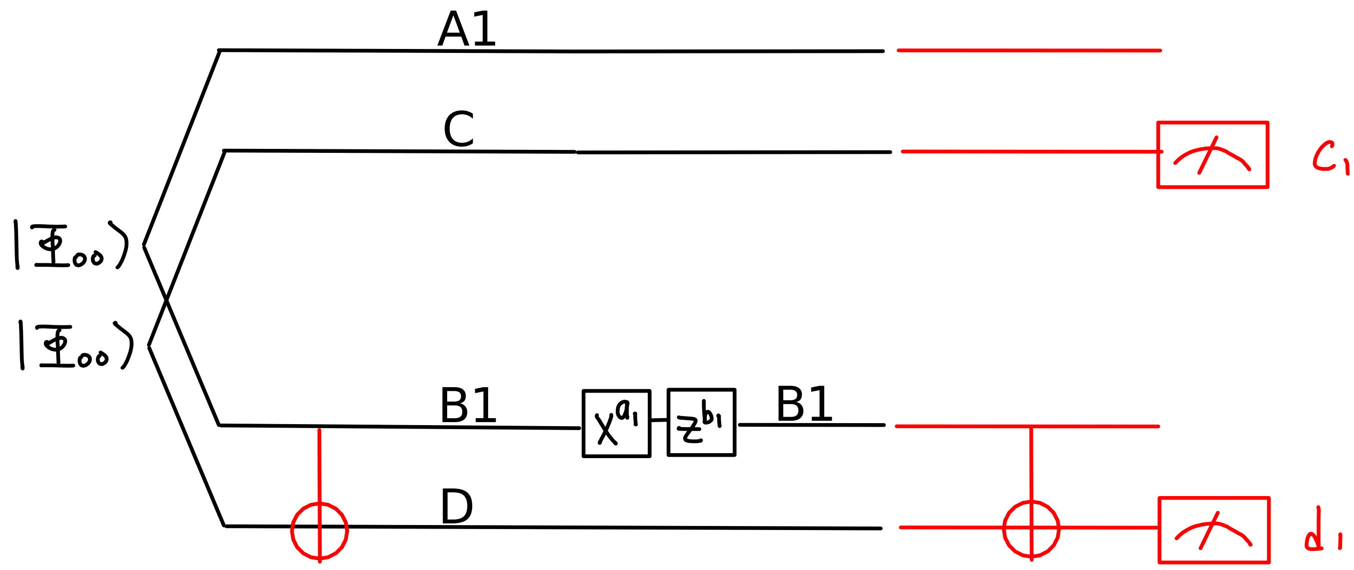
Let the noiseless copy of $|\Phi_{00}\rangle$ live on CD.

Circuit to learn a1:



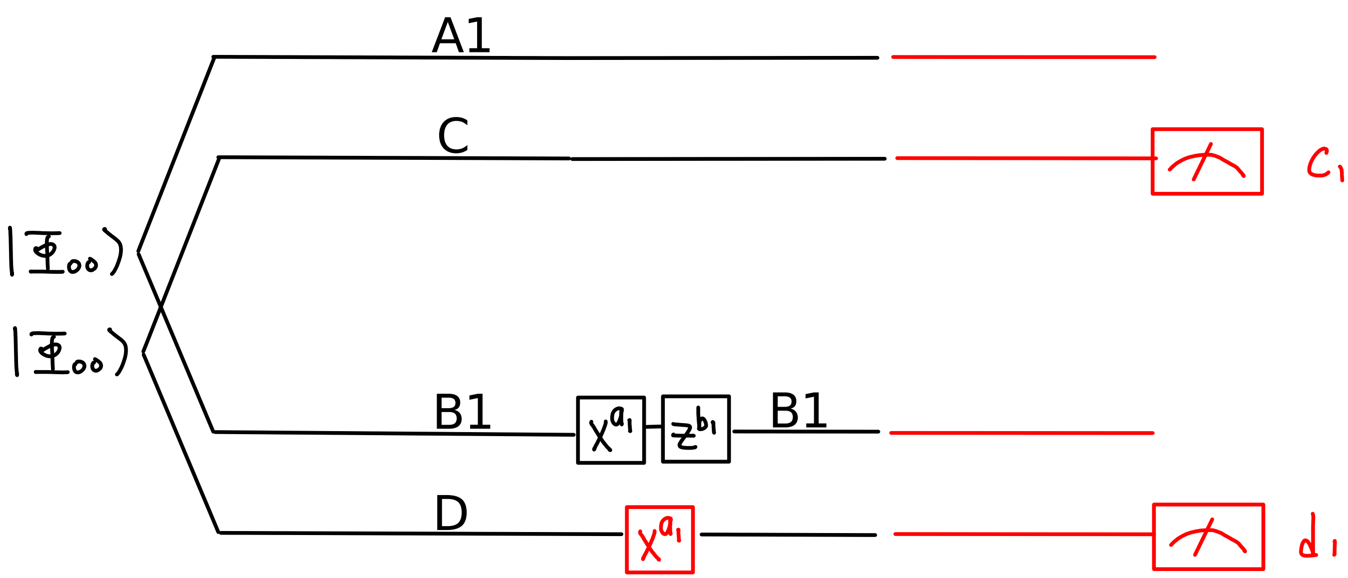
Claim: a1 = c1 + d1 mod 2

|| circuit giving the same output



A1 C and B1 D are in a maximally entangled state, use transpose trick (from assignment 1)

||



CNOT X1 CNOT = XX

CNOT Z1 CNOT = Z1

So, A1 B1 unchanged but CD is now $X^{a_1} \otimes I \, |\Phi_{00}\rangle$.

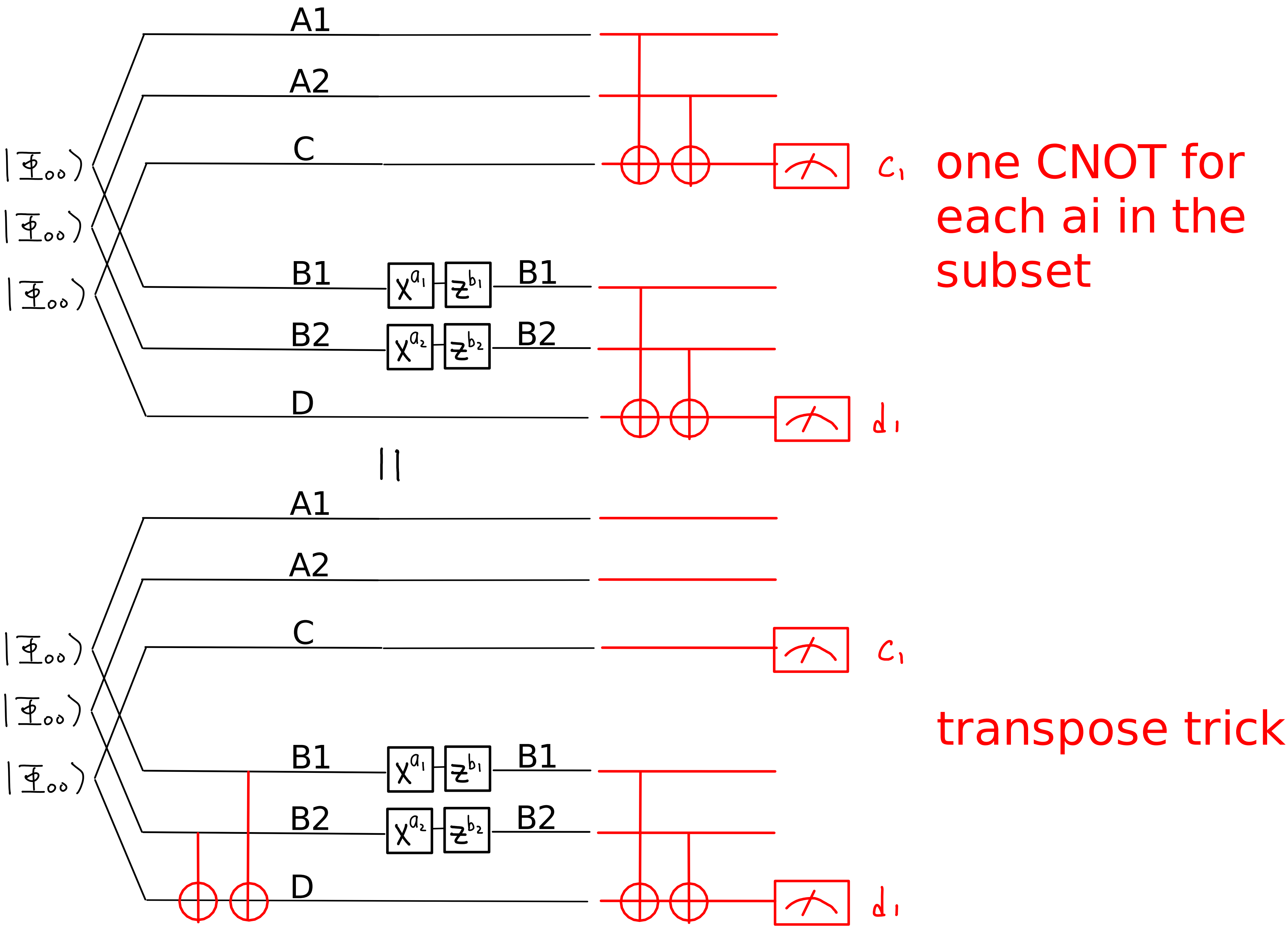
If a1 = 0, meas outcomes satisfy c1 = d1.

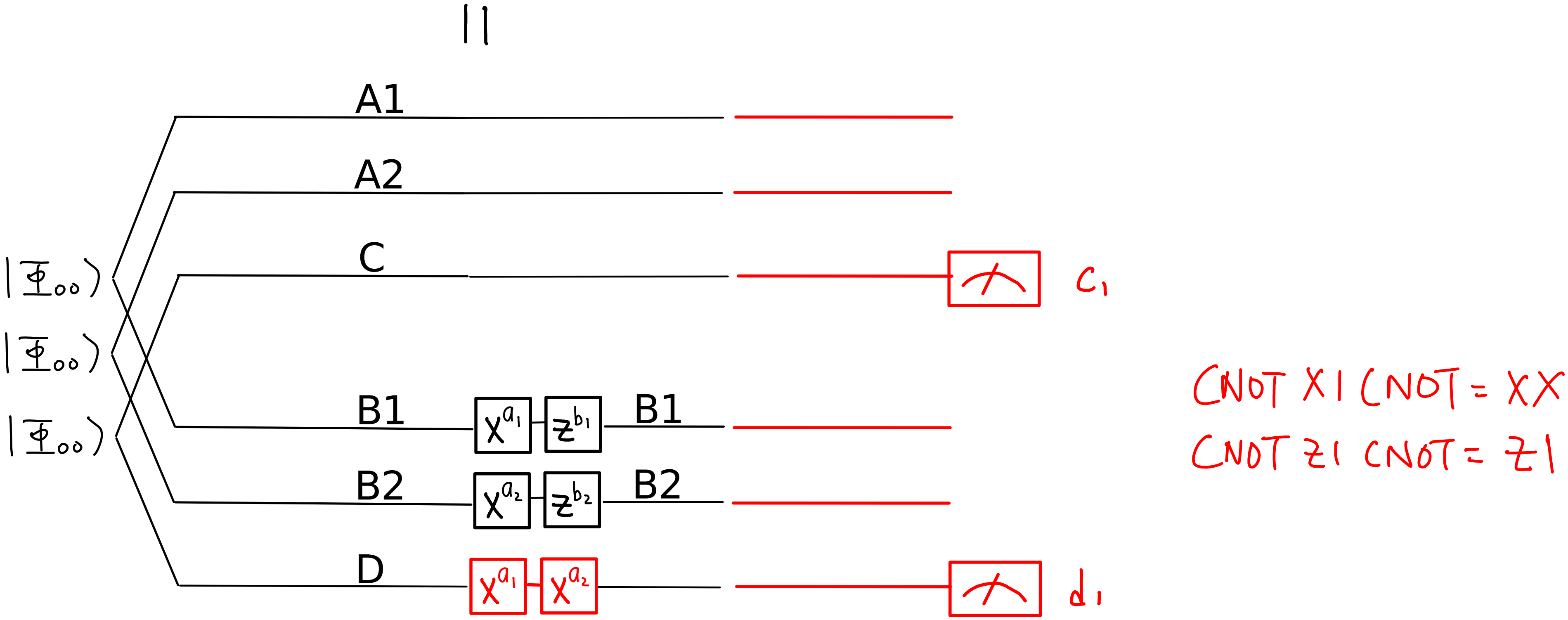
If a1 = 1, state is $\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$ so c1 + d1 mod 2 = 1.

$\therefore$ a1 = c1 + d1 mod 2

Using the authenticated classical channel, Alice and Bob compare c1, d1 to find a1.

Circuit to learn a1+a2 mod 2:

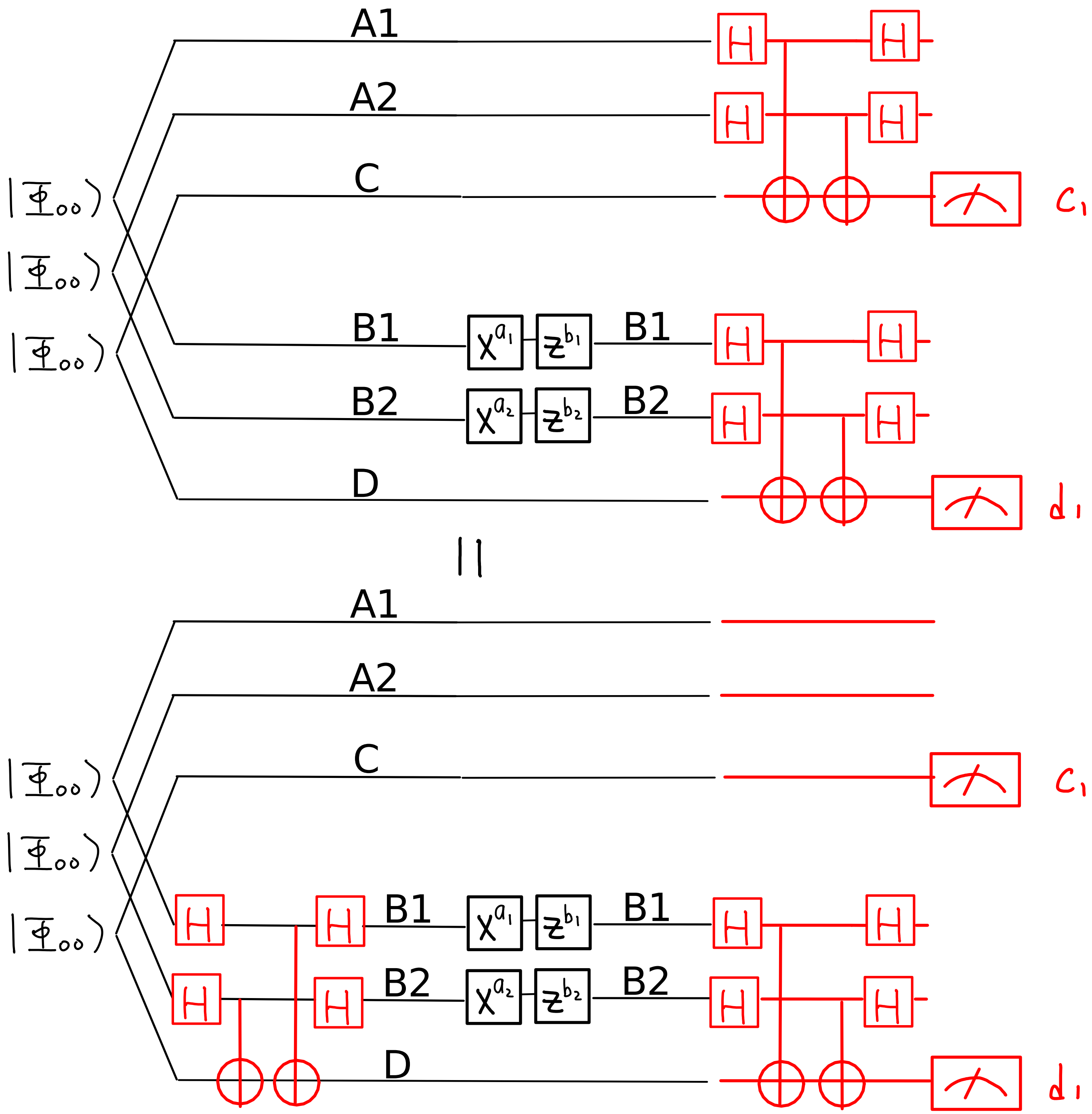




So, c1 + d1 = a1 + a2 mod 2.

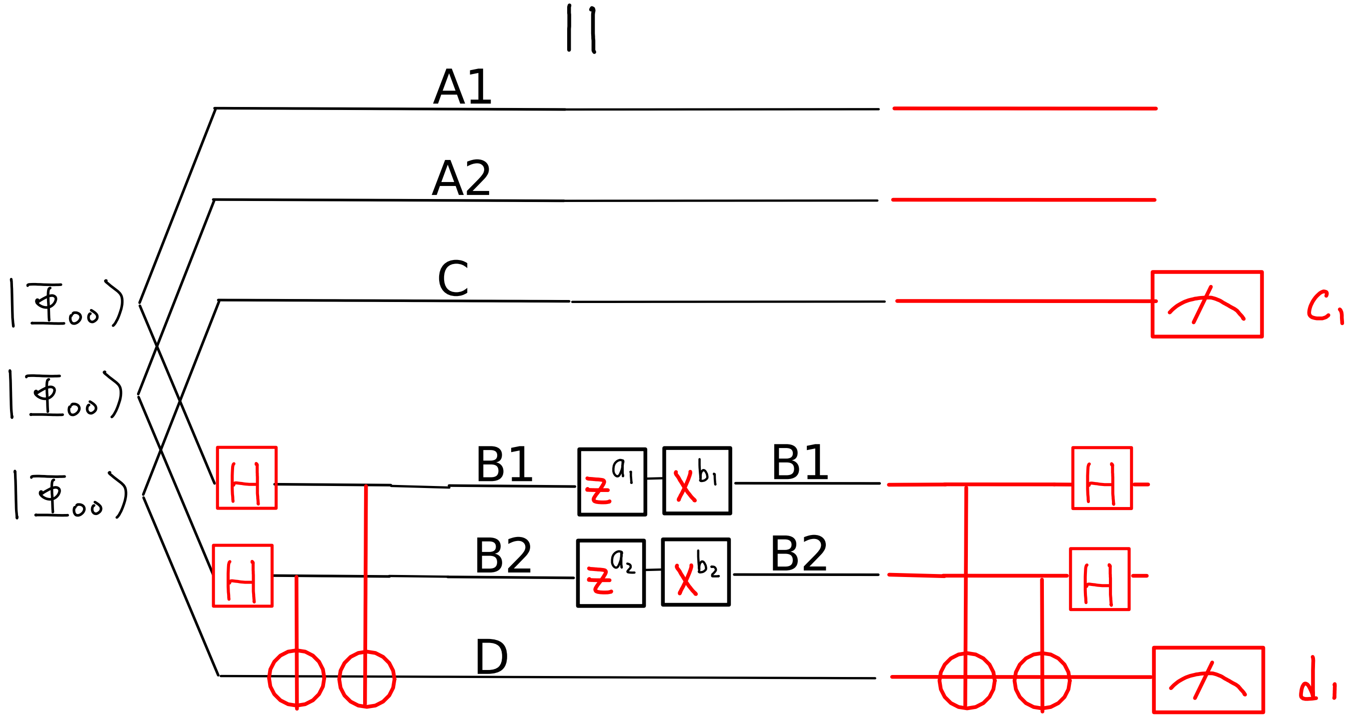
Method applies to the sum of any subset S of the ai's:
if aj in S, Alice applies CNOT from Aj to C,
Bob applies CNOT from Bj to D.

To learn b1+b2 mod 2:

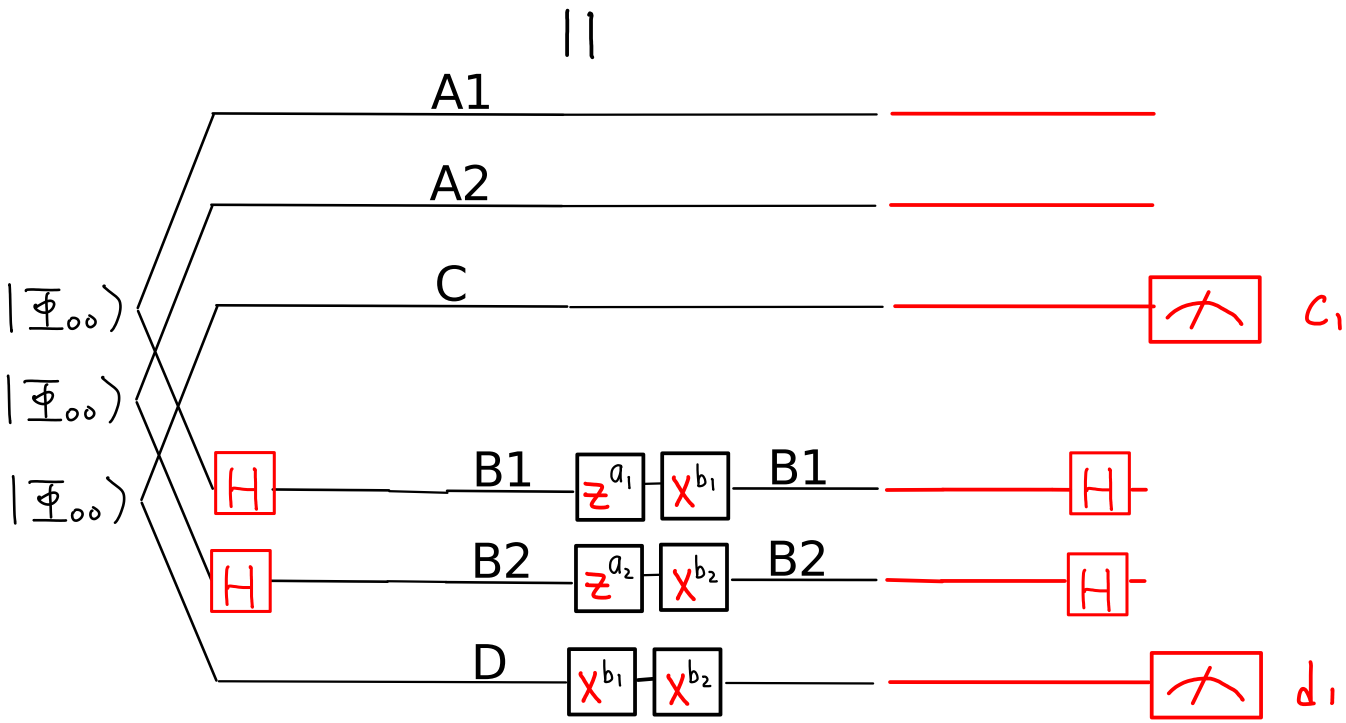


H's added to the control qubits before and after the CNOTs.

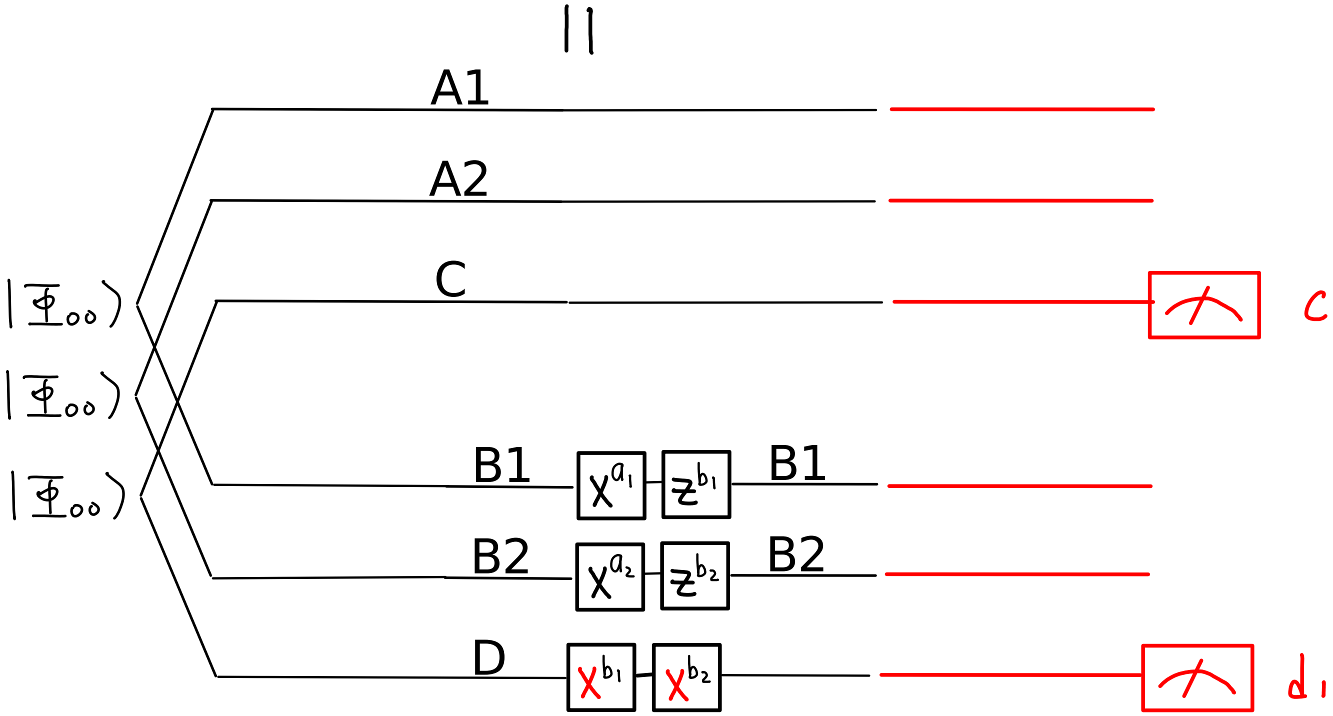
transpose trick



$$HXH = Z$$
$$HZH = X$$



$$CNOT\ X1\ CNOT = XX$$
$$CNOT\ Z1\ CNOT = Z1$$



HXH=Z
HZH=X

So, c1+d1 = b1+b2 mod 2.
The state on A1 A2 B1 B2 is unchanged by the meas.

To learn a1+b2 mod 2:

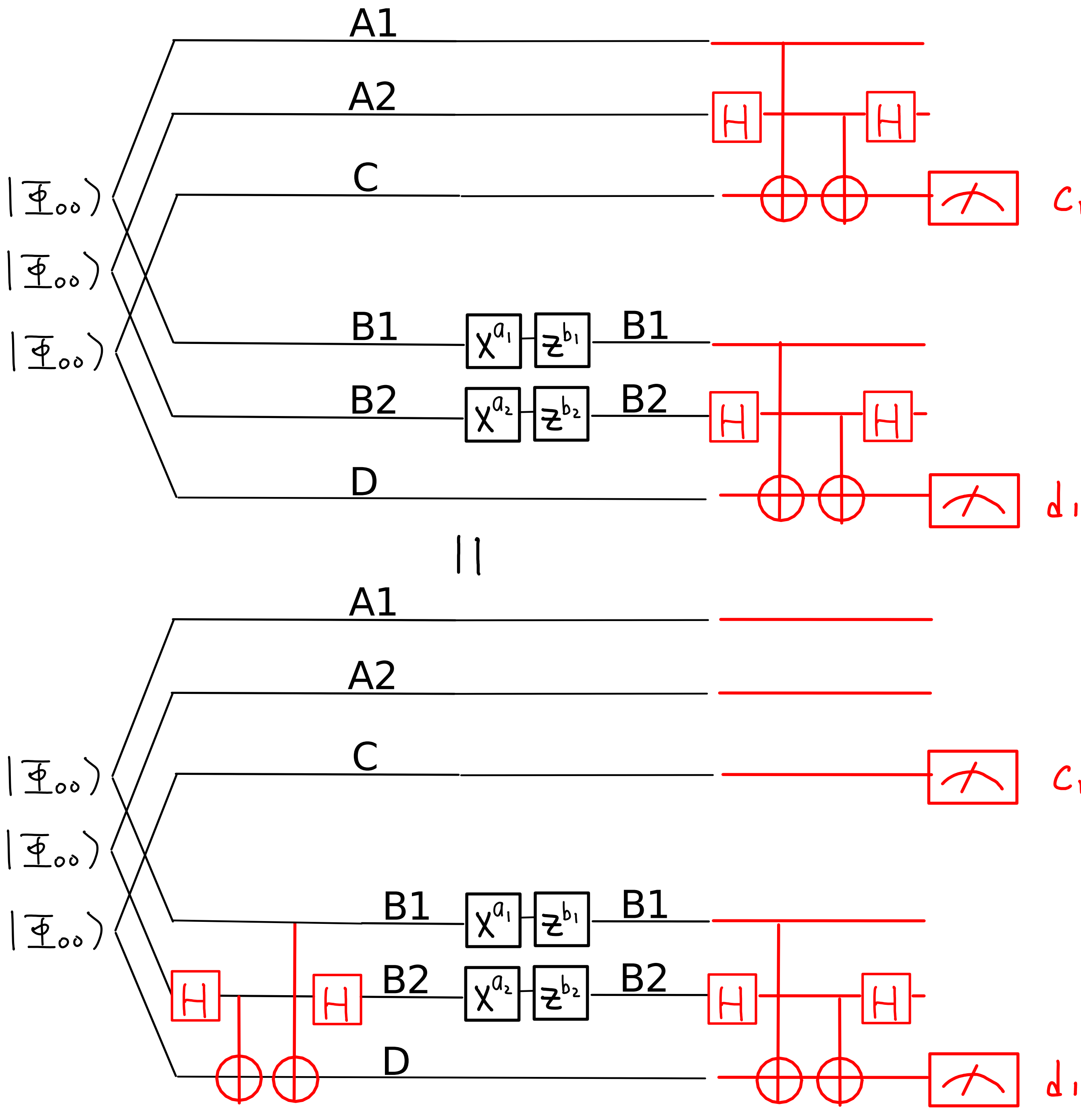
If in the exam, for parts (a), (b) you're guided to find

a1+a2 mod 2

b1+b2 mod 2

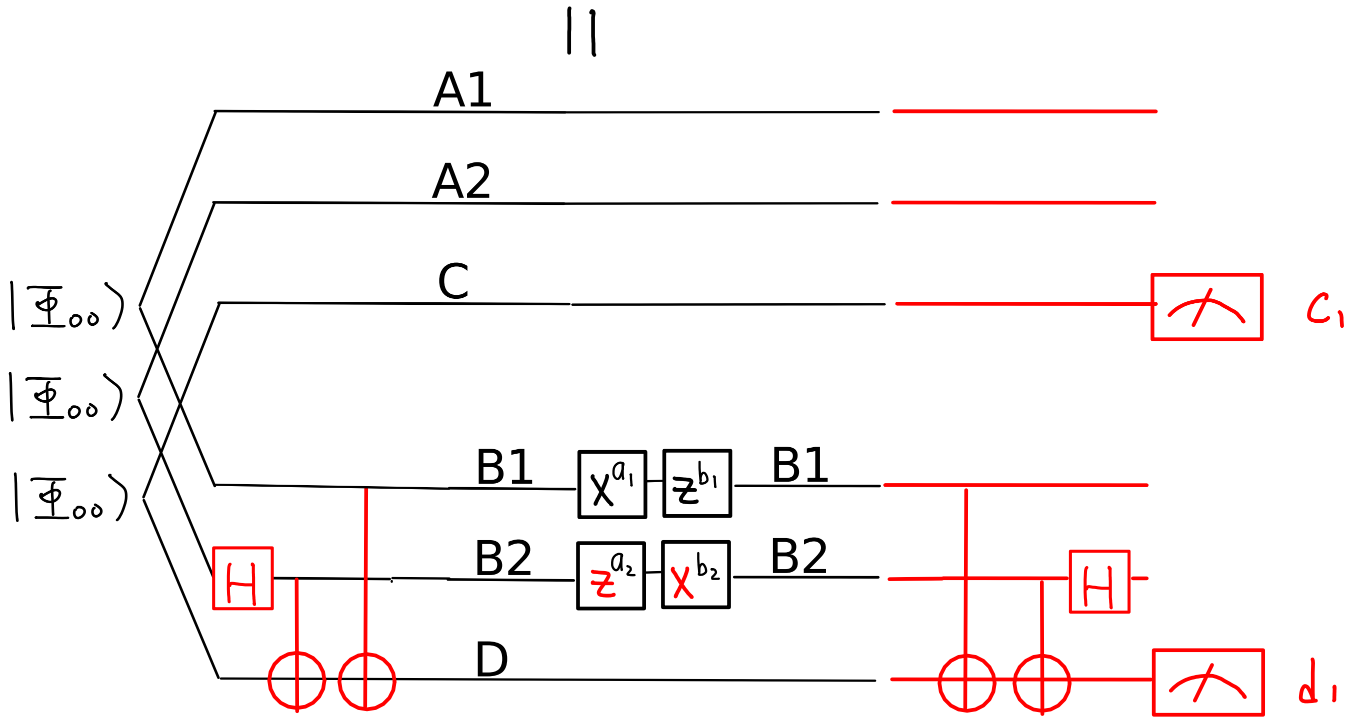
what would you propose for to learn a1+b2 mod 2?

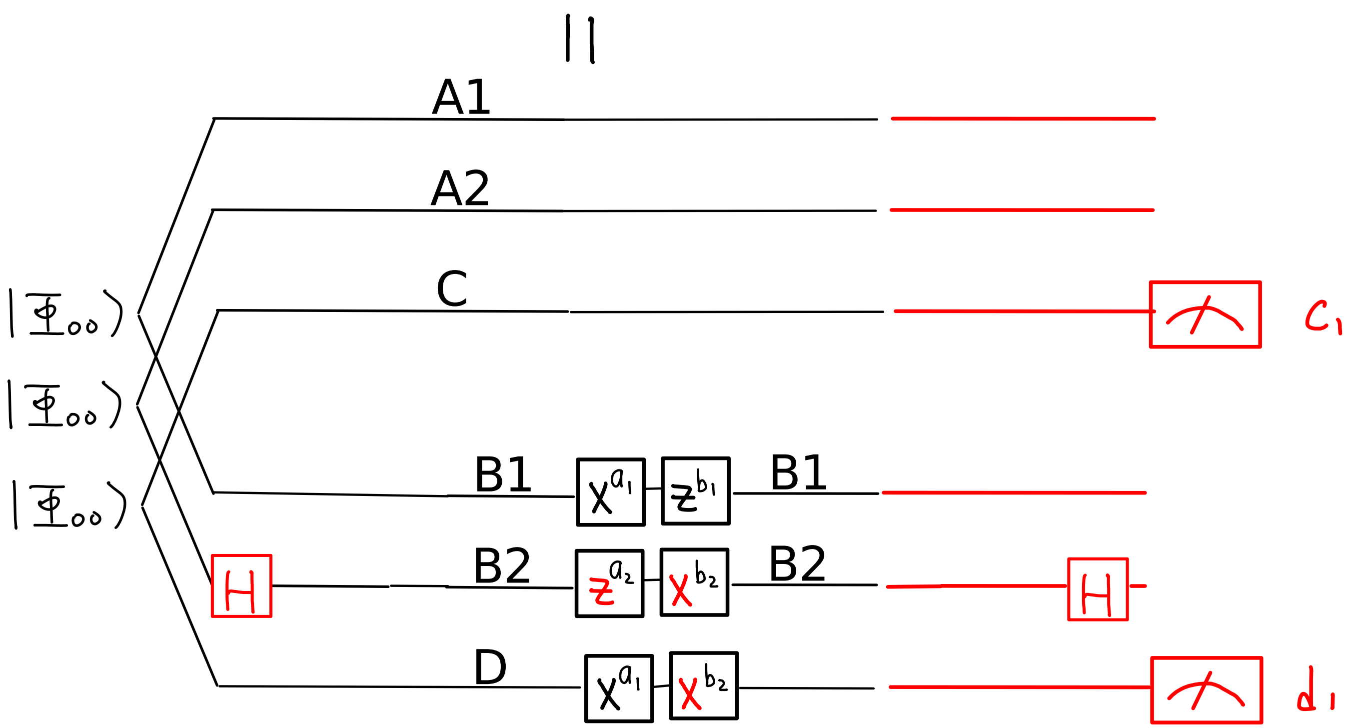
To learn a1+b2 mod 2:

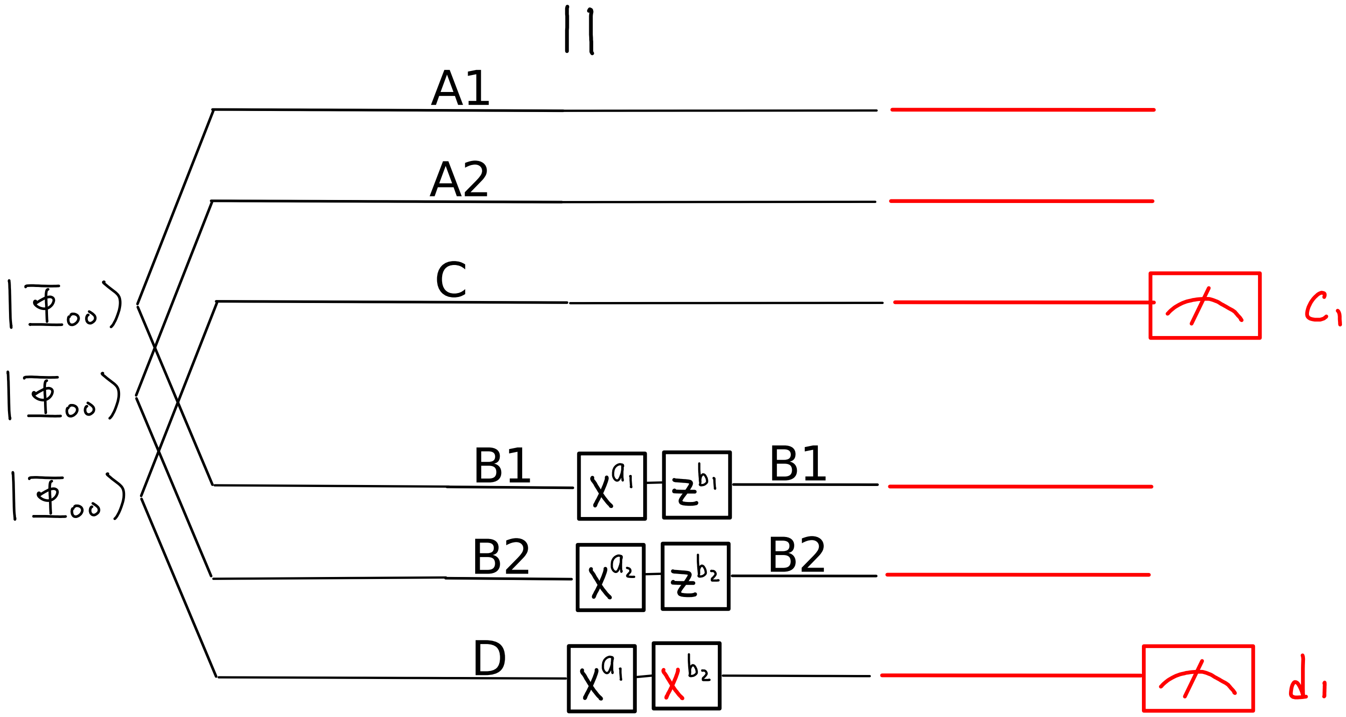


combining how to copy ai and bi (as X's) to CD

transpose trick


A1
A2
C
B1
B2
D
H
B1
B2
c1
d1


A1
A2
C
B1
B2
D
H
B1
B2
c1
d1

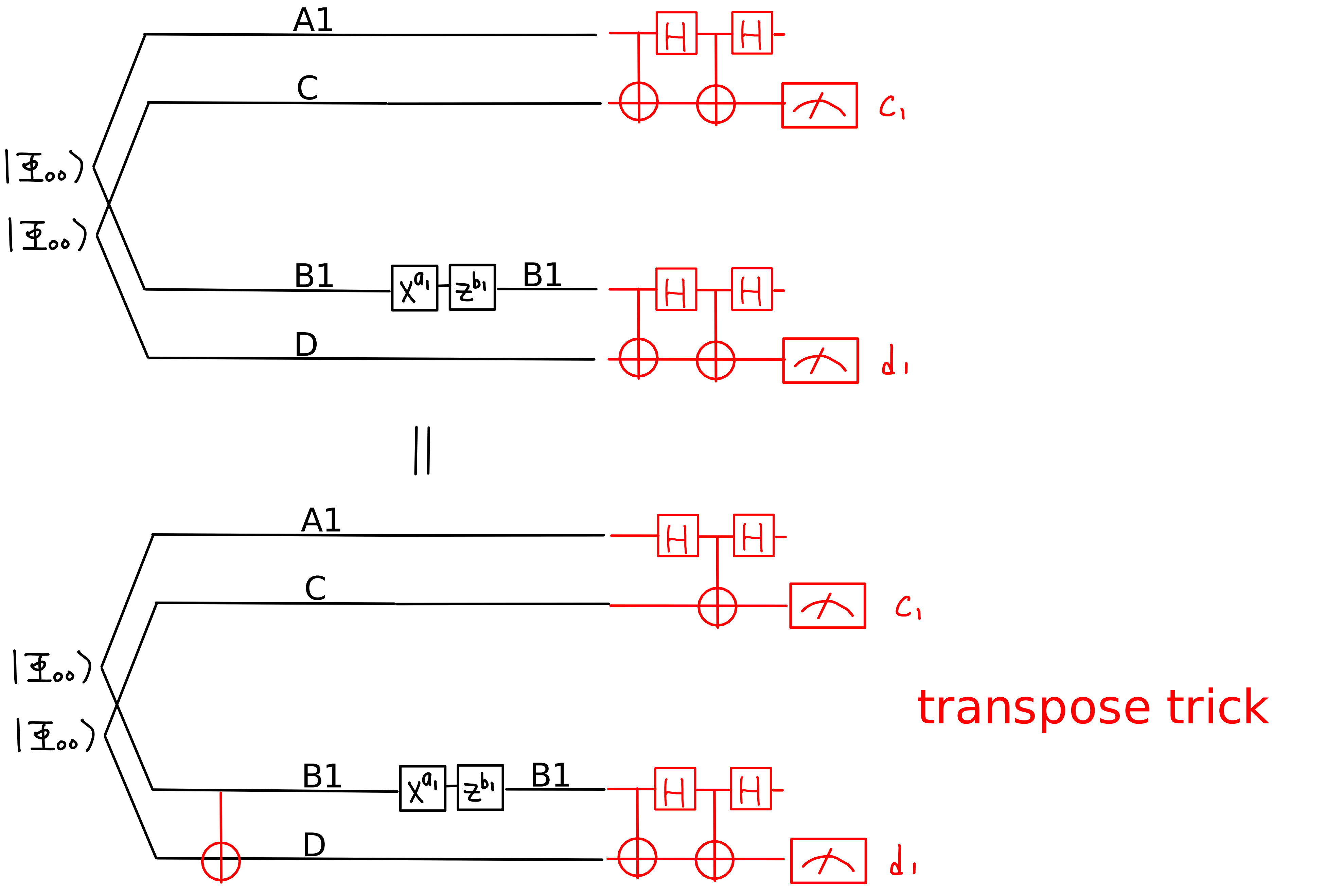


Again, A1B1A2B2 unchanged, c1+d1=a1+b2 mod 2.

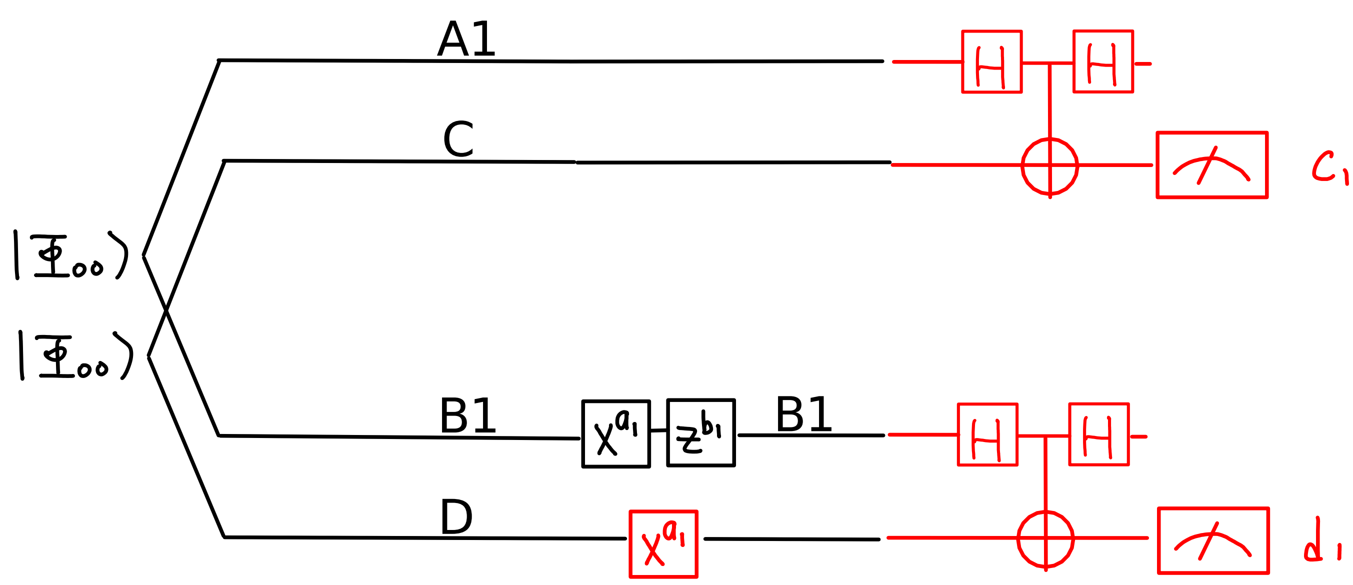
Circuit to learn a1+b1:

What circuit should we use?
Both a1, b1 come from the same EPR pair ...

Circuit to learn a1+b1:



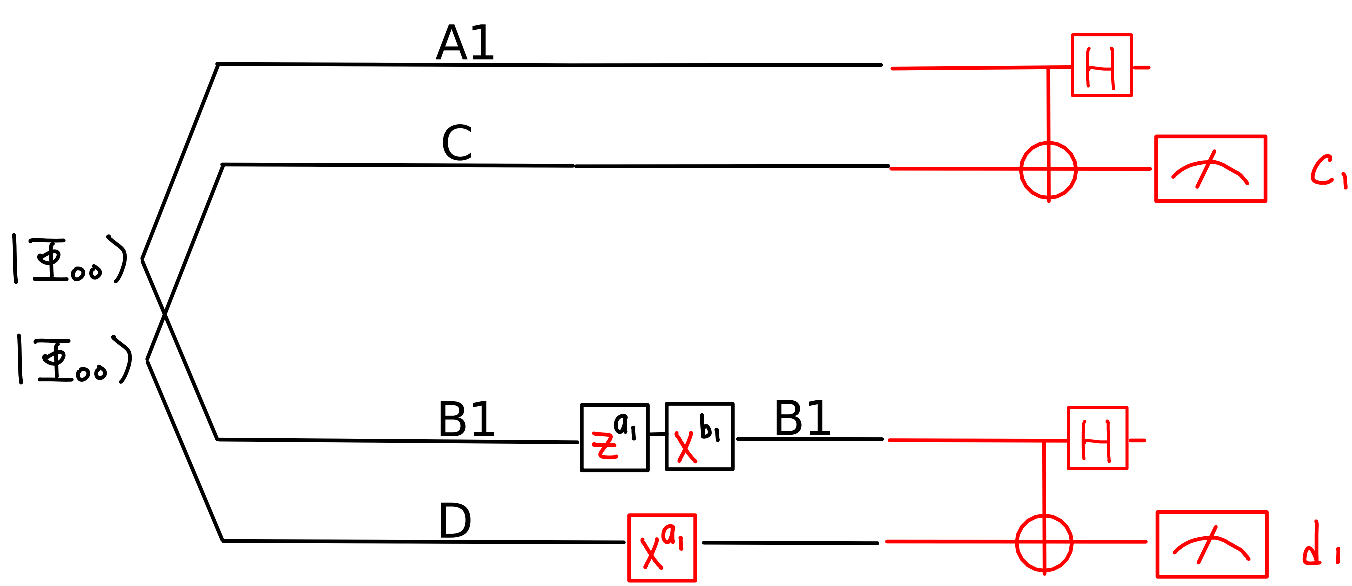
=



CNOT X1 CNOT = XX

CNOT Z1 CNOT = Z1

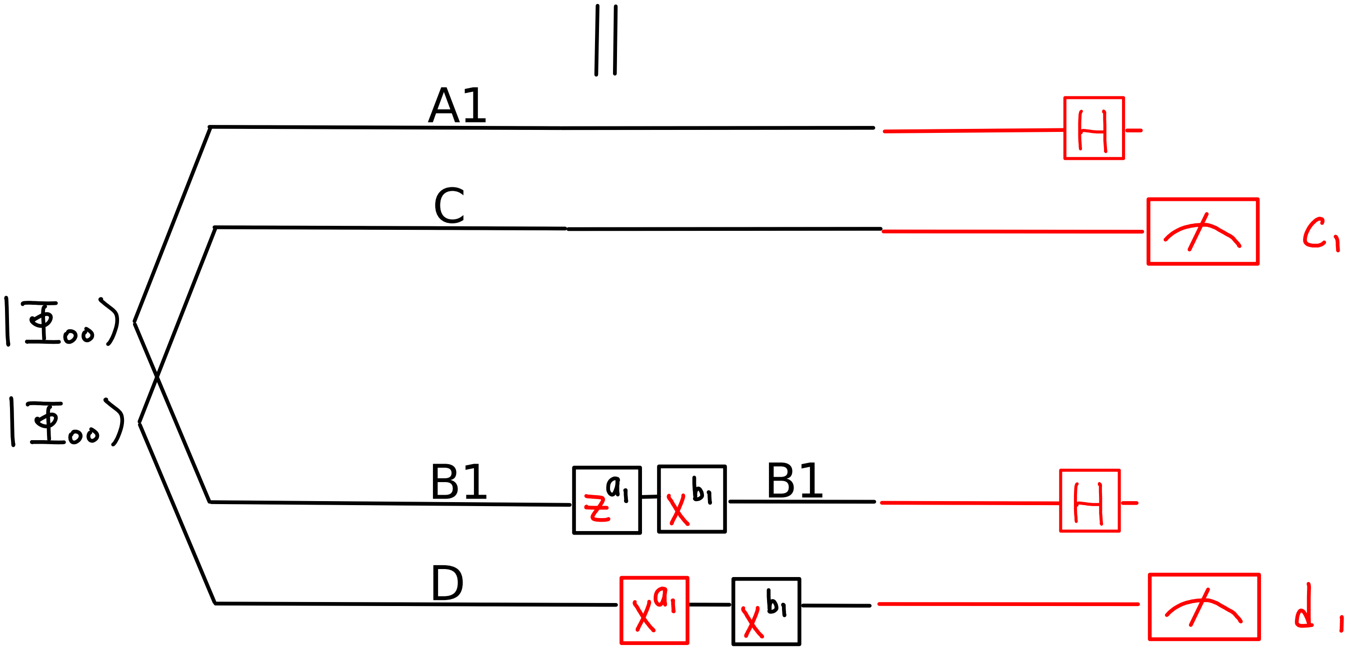
=



transpose trick

HXH=Z

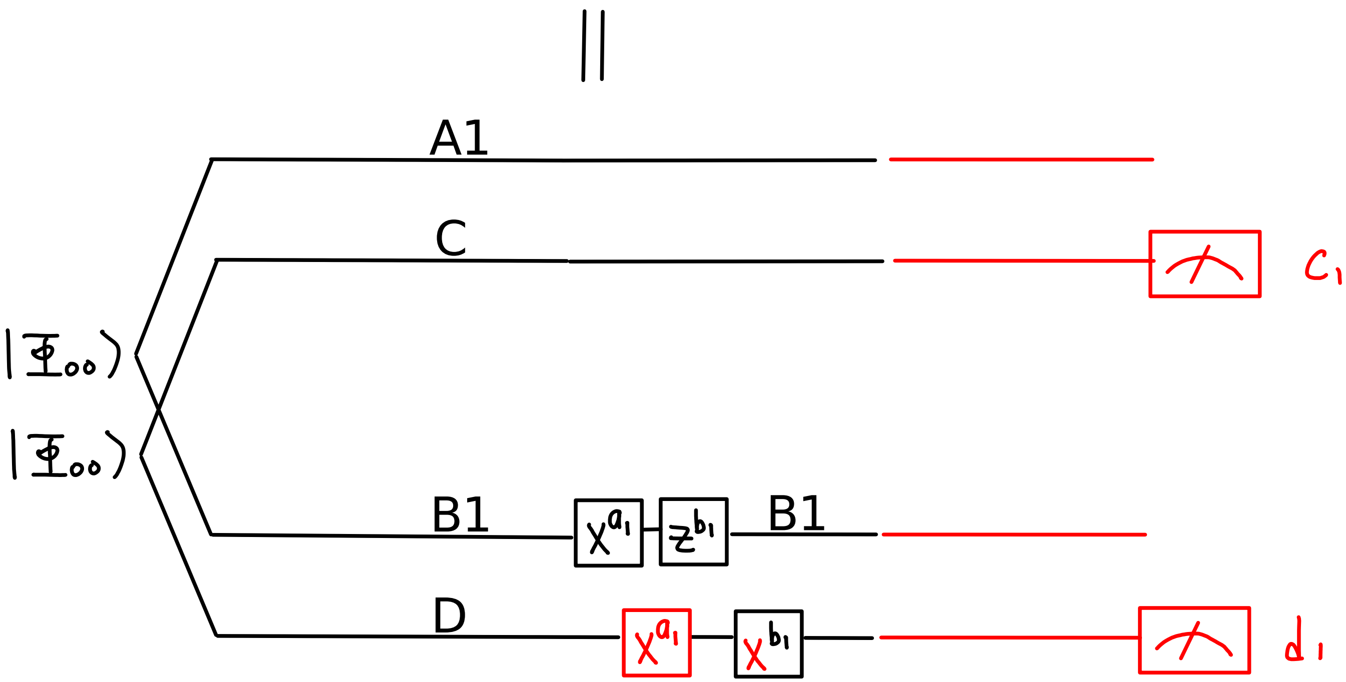
HZH=X



transpose trick

CNOT X1 CNOT = XX

CNOT Z1 CNOT = Z1



transpose trick

HXH=Z

HZH=X

∴ $a1 + b1 = c1 + d1 \mod 2$

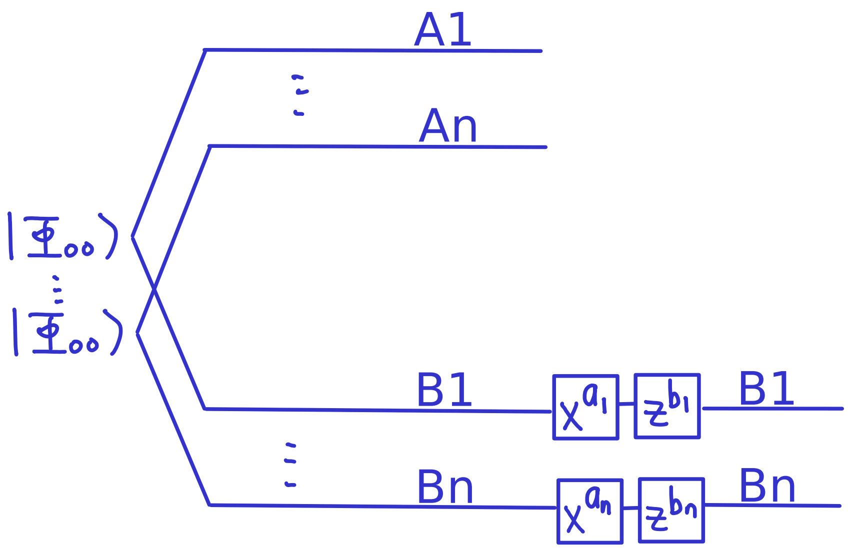
Generalizing these examples give an algorithmic proof for the lemma:

Lemma: with 1 copy of $|\Phi_{00}\rangle$ & CC, Alice and Bob can learn the parity of any subset in $a_1 b_1 a_2 b_2 \ldots a_n b_n$.

We can return to the theorem:

Stop continuous view ...

Theorem: suppose Alice and Bob share the following:



$\longleftrightarrow \quad a_1 b_1\, a_2 b_2 \cdots a_n b_n$

There is a test that consumes k copies of $|\Phi_{00}\rangle$ uses classical communication, without changing the above state, such that

$$\Pr(a_1 b_1 \cdots a_n b_n \neq 00 \cdots 00 \text{ and test passes}) \leq \frac{1}{2^k}$$

Proof (theorem):

If $a_1 b_1 \cdots a_n b_n \neq 00 \cdots 00$, WLOG, let a1 = 1.

Proof (theorem):

If $a_1 b_1 \cdots a_n b_n \neq 0 0 \cdots 0 0$, WLOG, let a1 = 1.

A random subset S of a1 b1 ... an bn is given by taking each bit in S with prob 1/2.

Proof (theorem):

If $a_1 b_1 \cdots a_n b_n \neq 00 \cdots 00$, WLOG, let a1 = 1.

A random subset S of a1 b1 ... an bn is given by taking each bit in S with prob 1/2.

Let S' = S \ {a1}, with parity u.

Proof (theorem):

If $a_1 b_1 \cdots a_n b_n \neq 00 \cdots 00$, WLOG, let a1 = 1.

A random subset S of a1 b1 ... an bn is given by taking each bit in S with prob 1/2.

Let S' = S \ {a1}, with parity u.

wp 1/2: a1 in S, parity(S) = u+1
wp 1/2: a1 not-in S, parity(S) = u

Proof (theorem):

If $a_1 b_1 \cdots a_n b_n \neq 00 \cdots 00$, WLOG, let a1 = 1.

A random subset S of a1 b1 ... an bn is given by taking each bit in S with prob 1/2.

Let S' = S \ {a1}, with parity u.

wp 1/2: a1 in S, parity(S) = u+1
wp 1/2: a1 not-in S, parity(S) = u

For all u, wp 1/2, parity(S) = 1.

Thus a random subset parity will detect any nontrivial Pauli error on the n EPR pairs wp 1/2.

Can amplify this detection ability by repeating ...

Proof (theorem):

If $a_1 b_1 \cdots a_n b_n \neq 00 \cdots 00$, WLOG, let a1 = 1.

A random subset S of a1 b1 ... an bn is given by taking each bit in S with prob 1/2.

Let S' = S \ {a1}, with parity u.

wp 1/2: a1 in S, parity(S) = u+1
wp 1/2: a1 not-in S, parity(S) = u

For all u, wp 1/2, parity(S) = 1.

"random hashing"

Alice and Bob pick k random subsets S1, S2, ... , Sk, independently, and find their parities. They pass the test iff all the subset parities are even.

Proof (theorem):

If $a_1 b_1 \cdots a_n b_n \neq 00 \cdots 00$, WLOG, let a1 = 1.

A random subset S of a1 b1 ... an bn is given by taking each bit in S with prob 1/2.

Let S' = S \ {a1}, with parity u.

wp 1/2: a1 in S, parity(S) = u+1
wp 1/2: a1 not-in S, parity(S) = u

For all u, wp 1/2, parity(S) = 1.

"random hashing"

Alice and Bob pick k random subsets S1, S2, ... , Sk, independently, and find their parities. They pass the test iff all the subset parities are even.

$$\Pr(a_1 b_1 \cdots a_n b_n \neq 00 \cdots 00 \text{ and test passes})$$
$$\leq \Pr(\text{test passes} \mid a_1 b_1 \cdots a_n b_n \neq 00 \cdots 00) = \frac{1}{2^k}$$

If all the subset parities are even, Alice and Bob conclude that they hold n noiseless EPR pairs $|\Phi_{00}\rangle$.
They return k pairs to "the bank" and harvest n-k pairs which can be measured to give them n-k bits of key.

This gives an information theoretic security proof of E91 using an insecure noiseless quantum channel.

On borrowing and return k EPR pairs from the bank -- this is not necessary. Also, an evil Eve can jam the quantum channel and "bankrupt" Alice and Bob causing them to be in serious entanglement debt :)

On borrowing and return k EPR pairs from the bank -- this is not necessary. Also, an evil Eve can jam the quantum channel and "bankrupt" Alice and Bob causing them to be in serious entanglement debt :)

Idea from BDSW96:
1a. Take the n potentially noisy EPR pairs
1b. pick S1 (random subset of 2n bits)
1c. write parity(S1) on one of the pairs

On borrowing and return k EPR pairs from the bank -- this is not necessary. Also, an evil Eve can jam the quantum channel and "bankrupt" Alice and Bob causing them to be in serious entanglement debt :)

Idea from BDSW96:
1a. Take the n potentially noisy EPR pairs
1b. pick S1 (random subset of 2n bits)
1c. write parity(S1) on one of the pairs (with the understanding that the noise of that special pair has to be added to the outcome, and also that the noise will propagate to the other n-1 pairs) and measure that special pair.

On borrowing and return k EPR pairs from the bank
-- this is not necessary. Also, an evil Eve can jam
the quantum channel and "bankrupt" Alice and Bob
causing them to be in serious entanglement debt :)

Idea from BDSW96:
1a. Take the n potentially noisy EPR pairs
1b. pick S1 (random subset of 2n bits)
1c. write parity(S1) on one of the pairs (with the understanding that the noise of that special pair has to be added to the outcome, and also that the noise will propagate to the other n-1 pairs) and measure that special pair.
2. Repeat for n-1 EPR pairs
3. Repeat for n-2 EPR pairs
...
until n-k pairs remaining.
The state changes, more messier algebra ... but it works.

Will keep our discussion clean with the catalytic approach.

What about noise? i.e., channel is noisy without eavesdropping, and can also be attacked by Eve. The noisy channel case appeared difficult to analyse because Eve may mask herself as channel noise.

What about noise? i.e., channel is noisy without eavesdropping, and can also be attacked by Eve. The noisy channel case appeared difficult to analyse because Eve may mask herself as channel noise.

Fact: noiseless copies of $|\Phi_{00}\rangle$ are necessarily secure; doesn't matter how the noise get there, once we get rid of it.

Correct intuition: if the EPR pairs are noiseless, then they're in a pure state so no one else has correlations with the state so measuring will give a private key!

We reduce the security of E91 using noisy channels to the ability to correct Pauli errors (an upgrade from the security of E91 using noiseless channel via the ability to detect Pauli errors).

For noisy insecure channel:

If Alice and Bob have characterized the channel,
they use QECC to obtain near-noiseless communication
without Eve; analysis reduces to the noiseless case.

For noisy insecure channel:

If Alice and Bob have characterized the channel, they use QECC to obtain near-noiseless communication without Eve; analysis reduces to the noiseless case.

Else: Alice and Bob take random Bell pairs to estimate X and Z error rates p_x , p_z (this requires large samples, but they can be sublinear in n).

For noisy insecure channel:

If Alice and Bob have characterized the channel, they use QECC to obtain near-noiseless communication without Eve; analysis reduces to the noiseless case.

Else: Alice and Bob take random Bell pairs to estimate X and Z error rates p_x, p_z (this requires large samples, but they can be sublinear in n).

So, there are $\approx \binom{n}{n p_x} \binom{n}{n p_z} \approx 2^{n h(p_x)} \, 2^{n h(p_z)}$ such $a_1 b_1 \cdots a_n b_n$.

$h(p_x) = -p_x \log p_x - (1-p_x) \log (1-p_x)$

For noisy insecure channel:

If Alice and Bob have characterized the channel, they use QECC to obtain near-noiseless communication without Eve; analysis reduces to the noiseless case.

Else: Alice and Bob take random Bell pairs to estimate X and Z error rates p_x , p_z (this requires large samples, but they can be sublinear in n).

So, there are $\approx \binom{n}{np_x}\binom{n}{np_z} \approx 2^{nh(p_x)}\, 2^{nh(p_z)}$ such $a_1 b_1 \cdots a_n b_n$.

$h(p_x) = -p_x \log p_x - (1-p_x)\log(1-p_x)$

Each random subset parity gives roughly 1 bit of info.

$\therefore\ nh(p_x) + nh(p_z)$ parities (+ a little more) identify the error.

(Syndrome of a random stabilizer code !)

Requires a bit more analysis, but learning subset parities is an efficient way to learning bit-strings.

Finally, Alice and Bob correct the identified error, and run the k parity checks as in the noiseless case, s.t.:

$$\Pr\left(\text{output } Q\,|\Phi_{00}\rangle^{\otimes n(1-h(p_x)-h(p_z))} \text{ and test passes}\right) \leq 2^{-k}.$$

any nontrivial Pauli error

key rate

Entanglement is awesome!

It can be reliably tested by two remote parties.

Many testing methods have been developed.

e.g., tested EPR pairs can be used for *secure* teleportation of quantum messages !
This idea also give rise to authentication protocols for sending quantum messages.

Entanglement is awesome!

It can be reliably tested by two remote parties.

Many testing methods have been developed.

e.g., tested EPR pairs can be used for *secure* teleportation of quantum messages !
This idea also give rise to authentication protocols for sending quantum messages.

e.g., self-testing means even the operations by Alice and Bob to test EPR pairs need not be trusted! Recall nonlocal games from topic 4. Some are "rigid": if the observed correlation is close to max allowed by QM, the shared state and local operations *must be of a certain form* and some games (CHSH, magic square game) can be verified to be like E91 with measurement outcomes giving secure key.

E91 is conceptually simple, but Alice and Bob need to hold quantum data and apply quantum gates to perform random hashing.

BB84 is much easier to implement.

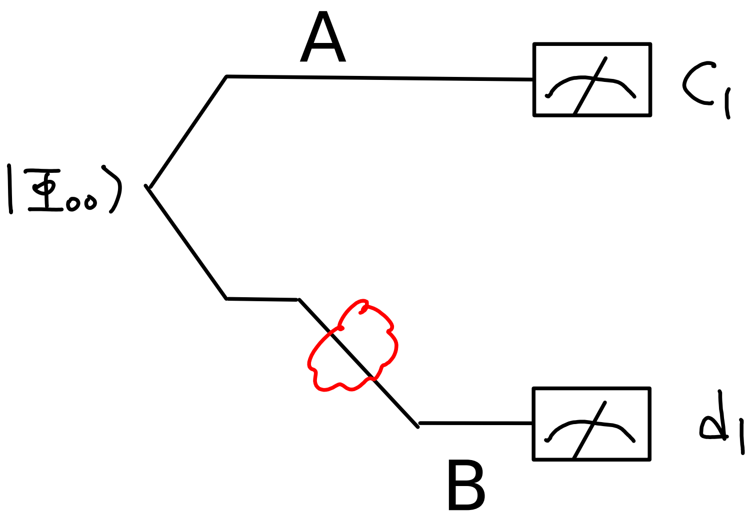
E91 is conceptually simple, but Alice and Bob need to hold quantum data and apply quantum gates to perform random hashing.

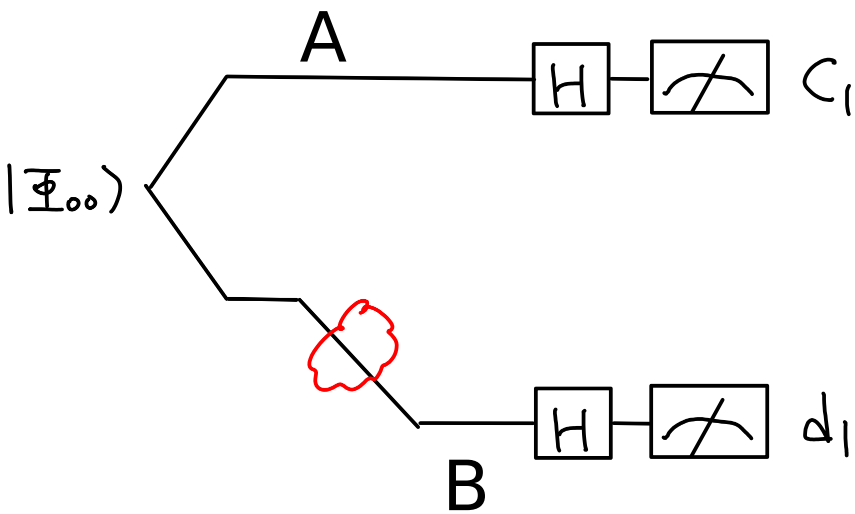
BB84 is much easier to implement.

How do we relate these 2 protocols?

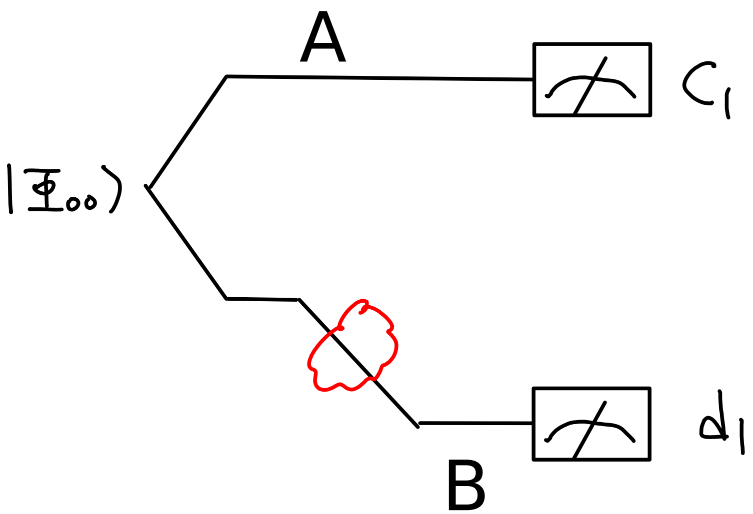
Recall bit commitment, how Alice can measure entangled state to create random bits in {|0>,|1>} or {|+>,|->} basis.

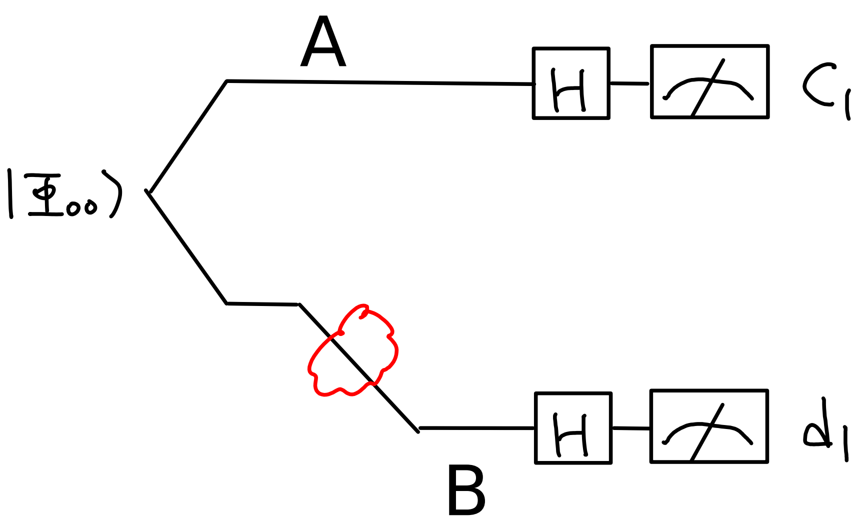
E91 : wp 1/2 do each of the following



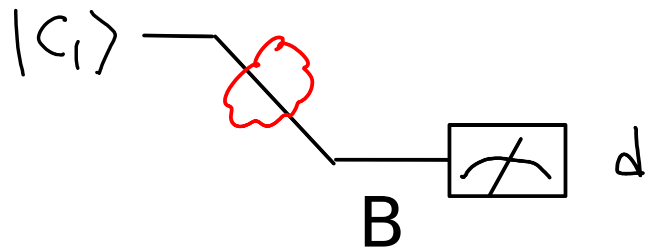


E91 : wp 1/2 do each of the following



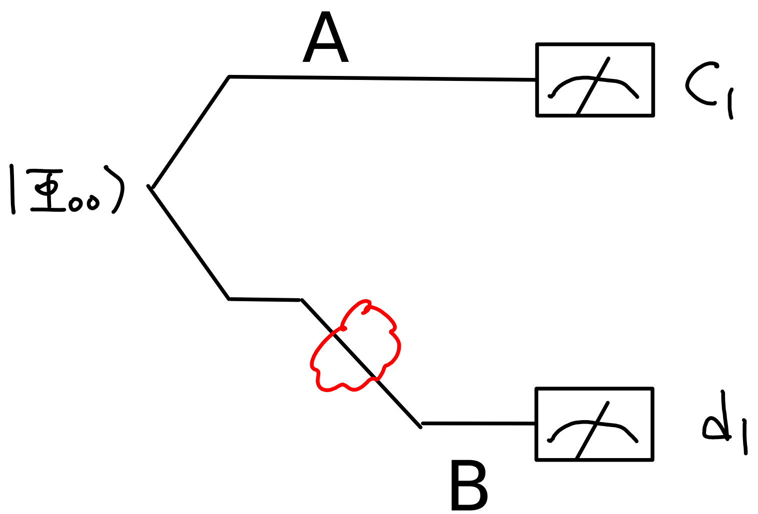


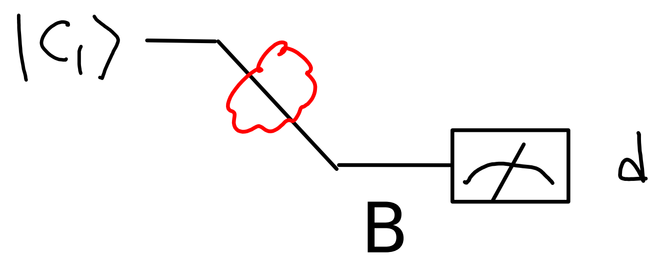
Operations on A commute with the sending. If Alice measures first, there is no observable diff, & we get:

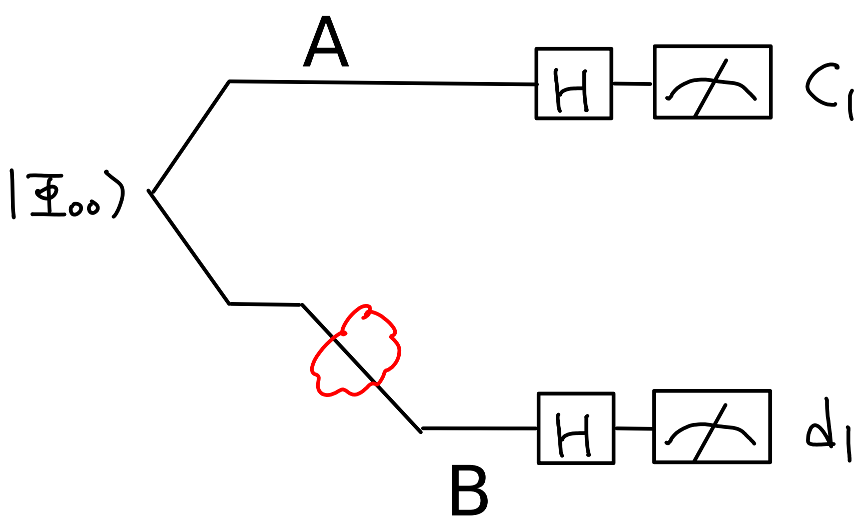


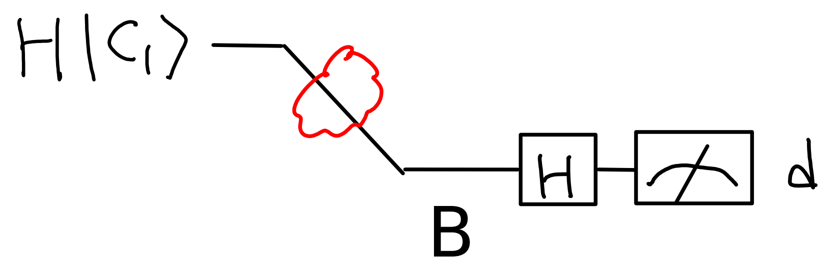
E91 : wp 1/2 do each of the following

Operations on A commute with the sending. If Alice measures first, there is no observable diff, & we get:









BB84!

Harder to transform the security proof from E91 (with random subset parity checks) to BB84 (with error correction and privacy amplification).

Harder to transform the security proof from E91 (with random subset parity checks) to BB84 (with error correction and privacy amplification).

* Replace random subset parities over a1 b1 a2 b2 ... an bn (random stabilizer code) by separate parities of a1 a2 ... an, and of b1 b2 ... bn (good CSS code).

Harder to transform the security proof from E91 (with random subset parity checks) to BB84 (with error correction and privacy amplification).

* Replace random subset parities over a1 b1 a2 b2 ... an bn (random stabilizer code) by separate parities of a1 a2 ... an, and of b1 b2 ... bn (good CSS code).

* X error correction (by Z generators) corresponds to classical error correction, and Z error correction (by X generators) corresponds to privacy amplification.

Prof. Thomas Jennewein's experiment has Alice riding on a plane and Bob sitting on the ground. Each pass generates 100 k bits of key!

Prof. Thomas Jennewein's experiment has Alice riding on a plane and Bob sitting on the ground. Each pass generates 100 k bits of key!

The trailer on Bearinger label IQC (now moved to back of RAC) is part of the test equipment. It used to connect a room in the Phys building to Prof. Laflamme's Perimeter Institute office.

Prof. Thomas Jennewein's experiment has Alice riding on a plane and Bob sitting on the ground. Each pass generates 100 k bits of key!

The trailer on Bearinger label IQC (now moved to back of RAC) is part of the test equipment. It used to connect a room in the Phys building to Prof. Laflamme's Perimeter Institute office.

It's nice some version of QKD has been realized and we do not need to wait for 20 or 30 years ...