Department of Information Engineering
MSc in Computer Engineering (a.y. 2024/2025)
University of Pisa

Quantum Computing and Quantum Internet

Luciano Lenzini
Full Professor
Department of Information Engineering
School of Engineering
University of Pisa, Italy
e-mail: lenzini44@gmail.com
http://www.iet.unipi.it/~lenzini/
http://www.originiinternetitalia.it/it/

Superconducting Qubits are Supercooled RF Circuits

Image: IBM

Quantum Key Distribution (QKD)

Concept of QKD

- Quantum key distribution (QKD) provides a means for two parties, traditionally called Alice and Bob, to establish **matching**, **assuredly private**, **cryptographic keys** across a **potentially insecure communications channel**
- There are many different ways in which a QKD scheme can be accomplished
- Although they may differ in the quantum physical resource used to encode the key material, at their core they all work basically the same way

Concept of QKD

- First, Alice generates a stream of truly random bits from which Alice and Bob are to distill a matching private cryptographic key
- Neither Alice nor Bob have any particular key in mind at the outset
- Once the stream of random bits has been generated, they are encoded in the quantum states of a corresponding stream of photons
- The encoding is chosen in such a manner as to guarantee that any attempt to measure the quantum-encoded key material in transit, without proper knowledge of the encoding used, will increase the bit error rate (BER) on the channel sufficient to expose the fact that eavesdropping had occurred

Concept of QKD

- Nothing like this is possible in conventional cryptography because classical information can be read and re-transmitted in a manner imperceptible to the legitimate parties
- However, in the quantum realm, the **laws of quantum physics** make it impossible to read the keys without scrambling enough of them to cause a detectable increase in the bit error rate (*BER*) on the channel, and hence alert the legitimate parties to the presence of an eavesdropper

Concept of QKD

- If such a test reveals no evidence of eavesdropping, then the channel may be assumed to have been secure during the key distribution, and hence the random bits remaining after the protocol has ended may be used as cryptographic keys
- However, if eavesdropping was detected, the keys exchanged must be discarded and a fresh key distribution exchange attempted

Concept of QKD

- Unlike classical public key cryptosystems whose security relies upon the difficulty of **factoring integers** or computing **discrete logarithms**, the security of QKD rests upon **quantum physical laws** that cannot be circumvented no matter how mathematically gifted, algorithmically sophisticated, or computationally powerful an adversary might be
- The basic idea behind QKD is the following fundamental observation: *Eve cannot gain any information from the qubits transmitted from Alice to Bob without disturbing their state*

Concept of QKD

- **First** of all, by the **no-cloning** theorem, Eve cannot clone Alice's qubit
- **Second**, we have the following

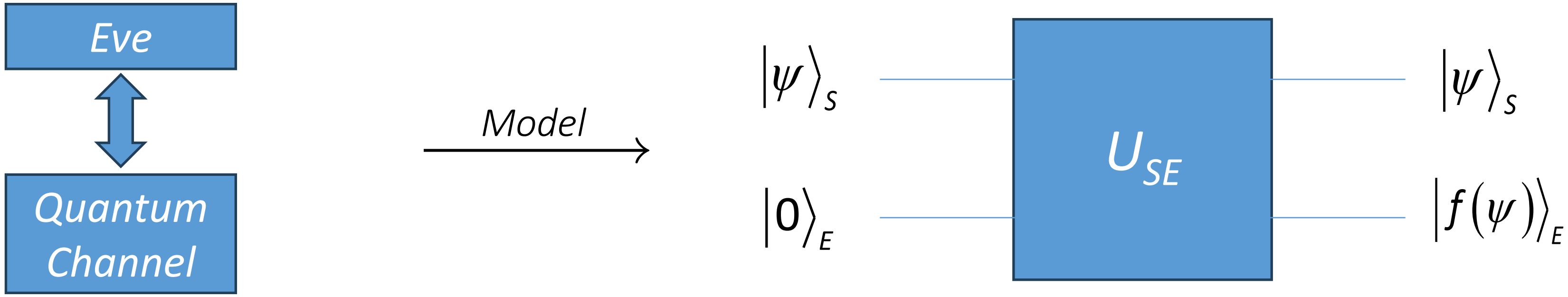
  Proposition: (**Information gain implies disturbance**) In any attempt to distinguish between two non-orthogonal quantum states, information gain is only possible at the expense of introducing disturbance to the signal

Proof

- Let $|\psi\rangle$ and $|\varphi\rangle$ be the non-orthogonal quantum states Eve is trying to obtain information about

Concept of QKD

- From the perspective of Quantum Operations, we may assume without loss of generality that the process Eve uses to obtain information is to unitarily interact the state $|\psi\rangle_S$ or $|\varphi\rangle_S$with an ancilla prepared in a standard state $|0\rangle_E$



Concept of QKD

- Assuming that this process does not disturb the states, in the two cases one obtains

$$|\psi\rangle_S \otimes |0\rangle_E \to U_{SE}\left(|\psi\rangle_S \otimes |0\rangle_E\right) \equiv |\psi\rangle_S \otimes |f(\psi)\rangle_E$$

$$|\varphi\rangle_S \otimes |0\rangle_E \to U_{SE}\left(|\varphi\rangle_S \otimes |0\rangle_E\right) \equiv |\varphi\rangle_S \otimes |f(\varphi)\rangle_E$$

- *Eve* would like $|f(\psi)\rangle_E$ and $|f(\varphi)\rangle_E$ to maintain some dependency on $|\psi\rangle_S$ and $|\varphi\rangle_S$ respectively
- If they are different, this allows her to acquire information about the identity of the state

Concept of QKD

- However, since inner products are preserved under unitary transformations, it must be that the following scalar product

$$\left({}_S\langle\psi|\otimes{}_E\langle 0|\right)\left(|\varphi\rangle_S\otimes|0\rangle_E\right)={}_S\langle\psi|\varphi\rangle_S\otimes{}_E\langle 0|0\rangle_E={}_S\langle\psi|\varphi\rangle_S$$

  should equate

$$\left({}_S\langle\psi|\otimes{}_E\langle f(\psi)|\right)\left(|\varphi\rangle_S\otimes|f(\varphi)\rangle_E\right)=\left({}_S\langle\psi|\varphi\rangle_S\otimes{}_E\langle f(\psi)|f(\varphi)\rangle_E\right)$$

  i.e.,

$${}_S\langle\psi|\varphi\rangle_S\otimes{}_E\langle f(\psi)|f(\varphi)\rangle_E={}_S\langle\psi|\varphi\rangle_S,\quad\forall|\psi\rangle_S,\ |\varphi\rangle_S$$

  which implies ${}_E\langle f(\psi)|f(\varphi)\rangle_E=1$

- Thus, distinguishing between $|\psi\rangle_S$ and $|\varphi\rangle_S$ must inevitably disturb at least one of these states

□

Varieties of QKD

- There are many different ways to make a QKD system
- These differ in the quantum physical effects being exploited, the key-establishment protocols being used, and the physical laws being relied upon for security.
- During the course, I will explain the following QKD protocols:
  - > Bennett and Brassard's "BB84" protocol based on two non-commuting observables [1]
  - > Bennett's "B92" protocol based on two non-orthogonal states [2]
  - > Ekert's "Entanglement-based" protocol [3]

Varieties of QKD

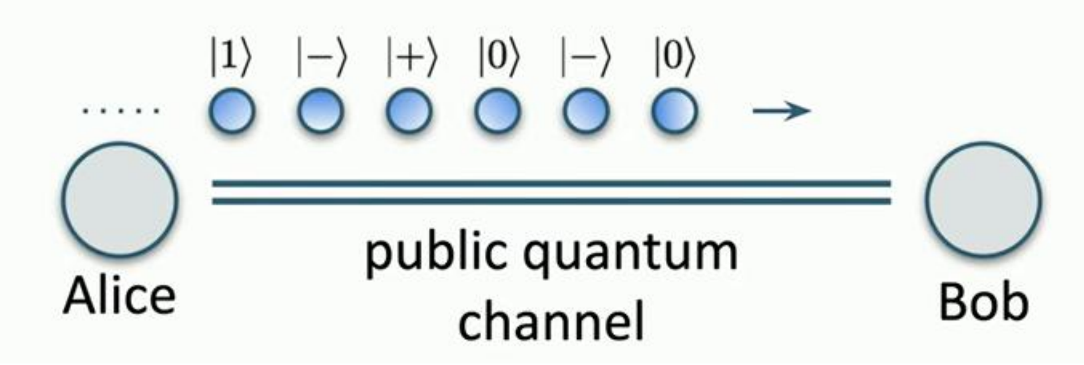
1. C. H. Bennett and G. Brassard, “Quantum Cryptography: Public Key Distribution and Coin Tossing,” in Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, December (1984) pp. 175–179. A scanned PDF of this paper is available at http://www.research.ibm.com/people/b/bennetc/bennettc198469790513.pdf.
2. C. H. Bennett, “Quantum Cryptography Using Any Two Nonorthogonal States,” Phys. Rev. Lett., Volume 68 (1992) pp. 3121–3124.
3. A. K. Ekert, “Quantum Cryptography Based on Bell’s Theorem,” Phys. Rev. Lett., Volume 67 (1991) pp. 661–663.

Concepts of QKD

- The earliest quantum key distribution (*QKD*) protocol is known as BB84 after its inventors, Charles Bennett and Gilles Brassard, and the year of the invention
- The BB84 protocol aims to establish a *secret key,* a random sequence of bit values 0 and 1, known only to the two parties, Alice and Bob, who may use this key to support a cryptographic task such as exchanging secret messages or detecting tampering

Concepts of QKD

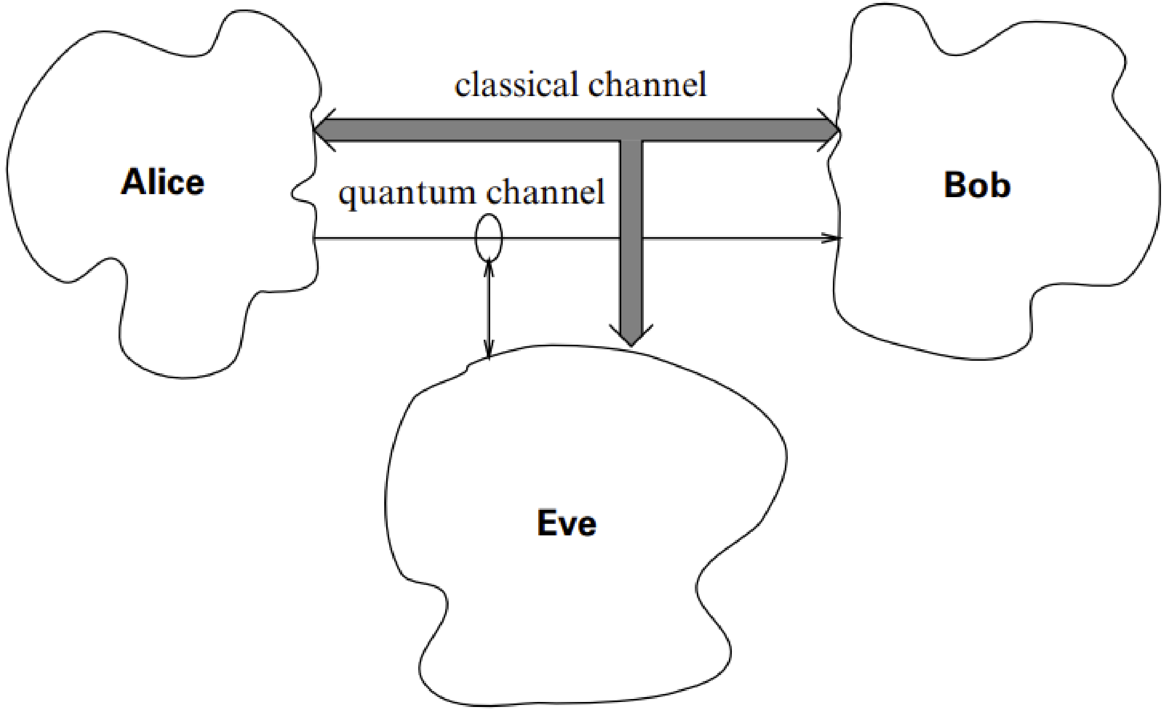
- Suppose **Alice** and **Bob** are connected by two *public channels*: an ordinary *bidirectional classical channel* and a *unidirectional quantum channel*
- The quantum channel allows Alice to send a sequence of single qubits to Bob; in our case, we suppose the qubits are encoded in the polarization states of individual photons


$|1\rangle$ $|-\rangle$ $|+\rangle$ $|0\rangle$ $|-\rangle$ $|0\rangle$
Alice
public quantum channel
Bob

- Both channels can be observed by an **eavesdropper Eve**

Concepts of QKD

- This situation is illustrated in the figure



Bennet and Brassard's BB84 QKD Protocol

BB84 QKD in the Absence of Eavesdropping

- The BB84 protocol employs two bases: *Z*-basis $\left\{|0\rangle,|1\rangle\right\}$ and *X*-basis $\left\{|+\rangle,|-\rangle\right\}$
- These bases are related in that

$$|+\rangle=\frac{1}{\sqrt{2}}\left(|0\rangle+|1\rangle\right),\quad |-\rangle=\frac{1}{\sqrt{2}}\left(|0\rangle-|1\rangle\right)\qquad \text{or}\qquad |0\rangle=\frac{1}{\sqrt{2}}\left(|+\rangle+|-\rangle\right),\quad |1\rangle=\frac{1}{\sqrt{2}}\left(|+\rangle-|-\rangle\right)$$

- Note that the four states are not all mutually orthogonal, and therefore no measurement can distinguish between (all of) them with certainty

BB84 QKD in the Absence of Eavesdropping

Stage 1: Qubit Preparation by Alice

Alice will start the process by initiating the *coding phase*

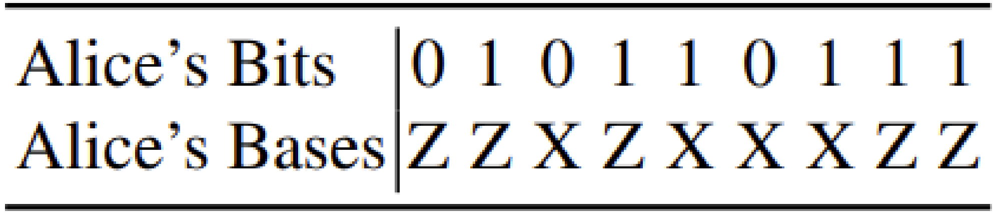
Random Bit Generation

- *Alice generates key material:* Alice uses a true random number generator to create a long string of *n random bits*
- These are the raw bits from which Alice and Bob must distill a matching private key
- Their job is to determine a subset of these bits *that they, and only they,* will know in common
- This privileged subset of bits becomes *their private cryptographic key*

BB84 QKD in the Absence of Eavesdropping

Random Basis Selection

- Alice, **for each bit** of the **bit string generated**, *randomly* chooses the basis *Z*, i.e. $\{|+\rangle,|-\rangle\}$ or the basis *X*, i.e. $\{|0\rangle,|1\rangle\}$
- For example:



Alice's Bits	0	1	0	1	1	0	1	1	1
Alice's Bases	Z	Z	X	Z	X	X	X	Z	Z

- This basis is called *qubit preparation basis*

BB84 QKD in the Absence of Eavesdropping

Qubit Encoding By Alice

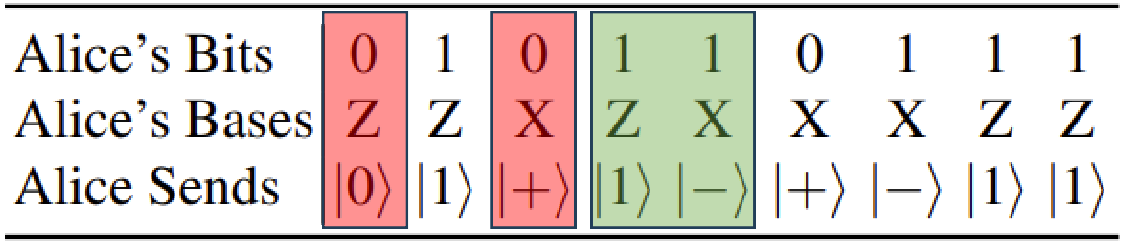
Alice prepares a sequence of qubits according to the chosen bases and bit values:

- If the bit is 0 and the basis is Z, she prepares $|0\rangle$
- If the bit is 1 and the basis is Z, she prepares $|1\rangle$
- If the bit is 0 and the basis is X, she prepares $|+\rangle$
- If the bit is 1 and the basis is X, she prepares $|-\rangle$

Alice Basis	Bit	Encoding
Z	0	$\|0\rangle$
	1	$\|1\rangle$
X	0	$\|+\rangle$
	1	$\|-\rangle$

BB84 Encoding Example

Alice Basis	Bit	Encoding
Z	0	$\vert 0\rangle$
	1	$\vert 1\rangle$
X	0	$\vert +\rangle$
	1	$\vert -\rangle$



Alice's Bits	0	1	0	1	1	0	1	1	1
Alice's Bases	Z	Z	X	Z	X	X	X	Z	Z
Alice Sends	$\vert 0\rangle$	$\vert 1\rangle$	$\vert +\rangle$	$\vert 1\rangle$	$\vert -\rangle$	$\vert +\rangle$	$\vert -\rangle$	$\vert 1\rangle$	$\vert 1\rangle$

BB84 QKD in the Absence of Eavesdropping

Stage 2: Quantum Communication

- Alice sends the prepared qubits to Bob through a public quantum channel (e.g., optical fiber) by encoding his bits in polarized photons
- Bob receive the prepared qubits sent by Alice
- Let's consider what Bob knows at this time
- Alice has not shared with Bob on which basis (*X*,*Z*) has been coded the bits of the random sequence
- All Bob knows is that he is receiving qubits that could be any of the four possible states $|0\rangle$, $|1\rangle$, $|+\rangle$ or $|-\rangle$

BB84 QKD in the Absence of Eavesdropping

- Then the **decoding phase** follows, performed by Bob
- During this phase, **Bob uses the same mapping as Alice to couple qubits to bits**, ensuring consistency when encoding and decoding information in the BB84 protocol
- This shared understanding is fundamental to the protocol, as it allows them to interpret the states and agree on a key after basis reconciliation

Alice Basis	Bit	Encoding
Z	0	$\|0\rangle$
	1	$\|1\rangle$
X	0	$\|+\rangle$
	1	$\|-\rangle$

BB84 QKD in the Absence of Eavesdropping

Two operations are involved in this phase

- *Random Basis Selection*: **For each received qubit**, Bob randomly chooses a basis *(qubit measurement basis)* (Z or X) to measure the qubit
- *Measurement*: Bob measures each qubit in the chosen basis, obtaining a sequence of measurement results (bits)

Alice Basis	Bit	Encoding
Z	0	$\|0\rangle$
	1	$\|1\rangle$
X	0	$\|+\rangle$
	1	$\|-\rangle$

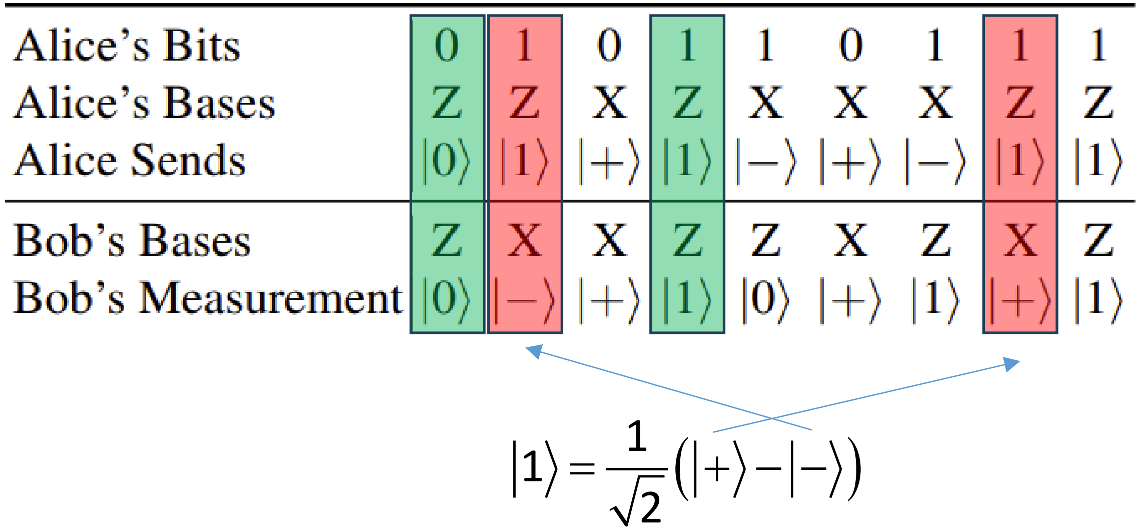
BB84 QKD in the Absence of Eavesdropping

- If the basis he picked was the same as Alice's, then he will get the same result as Alice
- If he picked the opposite basis, however, then he will get each possible result with probability 1/2

Alice Basis	*Bit*	*Encoding*	*Bob Basis*	*Bob Results*	*Decoding*	*Keep or Discard*
Z	0	$\|0\rangle$	Z	$\|0\rangle$, Pr $=1$	0	OK
			X	$\|+\rangle$, Pr $=1/2$	0	✗
			X	$\|-\rangle$, Pr $=1/2$	1	✗
Z	1	$\|1\rangle$	Z	$\|1\rangle$, Pr $=1$	1	OK
			X	$\|+\rangle$, Pr $=1/2$	0	✗
			X	$\|-\rangle$, Pr $=1/2$	1	✗
X	0	$\|+\rangle$	Z	$\|0\rangle$, Pr $=1/2$	0	✗
			Z	$\|1\rangle$, Pr $=1/2$	1	✗
			X	$\|+\rangle$, Pr $=1$	0	OK
X	1	$\|-\rangle$	Z	$\|0\rangle$, Pr $=1/2$	0	✗
			Z	$\|1\rangle$, Pr $=1/2$	1	✗
			X	$\|-\rangle$, Pr $=1$	1	OK

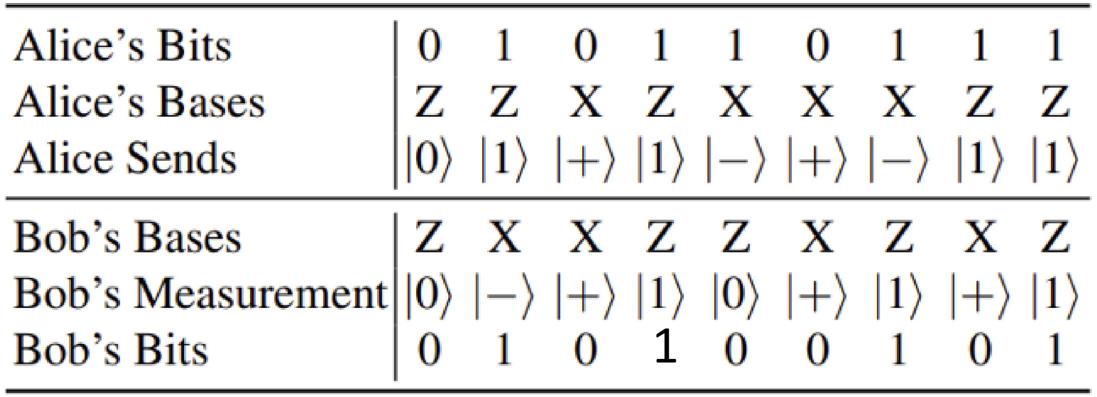
BB84 Decoding Example

- For example, if Alice sends Bob $\vert 1\rangle$ and he measures on the *Z*-basis, he is certain to get $\vert 1\rangle$ (see right green column)
- But if he measures on the *X*-basis, he gets $\vert +\rangle$ with probability 1/2 or $\vert -\rangle$ with probability 1/2 (see red columns)



Alice's Bits	0	1	0	1	1	0	1	1	1
Alice's Bases	Z	Z	X	Z	X	X	X	Z	Z
Alice Sends	$\vert 0\rangle$	$\vert 1\rangle$	$\vert +\rangle$	$\vert 1\rangle$	$\vert -\rangle$	$\vert +\rangle$	$\vert -\rangle$	$\vert 1\rangle$	$\vert 1\rangle$
Bob's Bases	Z	X	X	Z	Z	X	Z	X	Z
Bob's Measurement	$\vert 0\rangle$	$\vert -\rangle$	$\vert +\rangle$	$\vert 1\rangle$	$\vert 0\rangle$	$\vert +\rangle$	$\vert 1\rangle$	$\vert +\rangle$	$\vert 1\rangle$

$$\vert 1\rangle = \frac{1}{\sqrt{2}}\left(\vert +\rangle - \vert -\rangle\right)$$



Alice's Bits	0	1	0	1	1	0	1	1	1
Alice's Bases	Z	Z	X	Z	X	X	X	Z	Z
Alice Sends	$\vert 0\rangle$	$\vert 1\rangle$	$\vert +\rangle$	$\vert 1\rangle$	$\vert -\rangle$	$\vert +\rangle$	$\vert -\rangle$	$\vert 1\rangle$	$\vert 1\rangle$
Bob's Bases	Z	X	X	Z	Z	X	Z	X	Z
Bob's Measurement	$\vert 0\rangle$	$\vert -\rangle$	$\vert +\rangle$	$\vert 1\rangle$	$\vert 0\rangle$	$\vert +\rangle$	$\vert 1\rangle$	$\vert +\rangle$	$\vert 1\rangle$
Bob's Bits	0	1	0	1	0	0	1	0	1

BB84 QKD in the Absence of Eavesdropping

- The table summarizes the initial 3 stages of the BB84 protocol

Alice Basis	*Bit*	*Encoding*	*Bob Basis*	*Bob Results*	*Decoding*	*Keep or Discard*
Z	0	$\|0\rangle$	Z	$\|0\rangle$, $\mathrm{Pr}=1$	0	OK
			X	$\|+\rangle$, $\mathrm{Pr}=1/2$	0	✗
			X	$\|-\rangle$, $\mathrm{Pr}=1/2$	1	✗
Z	1	$\|1\rangle$	Z	$\|1\rangle$, $\mathrm{Pr}=1$	1	OK
			X	$\|+\rangle$, $\mathrm{Pr}=1/2$	0	✗
			X	$\|-\rangle$, $\mathrm{Pr}=1/2$	1	✗
X	0	$\|+\rangle$	Z	$\|0\rangle$, $\mathrm{Pr}=1/2$	0	✗
			Z	$\|1\rangle$, $\mathrm{Pr}=1/2$	1	✗
			X	$\|+\rangle$, $\mathrm{Pr}=1$	0	OK
X	1	$\|-\rangle$	Z	$\|0\rangle$, $\mathrm{Pr}=1/2$	0	✗
			Z	$\|1\rangle$, $\mathrm{Pr}=1/2$	1	✗
			X	$\|-\rangle$, $\mathrm{Pr}=1$	1	OK

BB84 QKD in the Absence of Eavesdropping

Then, over the classical channel, Alice and Bob check that Bob has received a photon for every one Alice has sent, and only then do Alice and Bob proceed to the next stage

Stage 3: Classical Communication

- Bob **discloses the basis** he used for each qubit measurement: to determine which bits are correct after Bob has completed all his measurements, he tells Alice (via the public classical channel) **the basis** in which he measured each incoming qubit, **but not the value he observed** for the measurement
- Alice then tells Bob (via the classical channel) about those occasions on which they used the same basis for Alice's encoding and Bob's measurement

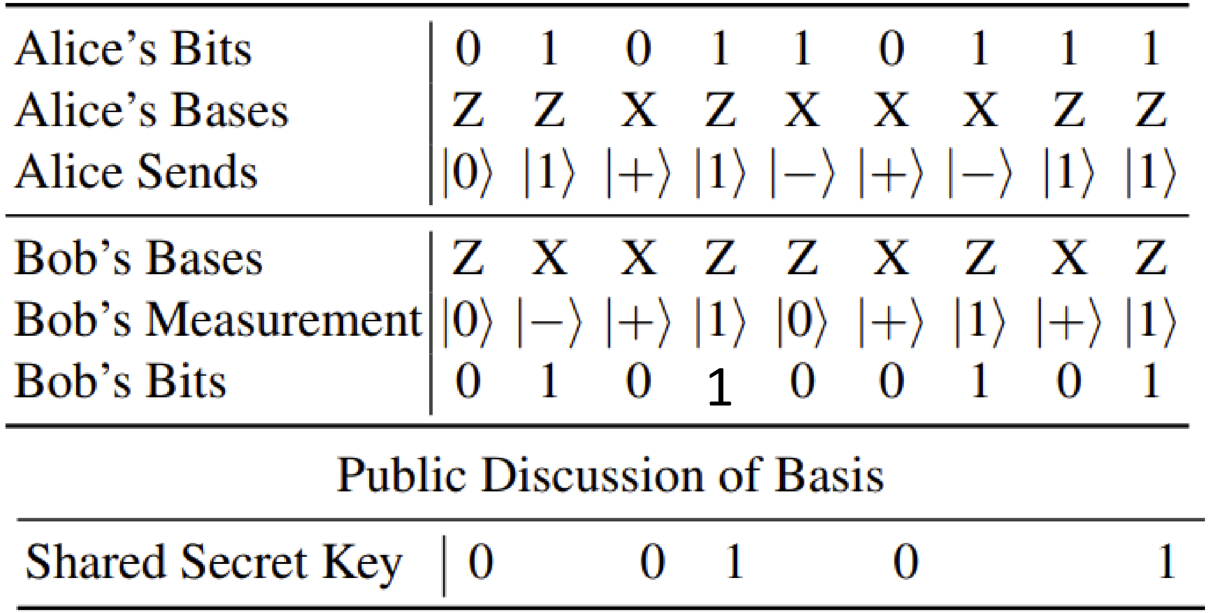
BB84 QKD in the Absence of Eavesdropping

Stage 4: Classical Post-Processing

- The above exchange of classical information between Alice and Bob enables Bob to identify the subset of bits he measured that should match the bits Alice sent
- Disclosing the basis Alice and Bob used **for each qubit measurement** does not make the protocol insecure, provided the communication occurs after the qubits are measured by Bob.

BB84 QKD in the Absence of Eavesdropping

- Alice and Bob can now discard all those cases in which they used different bases
- An average of 50 percent of all bits transmitted remain
- In the *absence* of any *noise, imperfections, and eavesdropping,* Alice and Bob should come to possess matching sequences of randomly generated bits which can serve as a fresh supply of keys

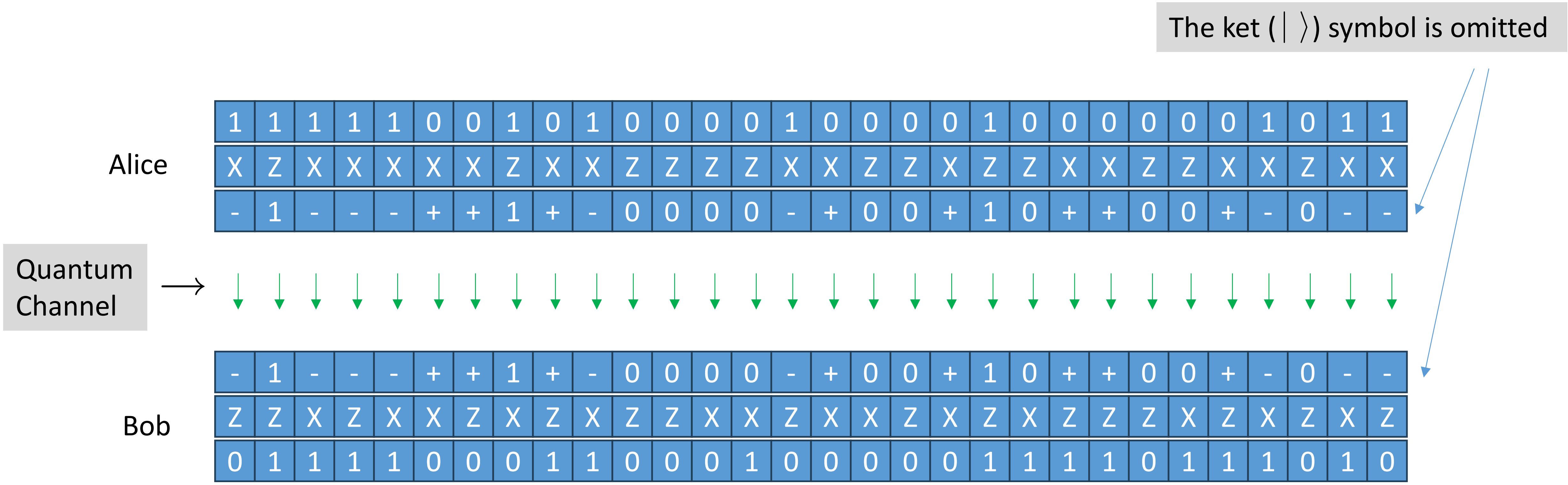


Alice's Bits	0	1	0	1	1	0	1	1	1
Alice's Bases	Z	Z	X	Z	X	X	X	Z	Z
Alice Sends	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|1\rangle$	$\|-\rangle$	$\|+\rangle$	$\|-\rangle$	$\|1\rangle$	$\|1\rangle$
Bob's Bases	Z	X	X	Z	Z	X	Z	X	Z
Bob's Measurement	$\|0\rangle$	$\|-\rangle$	$\|+\rangle$	$\|1\rangle$	$\|0\rangle$	$\|+\rangle$	$\|1\rangle$	$\|+\rangle$	$\|1\rangle$
Bob's Bits	0	1	0	1	0	0	1	0	1

Public Discussion of Basis

Shared Secret Key	0		0	1		0			1

BB84 QKD in the Absence of Eavesdropping



The ket (| 〉) symbol is omitted

Alice

1	1	1	1	1	0	0	1	0	1	0	0	0	0	1	0	0	0	0	1	0	0	0	0	0	0	1	0	1	1
X	Z	X	X	X	X	X	Z	X	X	Z	Z	Z	Z	X	X	Z	Z	X	Z	Z	X	X	Z	Z	X	X	Z	X	X
-	1	-	-	-	+	+	1	+	-	0	0	0	0	-	+	0	0	+	1	0	+	+	0	0	+	-	0	-	-

Quantum Channel →

Bob

-	1	-	-	-	+	+	1	+	-	0	0	0	0	-	+	0	0	+	1	0	+	+	0	0	+	-	0	-	-
Z	Z	X	Z	X	X	Z	X	Z	X	Z	Z	X	X	Z	X	X	Z	X	Z	X	Z	Z	Z	X	Z	X	Z	X	Z
0	1	1	1	1	0	0	0	1	1	0	0	0	1	0	0	0	0	0	1	1	1	1	0	1	1	1	0	1	0

BB84 QKD in the Absence of Eavesdropping

Alice	1	1	1	1	1	0	0	1	0	1	0	0	0	0	1	0	0	0	0	1	0	0	0	0	0	0	1	0	1	1
	X	Z	X	X	X	X	X	Z	X	X	Z	Z	Z	Z	X	X	Z	Z	X	Z	Z	X	X	Z	Z	X	X	Z	X	X
	-	1	-	-	-	+	+	1	+	-	0	0	0	0	-	+	0	0	+	1	0	+	+	0	0	+	-	0	-	-

Quantum Channel →

Bob	-	1	-	-	-	+	+	1	+	-	0	0	0	0	-	+	0	0	+	1	0	+	+	0	0	+	-	0	-	-
	Z	Z	X	Z	X	X	Z	X	Z	X	Z	Z	X	X	Z	X	X	Z	X	Z	X	Z	Z	Z	X	Z	X	Z	X	Z
	0	1	1	1	1	0	0	0	1	1	0	0	0	1	0	0	0	0	0	1	1	1	1	0	1	1	1	0	1	0

Alice		1	1		1	0				1	0	0				0		0	0	1				0			1	0	1	
		Z	X		X	X				X	Z	Z				X		Z	X	Z				Z			X	Z	X	
Bob		Z	X		X	X				X	Z	Z				X		Z	X	Z				Z			X	Z	X	
		1	1		1	0				1	0	0				0		0	0	1				0			1	0	1	

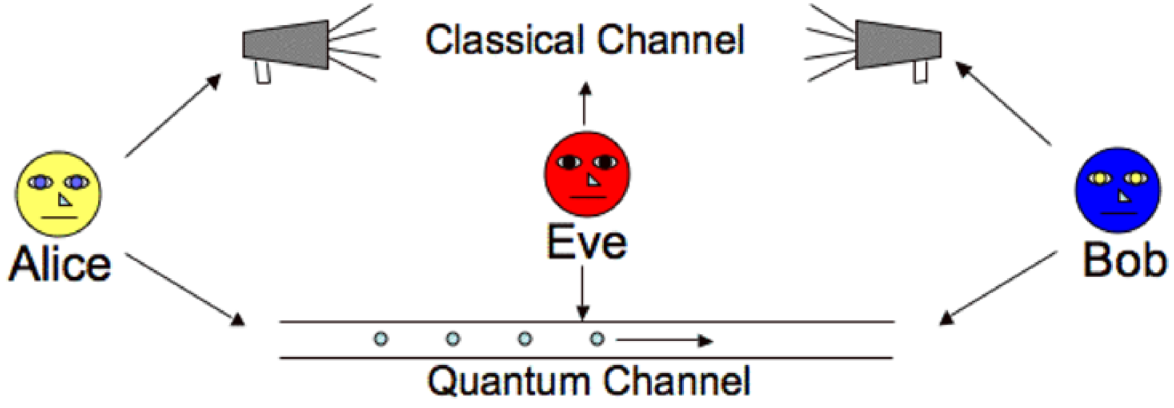
Quantum Key →

1	1	1	0	1	0	0	0	0	0	1	0	1	0	1

BB84 QKD in the Presence of Eavesdropping

Eavesdropper Detection (Intercept and Resend Attack)

- So far, we have only considered the **ideal scenario** where there was no eavesdropper
- Now let’s say that somebody is listening to both the *public classical channel* and the *public quantum channel*

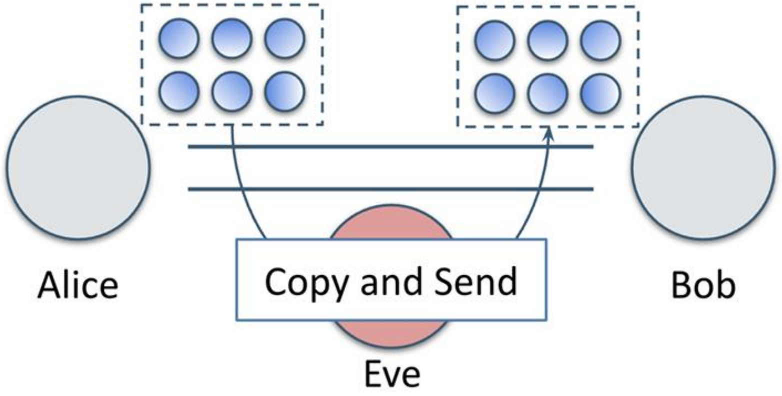


BB84 QKD in the Presence of Eavesdropping

- Next, we are going to consider the effect of an eavesdropper, whom we are going to name **Eve**, and see what effect she has on the protocol and how the protocol can discover the presence of such an eavesdropper

BB84 QKD in the Presence of Eavesdropping

- What can Eve do?
- Assume, for contradiction, that Eve can intercept the qubits that Alice is sending over the public quantum channel, copy them and then resend them to Bob, as in Figure



- If she could do that, she could hold her copy of the qubits, wait until Alice and Bob announce the *qubit preparation* and *measurement bases* respectively, then measure her copies

BB84 QKD in the Presence of Eavesdropping

- Doing that, she would discover which qubits are used for the generation of the secret key, and she would also know in which basis to measure them in order to generate a key that is perfectly correlated with the one built by Alice and Bob
- Luckily, it is **impossible** for Eve to do that due to the **no-cloning theorem**
- If Eve cannot copy the qubits and hold them, then in order to gain any access to the information that Alice is trying to share with Bob, she has to measure the qubits and forward them to Bob

BB84 QKD in the Presence of Eavesdropping

- What can happen in this case?
- Remember, the preparation basis is still kept secret by Alice.
- That basis has not yet been communicated over a public classical channel to Bob
- Without access to this information, Eve has to pick either the *X* or *Z* basis at random for her measurement
- Eve therefore runs the risk of **disturbing and altering** the state of the qubits that she intercepted from Alice

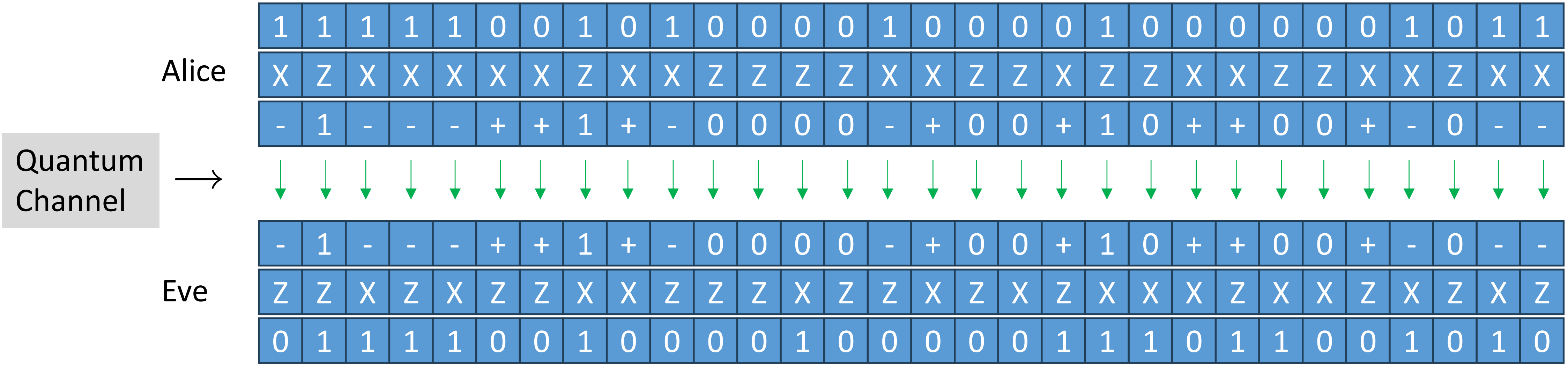
BB84 QKD in the Presence of Eavesdropping

- Thus, let’s consider in detail what would have happened if there had been an eavesdropper, “Eve”, present
- Alice and Bob do not know that eavesdropping is taking place, so the first step proceeds as before with Alice encoding her bits in polarized photons, as in Figure

1	1	1	1	1	0	0	1	0	1	0	0	0	0	1	0	0	0	0	1	0	0	0	0	0	0	1	0	1	1
X	Z	X	X	X	X	X	Z	X	X	Z	Z	Z	Z	X	X	Z	Z	X	Z	Z	X	X	Z	Z	X	X	Z	X	X
-	1	-	-	-	+	+	1	+	-	0	0	0	0	-	+	0	0	+	1	0	+	+	0	0	+	-	0	-	-

BB84 QKD in the Presence of Eavesdropping

- Eve, who is intercepting Alice's photons, goes through the operations that Bob would have performed: she **intercepts** the photons, i.e., qubit (first row), picks a **basis** (second row), and decodes the polarized photons as bits, (third row)



Alice	1	1	1	1	1	0	0	1	0	1	0	0	0	0	1	0	0	0	0	1	0	0	0	0	0	0	1	0	1	1
	X	Z	X	X	X	X	X	Z	X	X	Z	Z	Z	Z	X	X	Z	Z	X	Z	Z	X	X	Z	Z	X	X	Z	X	X
	-	1	-	-	-	+	+	1	+	-	0	0	0	0	-	+	0	0	+	1	0	+	+	0	0	+	-	0	-	-
Quantum Channel →	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
Eve	-	1	-	-	-	+	+	1	+	-	0	0	0	0	-	+	0	0	+	1	0	+	+	0	0	+	-	0	-	-
	Z	Z	X	Z	X	Z	Z	X	X	Z	Z	Z	X	Z	Z	X	Z	X	Z	X	X	X	Z	X	X	Z	X	Z	X	Z
	0	1	1	1	1	0	0	1	0	0	0	0	1	0	0	0	0	0	1	1	1	0	1	1	0	0	1	0	1	0

BB84 QKD in the Presence of Eavesdropping

- However, here's the rub: the qubit has now collapsed to one of the two elements of Eve's basis

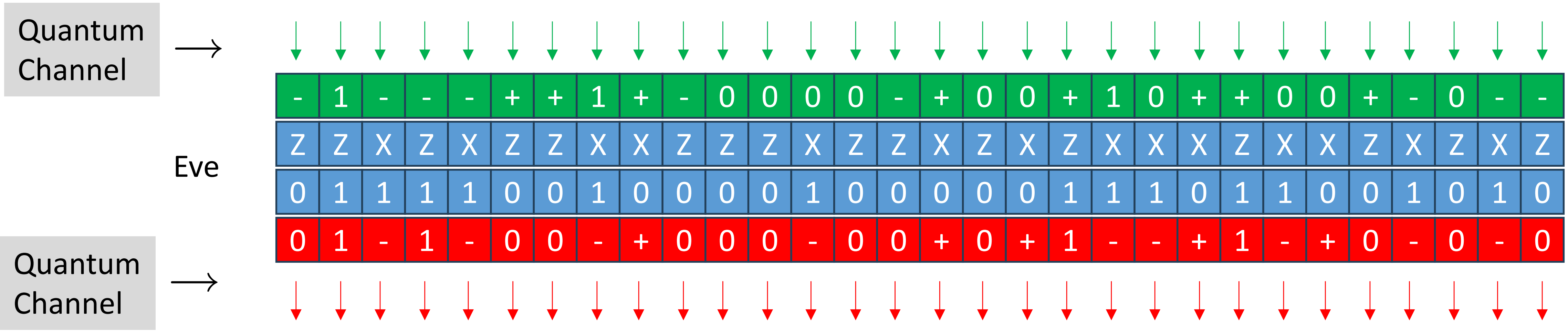
-	1	-	-	-	+	+	1	+	-	0	0	0	0	-	+	0	0	+	1	0	+	+	0	0	+	-	0	-	-
Z	Z	X	Z	X	Z	Z	X	X	Z	Z	Z	X	Z	Z	X	Z	X	Z	X	X	X	Z	X	X	Z	X	Z	X	Z
0	1	1	1	1	0	0	1	0	0	0	0	1	0	0	0	0	0	1	1	1	0	1	1	0	0	1	0	1	0

- Because of the no-cloning theorem, Eve does not have the luxury of making a copy of the original qubit and then sending it on (after her probe) to Bob, so she just sends the qubit **after her observation**

BB84 QKD in the Presence of Eavesdropping

- To cover her tracks Eve then re-transmits the photons she measured to Bob
- Eve is free to do a complete recoding of her measured bits into photons in whatever basis she chooses
- But the simplest situation has Eve using the same basis that she used during her decoding step

qbits received from Alice



-	1	-	-	-	+	+	1	+	-	0	0	0	0	-	+	0	0	+	1	0	+	+	0	0	+	-	0	-	-
Z	Z	X	Z	X	Z	Z	X	X	Z	Z	Z	X	Z	Z	X	Z	X	Z	X	X	X	Z	X	X	Z	X	Z	X	Z
0	1	1	1	1	0	0	1	0	0	0	0	1	0	0	0	0	0	1	1	1	0	1	1	0	0	1	0	1	0
0	1	-	1	-	0	0	-	+	0	0	0	-	0	0	+	0	+	1	-	-	+	1	-	+	0	-	0	-	0

qbits sent to Bob

BB84 QKD in the Presence of Eavesdropping

- At this moment Bob is unaware of Eve’s presence, so he proceeds to decode the photons he thinks are coming from Alice, but which are coming from Eve

0	1	-	1	-	0	0	-	+	0	0	0	-	0	0	+	0	+	1	-	-	+	1	-	+	1	-	0	-	0
Z	Z	X	Z	X	X	Z	X	Z	X	Z	Z	X	X	Z	X	X	Z	X	Z	X	Z	Z	Z	X	Z	X	Z	X	Z
0	1	1	1	1	1	0	1	1	1	0	0	1	0	0	0	0	0	1	1	1	1	1	0	0	0	1	0	1	0

- Bob intercepts the photons (first row), picks up a basis (second row), and decodes the photons as a sequence of ***n*** bits, i.e., Bob implements the Stage 2 described earlier

BB84 QKD in the Presence of Eavesdropping

- At this point, Alice and Bob proceed with Stage 3 and Stage 4 of the previously described algorithm which assumes that Eve (the eavesdropper) is not present

Alice basis	X	Z	X	X	X	X	X	Z	X	X	Z	Z	Z	Z	X	X	Z	Z	X	Z	Z	X	X	Z	Z	X	X	Z	X	X
Bob basis	Z	Z	X	Z	X	X	Z	X	Z	X	Z	Z	X	X	Z	X	X	Z	X	Z	X	Z	Z	Z	X	Z	X	Z	X	Z
Bob bit string	0	1	1	1	1	1	0	1	1	1	0	0	1	0	0	0	0	0	1	1	1	1	1	0	0	0	1	0	1	0
Alice bit string	1	1	1	1	1	0	0	1	0	1	0	0	0	0	1	0	0	0	0	1	0	0	0	0	0	0	1	0	1	1

Alice basis	X	Z	X	X	X	X	X	Z	X	X	Z	Z	Z	Z	X	X	Z	Z	X	Z	Z	X	X	Z	Z	X	X	Z	X	X
Bob basis	Z	Z	X	Z	X	X	Z	X	Z	X	Z	Z	X	X	Z	X	X	Z	X	Z	X	Z	Z	Z	X	Z	X	Z	X	Z
Bob bit string	0	1	1	1	1	1	0	1	1	1	0	0	1	0	0	0	0	0	1	1	1	1	1	0	0	0	1	0	1	0
Alice bit string	1	1	1	1	1	0	0	1	0	1	0	0	0	0	1	0	0	0	0	1	0	0	0	0	0	0	1	0	1	1

BB84 QKD in the Presence of Eavesdropping

- As we saw earlier, if Eve was not listening to the quantum channel, this subsequence should be identical
- On average, this subsequence is of length $n/2$
- But what if Eve was eavesdropping?
- Alice and Bob would also like to engage in some intrusion detection
- They want to know if Eve (or anyone else) was listening in
- They do this *by comparing some of the bits of the subsequence*

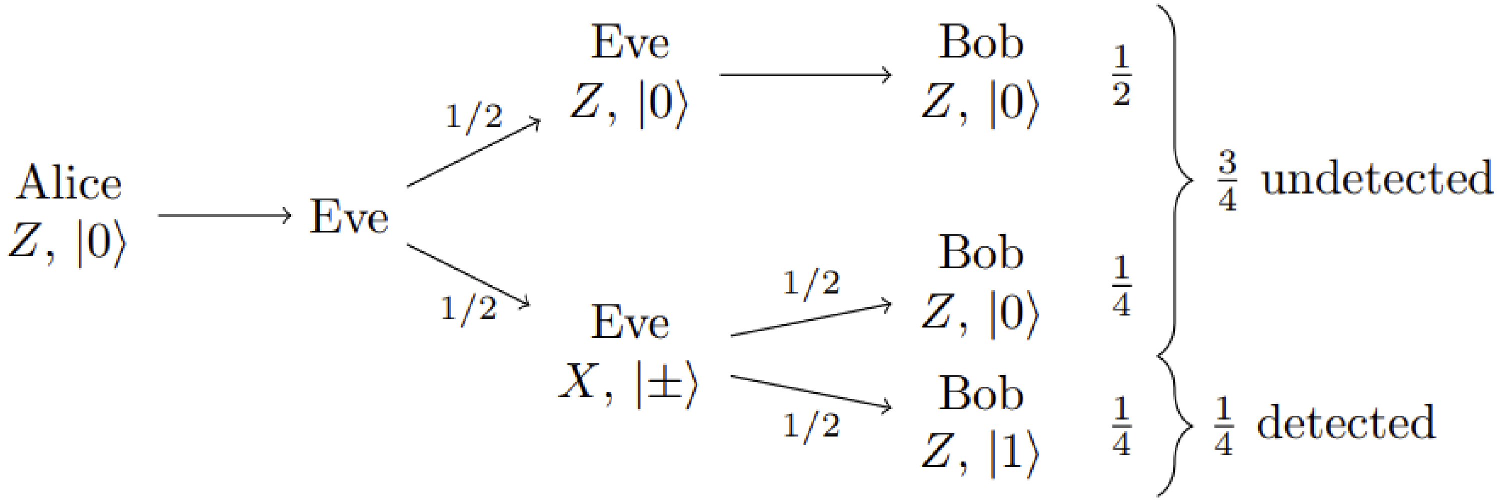
BB84 QKD in the Presence of Eavesdropping

Error Checking and Key Reconciliation

- To ensure Eve did not measure the qubits along the way, Alice and Bob can reveal a **fraction** of their shared secret key and make sure they agree
- If Alice and Bob reveal (for example) ***k* bits** of their shared secret key, what is the probability they will catch Eve if Eve is measuring every qubit along the way?
- To answer this, let us start by *revealing one bit*
- Say Alice and Bob are revealing a bit where they both used the *Z*-basis and say Alice sent qubit in the state $|0\rangle$

BB84 QKD in the Presence of Eavesdropping

- Then, Alice will reveal that her bit is 0, while Bob could reveal that his bit is 0 or 1, and we determine the probabilities of these outcomes using the following diagram:



- On the left side of the diagram, Alice is using the *Z*-basis, and she sends a qubit in the $|0\rangle$ state

BB84 QKD in the Presence of Eavesdropping

- In the middle of the diagram, Eve intercepted the qubit and measured it in either the *Z*-basis or the *X*-basis, each with probability 1/2
- If Eve measured on the *Z*-basis, she got $|0\rangle$, and then forwarded the qubit to Bob
- Bob measured the qubit in the *Z*-basis, so he also got $|0\rangle$
- This is the top row of the above diagram
- In this scenario, which occurs with probability 1/2, Alice and Bob both reveal that they got the bit 0, and Eve's eavesdropping was undetected

BB84 QKD in the Presence of Eavesdropping

- Now, if Eve measured on the *X*-basis instead, then she collapsed the state to $|+\rangle$ or $|-\rangle$ and forwarded it to Bob
- In the above figure, this is the bottom row
- Bob then measured the qubit in the *Z*-basis, getting $|0\rangle$ with probability 1/2 or $|1\rangle$ with probability 1/2
- Overall, each of these outcomes occurs with probability 1/4
- If Bob got $|0\rangle$, Eve is undetected, but if he got $|1\rangle$, Alice and Bob will realize there was an eavesdropper when they reveal their results

BB84 QKD in the Presence of Eavesdropping

- Overall, Eve has a probability of **3/4 of being undetected** and a probability of **1/4 of being detected**, as indicated by the curly brace in the above figure, when Alice and Bob reveal this bit of their shared secret key
- In other words, there is a probability of 3/4 that Alice and Bob both have 0 as their bits, and probability 1/4 that Alice has 0 and Bob has 1

BB84 QKD in the Presence of Eavesdropping

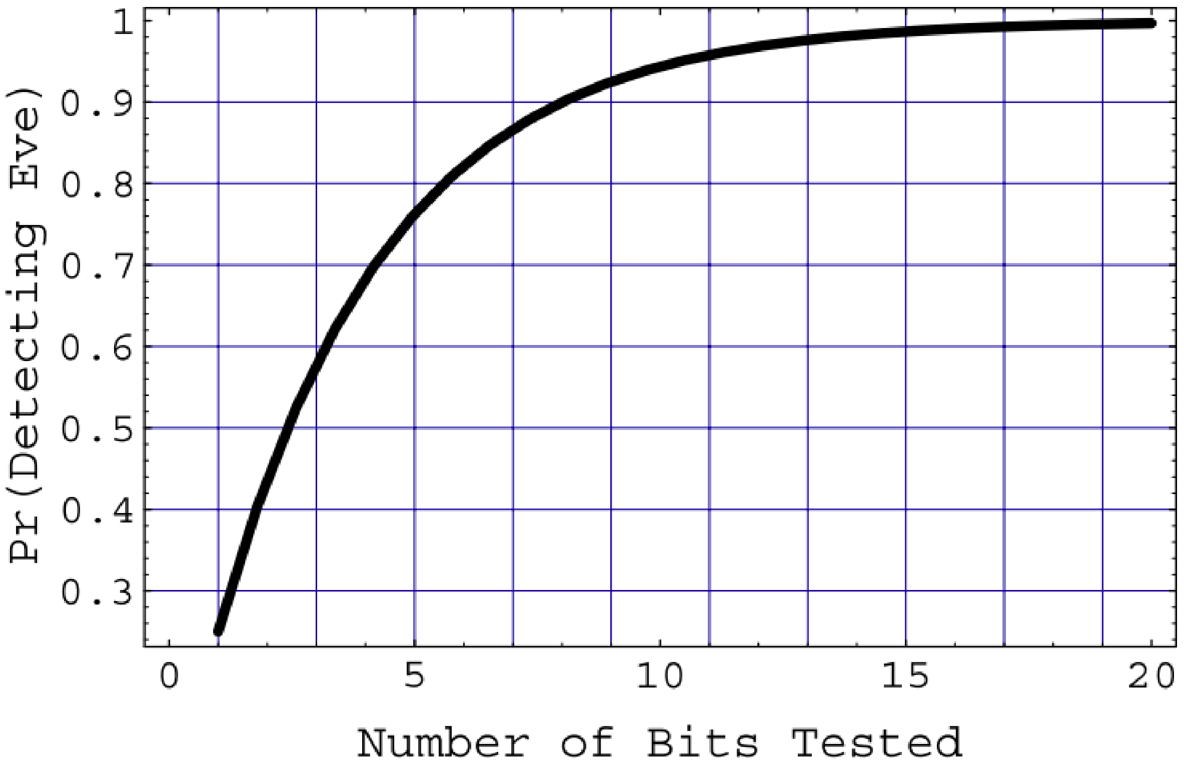
- If Alice and Bob share *k* bits of their shared secret key, the probability that Eve is undetected for all *k* bits is $(3/4)^k$
- Then, the probability that Eve is detected is one minus this, or

$$\text{Probability}\{\text{Alice and Bob detect Eve}\} = 1 - \left(\frac{3}{4}\right)^k$$

- Thus, if Alice and Bob share 50 bits of their shared secret key, the probability that they detect Eve is $1-(3/4)^{50} = 0.99999943$, which is very close to certainty

BB84 QKD in the Presence of Eavesdropping

- The curve on the side reports the probability of detecting eavesdropping as a function of the number of bits tested by Alice and Bob
- For a bit to be testable, Alice and Bob must have used the same basis to encode and decode that bit, respectively



BB84 QKD in the Presence of Eavesdropping

- Noise can also change the state of the qubits transmitted by Alice
- Qubits affected by noise can flip to their orthogonal state, they can be rotated to a new basis, or more generally, they can become a mixture of pure states
- This means that even in the absence of malicious Eve, there is a substantial probability that some of the qubits reserved for eavesdropper detection will be disturbed and projected onto the wrong state by Bob
- This will lead to Alice and Bob to the erroneous conclusion that someone is trying to eavesdrop on their communication

BB84 QKD in the Presence of Eavesdropping

- In order to avoid this scenario, Alice and Bob must be ready to accept some deviation from the ideal protocol and make peace with the fact that some level disturbance will be always present
- If the channel is nearly ideal with low levels of noise, the expected amount disturbance is also low
- Noisy channels will result in more disturbance
- The question of what amount of disturbance Alice and Bob are willing to tolerate is crucial

BB84 QKD in the Presence of Eavesdropping

- If they set the acceptable level too high, malicious Eve will have a good chance to go undetected and gain some information about the secret key
- If the acceptable level is set too low, Alice and Bob will have a high chance of unnecessarily rejecting the secret key, leading to a waste of network resources
- *Picking the middle ground is a challenging task that goes beyond the scope of this book*

BB84 QKD in the Presence of Eavesdropping

Besides the **intercept and resend attacks**, there are many other attacks that exist, such as:

- Man-in-the-middle Attack
- Photon number splitting attack
- Denial of service
- Trojan-horse attacks

BB84 QKD in the Presence of Eavesdropping

Security Proofs

- BB84 has been proven secure against any attacks allowed by quantum mechanics, both for sending information using an ideal photon source which only ever emits a single photon at a time, and also using practical photon sources which sometimes emit multiphoton pulses
- These proofs are **unconditionally secure** in the sense that no conditions are imposed on the resources available to the eavesdropper

BB84 QKD in the Presence of Eavesdropping

However, the following conditions must be met:

1. Eve cannot physically access Alice and Bob's **encoding and decoding devices**
2. The random number generators used by Alice and Bob must be trusted and truly random (for example a **quantum random number generator**)
3. The classical communication channel must be authenticated using an **unconditionally secure authentication scheme**
4. The message must be encrypted using **one-time pad** like scheme

Another topic of paramount importance is the so-called **quantum hacking**, which however, is outside the scope of this course

Bennet's 2-State B92 QKD Protocol

B92 QKD Protocol

- In 1992 Charles Bennett showed that one did not need to use four states (as in BB84) to support a QKD protocol, but that two non-orthogonal states were sufficient
- This led to a QKD scheme known as the B92 *protocol* which is similar to BB84 except that two states are used instead of four
- Let's work out the protocol with the following example

$$\{|0\rangle,|+\rangle\} \equiv \left\{|0\rangle,\frac{1}{\sqrt{2}}\left(|0\rangle+|1\rangle\right)\right\}$$

- Thus, only two non-orthogonal states are used

B92 QKD Protocol

Step 1

- Alice uses a true random number generator to create a long string of *n* random bits
- These are the raw bits from which Alice and Bob must distill a matching private key
- Alice and Bob’s job is to determine a subset of these bits that they, and only they, will know in common
- This privileged subset of bits becomes their private cryptographic key

B92 QKD Protocol

Step 2

- By using the quantum channel, Alice sends each of her *n* random bits to Bob, one after another, encoded in the *polarization state of single photons* (i.e., qubits)
- **Alice** and **Bob agree** on the following encoding strategy:

  > if Alice wants to send Bob a **0** she transmits $|0\rangle$, and

  > if Alice wants to send a **1** she transmits

$$|+\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$$

B92 QKD Protocol

Here is an example

Step 1: Alice Sends *n* Random Bits												
Bit Number	1	2	3	4	5	6	7	8	9	10	11	12
Alice’s Random Bits	0	0	1	0	1	0	1	0	1	1	1	0
Alice’s Qubits	$\|0\rangle$	$\|0\rangle$	$\|+\rangle$	$\|0\rangle$	$\|+\rangle$	$\|0\rangle$	$\|+\rangle$	$\|0\rangle$	$\|+\rangle$	$\|+\rangle$	$\|+\rangle$	$\|0\rangle$
Quantum Channel	⇩	⇩	⇩	⇩	⇩	⇩	⇩	⇩	⇩	⇩	⇩	⇩

B92 QKD Protocol

Step 3

- For each of the *n* qubits, Bob measures the received qubits in either the *Z* basis or the *X* basis
- He flips a coin to determine which basis to use
- Several possible scenarios can occur

B92 QKD Protocol

Bob Receives	*Bob Basis*	*Bob Results*	*Decoding*	*Keep or Discard*
$\vert 0\rangle$	Z	$\vert 0\rangle$, $\Pr = 1$	?	✗
	X	$\vert +\rangle$, $\Pr = 1/2$	?	✗
	X	$\vert -\rangle$, $\Pr = 1/2$	0	OK
$\vert +\rangle$	Z	$\vert 0\rangle$, $\Pr = 1/2$	?	✗
	Z	$\vert 1\rangle$, $\Pr = 1/2$	1	OK
	X	$\vert +\rangle$, $\Pr = 1$	?	✗

B92 QKD Protocol

$$|+\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \qquad |0\rangle = \frac{1}{\sqrt{2}}\left(|+\rangle + |-\rangle\right)$$

Continuing the example, we have the following:

Step 2: Bob Receives *n* Random Bits in a Random Basis

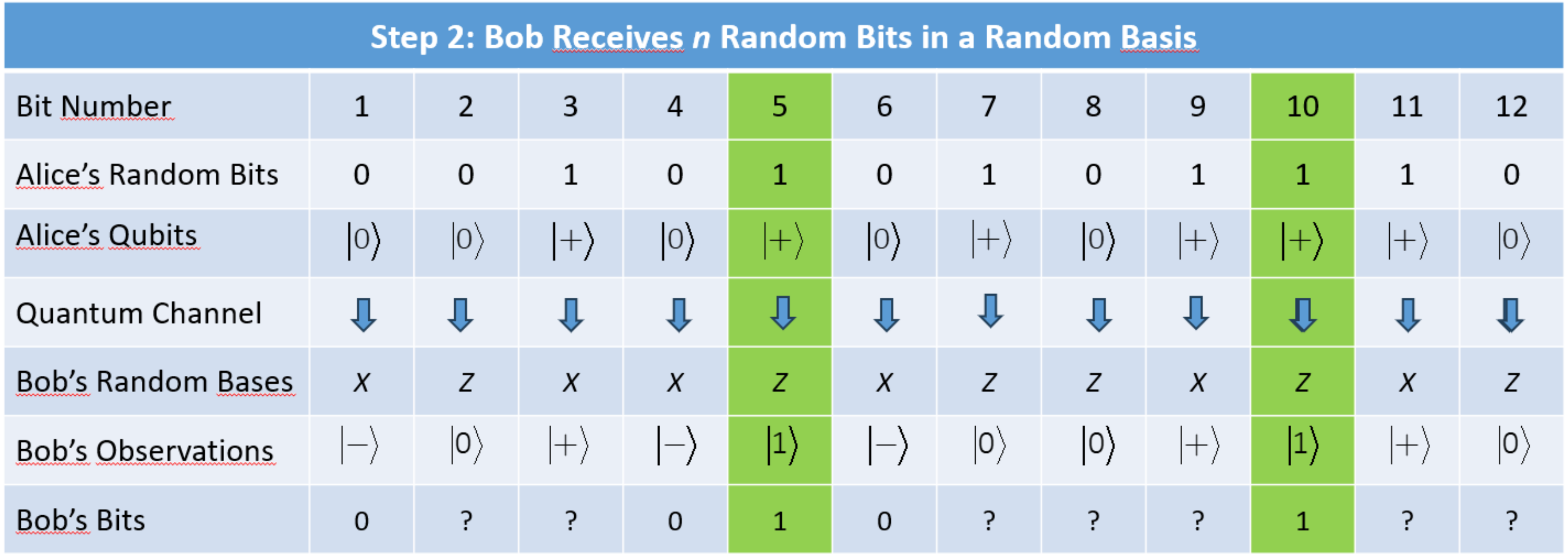
Bit Number	1	2	3	4	5	6	7	8	9	10	11	12
Alice’s Random Bits	0	0	1	0	1	0	1	0	1	1	1	0
Alice’s Qubits	$\|0\rangle$	$\|0\rangle$	$\|+\rangle$	$\|0\rangle$	$\|+\rangle$	$\|0\rangle$	$\|+\rangle$	$\|0\rangle$	$\|+\rangle$	$\|+\rangle$	$\|+\rangle$	$\|0\rangle$
Quantum Channel	⇩	⇩	⇩	⇩	⇩	⇩	⇩	⇩	⇩	⇩	⇩	⇩
Bob’s Random Bases	X	Z	X	X	Z	X	Z	Z	X	Z	X	Z
Bob’s Observations	$\|-\rangle$	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$	$\|1\rangle$	$\|-\rangle$	$\|0\rangle$	$\|0\rangle$	$\|+\rangle$	$\|1\rangle$	$\|+\rangle$	$\|0\rangle$
Bob’s Bits	0	?	?	0	1	0	?	?	?	1	?	?

B92 QKD Protocol

- If Bob uses the Z basis and observes $|1\rangle$, *then he knows that Alice must have sent a*

$$|+\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$$ which collapsed to $|1\rangle$

because if Alice had sent a $|0\rangle$, Bob would have received a $|0\rangle$



Step 2: Bob Receives *n* Random Bits in a Random Basis

Bit Number	1	2	3	4	5	6	7	8	9	10	11	12
Alice's Random Bits	0	0	1	0	1	0	1	0	1	1	1	0
Alice's Qubits	$\|0\rangle$	$\|0\rangle$	$\|+\rangle$	$\|0\rangle$	$\|+\rangle$	$\|0\rangle$	$\|+\rangle$	$\|0\rangle$	$\|+\rangle$	$\|+\rangle$	$\|+\rangle$	$\|0\rangle$
Quantum Channel	⇩	⇩	⇩	⇩	⇩	⇩	⇩	⇩	⇩	⇩	⇩	⇩
Bob's Random Bases	X	Z	X	X	Z	X	Z	Z	X	Z	X	Z
Bob's Observations	$\|-\rangle$	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$	$\|1\rangle$	$\|-\rangle$	$\|0\rangle$	$\|0\rangle$	$\|+\rangle$	$\|1\rangle$	$\|+\rangle$	$\|0\rangle$
Bob's Bits	0	?	?	0	1	0	?	?	?	1	?	?

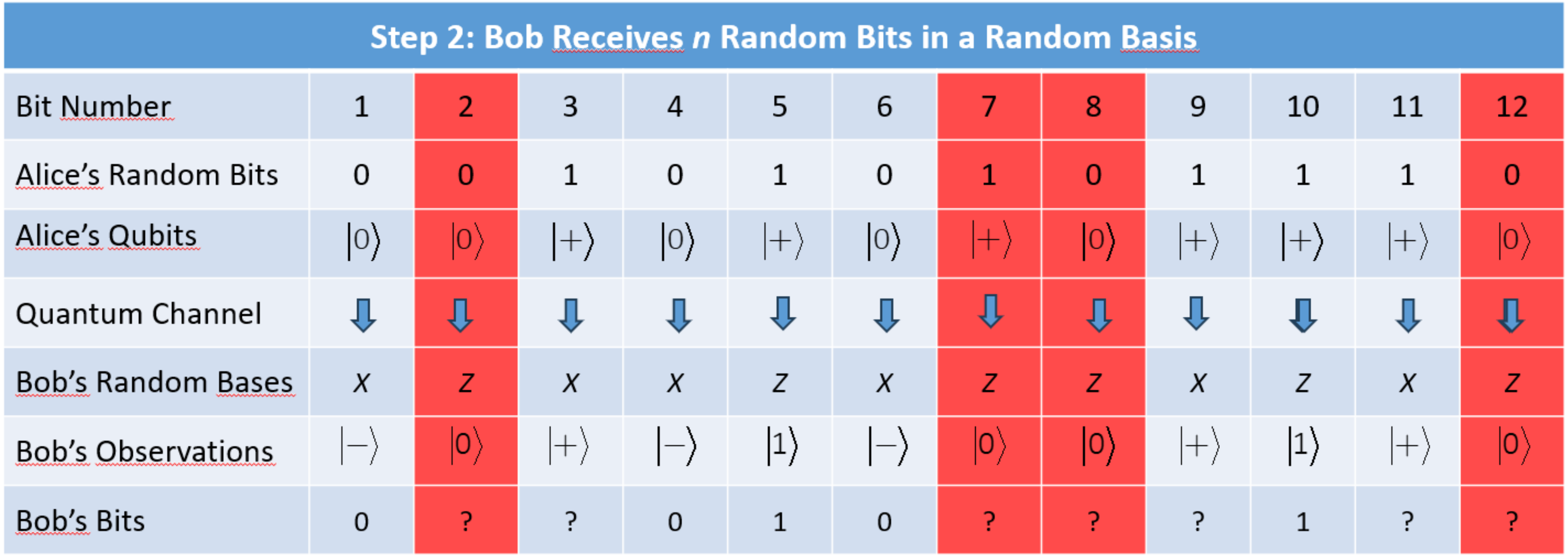
B92 QKD Protocol

$$|0\rangle = \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle)$$

- If Bob uses the Z basis and observes $|0\rangle$ (see red columns) then it is not clear to him which qubit Alice sent:

  > she could have sent a $|0\rangle$ but

  > she could also have sent a $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ which collapsed to $|0\rangle$



Step 2: Bob Receives *n* Random Bits in a Random Basis

Bit Number	1	2	3	4	5	6	7	8	9	10	11	12
Alice's Random Bits	0	0	1	0	1	0	1	0	1	1	1	0
Alice's Qubits	$\|0\rangle$	$\|0\rangle$	$\|+\rangle$	$\|0\rangle$	$\|+\rangle$	$\|0\rangle$	$\|+\rangle$	$\|0\rangle$	$\|+\rangle$	$\|+\rangle$	$\|+\rangle$	$\|0\rangle$
Quantum Channel	⇩	⇩	⇩	⇩	⇩	⇩	⇩	⇩	⇩	⇩	⇩	⇩
Bob's Random Bases	*X*	*Z*	*X*	*X*	*Z*	*X*	*Z*	*Z*	*X*	*Z*	*X*	*Z*
Bob's Observations	$\|-\rangle$	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$	$\|1\rangle$	$\|-\rangle$	$\|0\rangle$	$\|0\rangle$	$\|+\rangle$	$\|1\rangle$	$\|+\rangle$	$\|0\rangle$
Bob's Bits	0	?	?	0	1	0	?	?	?	1	?	?

Because Bob is in doubt, he will omit this bit

B92 QKD Protocol

$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

- If Bob uses the *X* basis and observes a $|-\rangle$, then he knows that Alice must have sent a $|0\rangle$ because if Alice had sent a $|+\rangle$, Bob would have received a $|+\rangle$

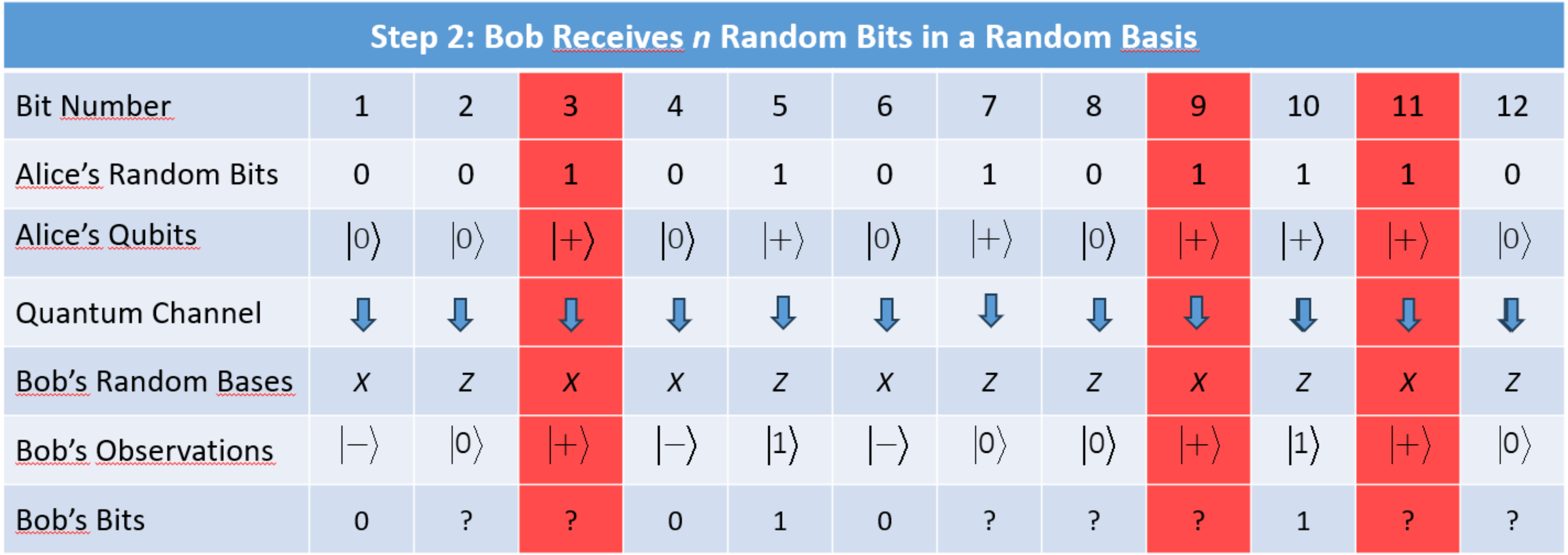
Step 2: Bob Receives *n* Random Bits in a Random Basis

Bit Number	1	2	3	4	5	6	7	8	9	10	11	12
Alice's Random Bits	0	0	1	0	1	0	1	0	1	1	1	0
Alice's Qubits	$\|0\rangle$	$\|0\rangle$	$\|+\rangle$	$\|0\rangle$	$\|+\rangle$	$\|0\rangle$	$\|+\rangle$	$\|0\rangle$	$\|+\rangle$	$\|+\rangle$	$\|+\rangle$	$\|0\rangle$
Quantum Channel	⇩	⇩	⇩	⇩	⇩	⇩	⇩	⇩	⇩	⇩	⇩	⇩
Bob's Random Bases	*X*	*Z*	*X*	*X*	*Z*	*X*	*Z*	*Z*	*X*	*Z*	*X*	*Z*
Bob's Observations	$\|-\rangle$	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$	$\|1\rangle$	$\|-\rangle$	$\|0\rangle$	$\|0\rangle$	$\|+\rangle$	$\|1\rangle$	$\|+\rangle$	$\|0\rangle$
Bob's Bits	0	?	?	0	1	0	?	?	?	1	?	?

B92 QKD Protocol

$$|0\rangle = \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle)$$

- If Bob uses the X basis and observes a $|+\rangle$, then it is not clear to him which qubit Alice sent
- She could have sent a $|+\rangle$ but she could also have sent a $|0\rangle$ that collapsed to a $|+\rangle$



Step 2: Bob Receives *n* Random Bits in a Random Basis

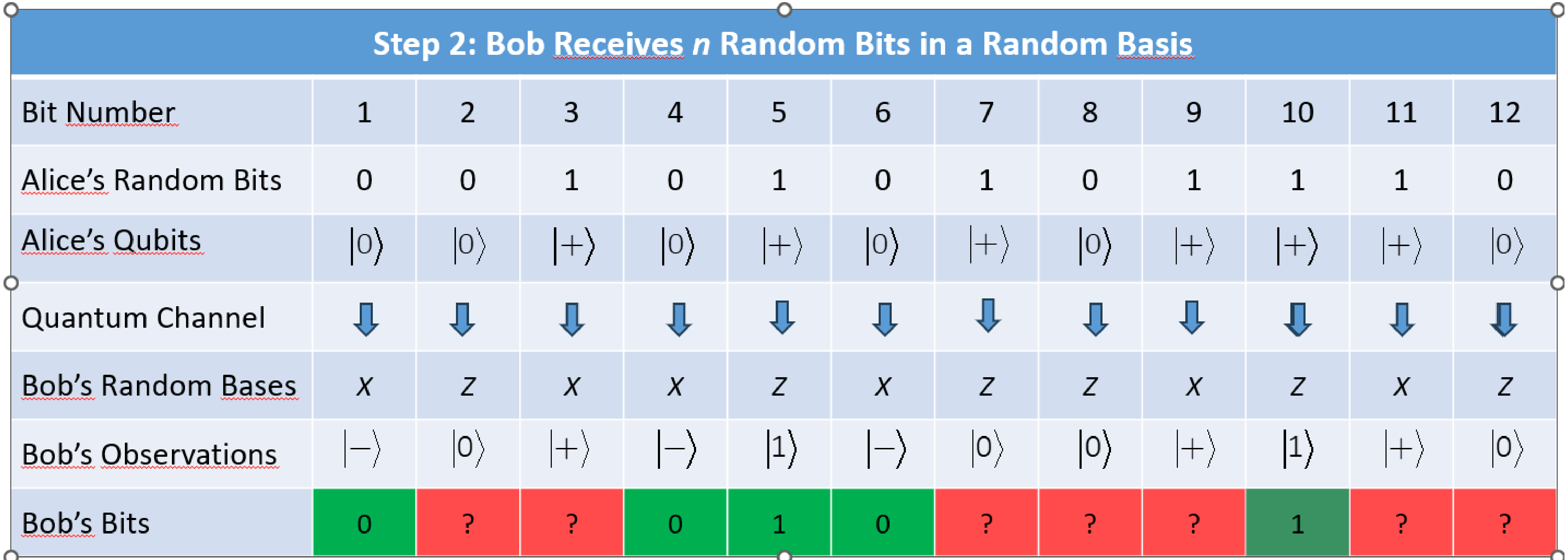
Bit Number	1	2	3	4	5	6	7	8	9	10	11	12
Alice's Random Bits	0	0	1	0	1	0	1	0	1	1	1	0
Alice's Qubits	$\lvert 0\rangle$	$\lvert 0\rangle$	$\lvert +\rangle$	$\lvert 0\rangle$	$\lvert +\rangle$	$\lvert 0\rangle$	$\lvert +\rangle$	$\lvert 0\rangle$	$\lvert +\rangle$	$\lvert +\rangle$	$\lvert +\rangle$	$\lvert 0\rangle$
Quantum Channel	⇩	⇩	⇩	⇩	⇩	⇩	⇩	⇩	⇩	⇩	⇩	⇩
Bob's Random Bases	X	Z	X	X	Z	X	Z	Z	X	Z	X	Z
Bob's Observations	$\lvert -\rangle$	$\lvert 0\rangle$	$\lvert +\rangle$	$\lvert -\rangle$	$\lvert 1\rangle$	$\lvert -\rangle$	$\lvert 0\rangle$	$\lvert 0\rangle$	$\lvert +\rangle$	$\lvert 1\rangle$	$\lvert +\rangle$	$\lvert 0\rangle$
Bob's Bits	0	?	?	0	1	0	?	?	?	1	?	?

Because Bob is in doubt, he will omit this bit

B92 QKD Protocol

Step 4

- Bob publicly tells Alice which bits were uncertain and they both omit them



Step 2: Bob Receives *n* Random Bits in a Random Basis

Bit Number	1	2	3	4	5	6	7	8	9	10	11	12
Alice's Random Bits	0	0	1	0	1	0	1	0	1	1	1	0
Alice's Qubits	$\|0\rangle$	$\|0\rangle$	$\|+\rangle$	$\|0\rangle$	$\|+\rangle$	$\|0\rangle$	$\|+\rangle$	$\|0\rangle$	$\|+\rangle$	$\|+\rangle$	$\|+\rangle$	$\|0\rangle$
Quantum Channel	⇩	⇩	⇩	⇩	⇩	⇩	⇩	⇩	⇩	⇩	⇩	⇩
Bob's Random Bases	X	Z	X	X	Z	X	Z	Z	X	Z	X	Z
Bob's Observations	$\|-\rangle$	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$	$\|1\rangle$	$\|-\rangle$	$\|0\rangle$	$\|0\rangle$	$\|+\rangle$	$\|1\rangle$	$\|+\rangle$	$\|0\rangle$
Bob's Bits	0	?	?	0	1	0	?	?	?	1	?	?

B92 QKD Protocol

- At this point, Alice and Bob know which bits are secret, so they may use those
- But there is **one more step** if they want to detect whether or not Eve was listening in
- They can, as in BB84, sacrifice a **fraction** of their hidden bits and publicly compare them
- If they do not agree for a significant number, then they know that evil Eve has been doing her wicked deeds and the entire bit string should be ignored

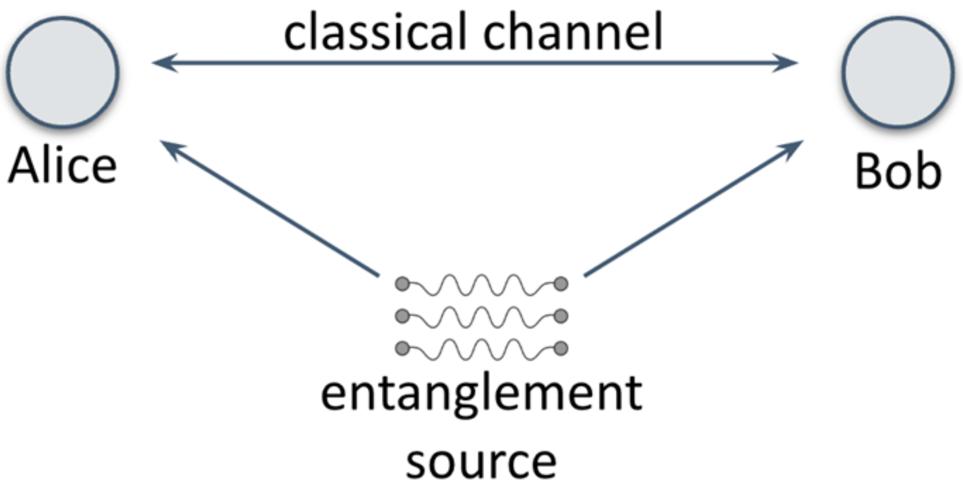
Ekert's Entanglement-Based E91 QKD Protocol

Introduction

- Continuing with our study of quantum key distribution, in the next slides we discuss an **entanglement-based protocol**, known as E91
- This protocol was introduced by Artur Ekert in 1991
- Unlike BB84, the E91 protocol relies on *entanglement shared between Alice and Bob* to establish a secret key
- We will see that this difference offers Alice and Bob a very powerful tool when it comes to verifying the security of their key

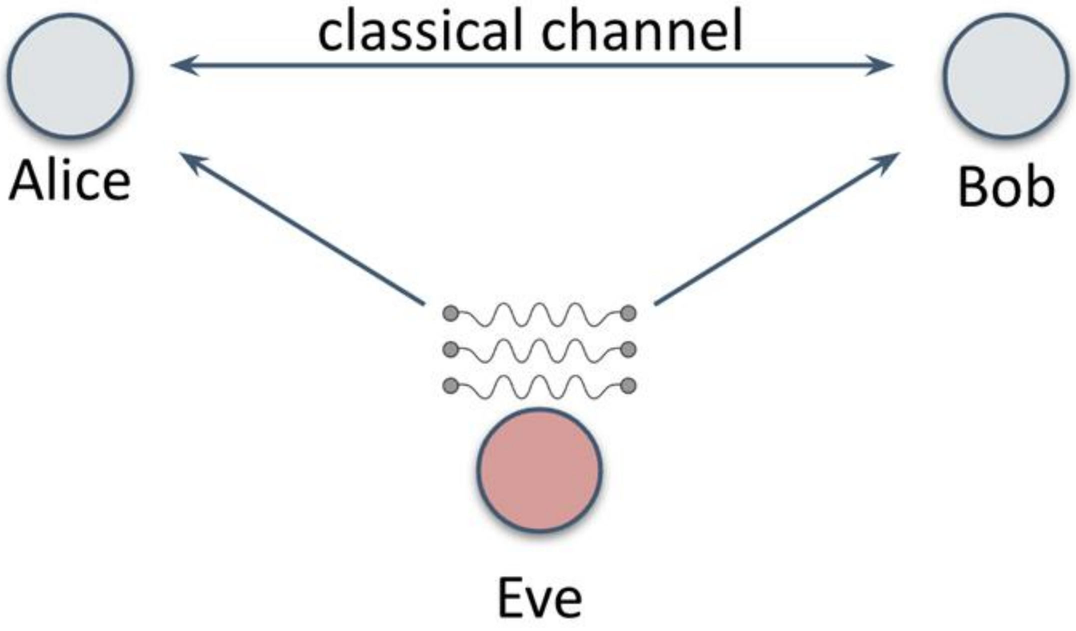
Introduction

- The protocol relies on **pre-shared entanglement between Alice and Bob**
- We will assume that Alice and Bob can communicate over a classical channel, and also that there is some **source of entangled states**, as in figure
- This source generates multiple copies of an entangled state and distributes the qubits to Alice and to Bob



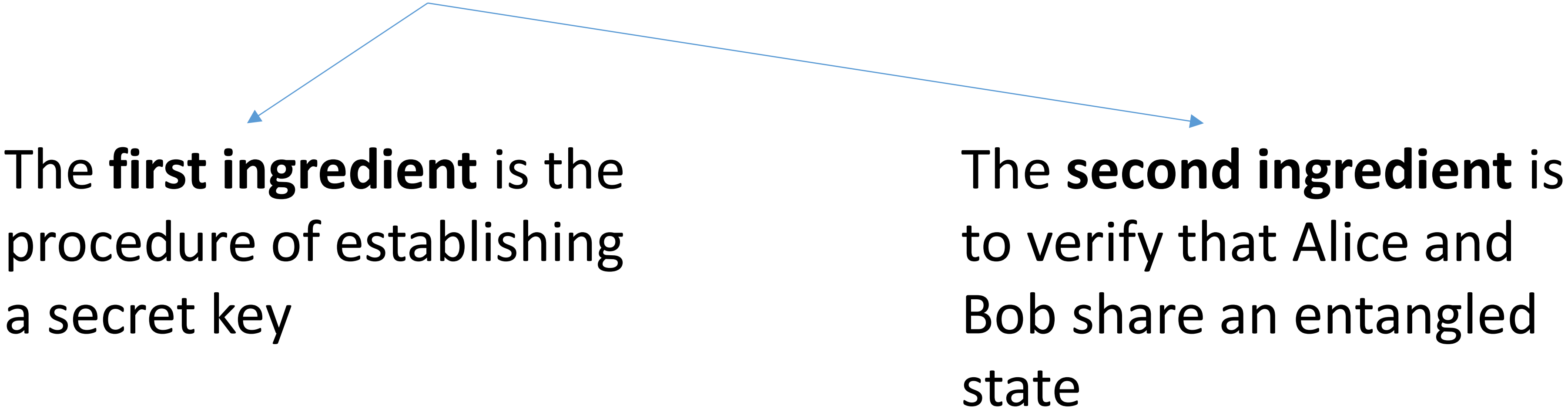
Introduction

- We will see that in this protocol, **even if Eve controls the source of the qubits**, as in figure, the protocol still remains secure in the sense that Alice and Bob can **easily detect** an eavesdropping Eve



E91 QKD Protocol/Basic Ingredients

There are **two basic ingredients** to our entanglement-based QKD protocol

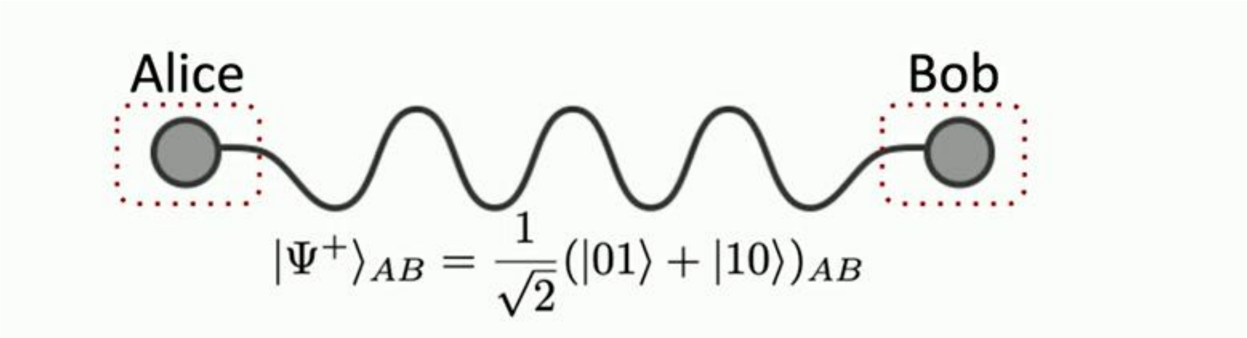


The **first ingredient** is the procedure of establishing a secret key

The **second ingredient** is to verify that Alice and Bob share an entangled state

Basic Ingredients

- As we said in the previous slide, the **first ingredient** is the procedure of establishing a secret key
- For that purpose, we will use an entangled state of two qubits
- Let's consider the case where Alice and Bob are sharing the following Bell pair



$$|\Psi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)_{AB}$$

- If we measure these qubits in the same basis, the outcomes will be correlated or anti-correlated depending in which basis they are measured
- Furthermore, the probability of these outcomes is uniformly random

Basic Ingredients

- Let’s look at an example to demonstrate how this measurement works
- Assume that both Alice and Bob measure in the *X* basis
- We can compute the probabilities of all four possible outcomes
- Before doing this, we recall that on the *Z* basis

$$\left|\Psi^{+}\right\rangle_{AB} = \frac{1}{\sqrt{2}}\left(\left|01\right\rangle_{AB} + \left|10\right\rangle_{AB}\right)$$

while on the *X* basis

$$\left|\Psi^{+}\right\rangle_{AB} = \frac{1}{\sqrt{2}}\left(\left|++\right\rangle_{AB} - \left|--\right\rangle_{AB}\right)$$

$$\rightarrow$$

Basic Ingredients

$$\text{Prob}\left\{\left|++\right\rangle_{AB}\right\}=\frac{1}{2},\quad \text{Prob}\left\{\left|+-\right\rangle_{AB}\right\}=0,$$

$$\text{Prob}\left\{\left|--\right\rangle_{AB}\right\}=\frac{1}{2},\quad \text{Prob}\left\{\left|-+\right\rangle_{AB}\right\}=0.$$

- The probability that both Alice and Bob obtain a correlated result of $|++\rangle$ is given by a half
- The probability that they get a $|--\rangle$ outcome is also a half, leaving the other with no probability of being observed
- In this way, when Alice measures state $|+\rangle$, Bob always measures state $|+\rangle$
- When Alice measures state $|-\rangle$, Bob always measures state $|-\rangle$

Basic Ingredients

- If they measure on the Z basis, the scenario is very similar, although now the results are anti-correlated

$$\text{Prob}\left\{|00\rangle_{AB}\right\}=0, \quad \text{Prob}\left\{|01\rangle_{AB}\right\}=\frac{1}{2},$$
$$\text{Prob}\left\{|11\rangle_{AB}\right\}=0, \quad \text{Prob}\left\{|10\rangle_{AB}\right\}=\frac{1}{2}.$$

- The probability of correlated outcomes is zero this time
- When Alice and Bob both measure in the Z basis, the outcomes will never be $|00\rangle_{AB}$ or $|11\rangle_{AB}$

Basic Ingredients

- The outcomes are always anti-correlated, meaning that when Alice's outcome is $|0\rangle_A$, Bob will measure $|1\rangle_B$
- Similarly, when Alice measures $|1\rangle_A$, Bob's outcome will be $|0\rangle_B$
- An important thing to note is that both possibilities are equally probable, with 50% probability they share $|01\rangle_{AB}$, and with the same probability they share $|10\rangle_{AB}$

Basic Ingredients

- The corresponding classical keys are anti correlated as well
- All that Bob has to do is flip his bits in order to obtain a random, correlated key, which can then be used to encrypt data for communication

$$\begin{matrix} 0_A \\ 1_B \end{matrix} \text{ or } \begin{matrix} 1_A \\ 0_B \end{matrix} \xrightarrow{\textit{Flip B}} \begin{matrix} 0_A \\ 0_B \end{matrix} \text{ or } \begin{matrix} 1_A \\ 1_B \end{matrix} \leftarrow$$

secret random correlated key

E91 QKD Protocol/Monogamy of Entanglement

- The **second ingredient** of an entangled-based QKD protocol is to verify that they (Alice and Bob) have an entangled state.
- Why do they need to do this verification?
- The *first reason*, as we just saw, is that **entangled states can be used to generate a correlated random key**, so it is crucial to confirm that we really have entanglement before we try to use it.
- But also, there is a very important *second step* which was not present in the BB84 protocol, and that is that entanglement can be used for **security** as well, namely **maximally entangled states** are guaranteed to be secure due to something known as *monogamy of entanglement*.

E91 QKD Protocol

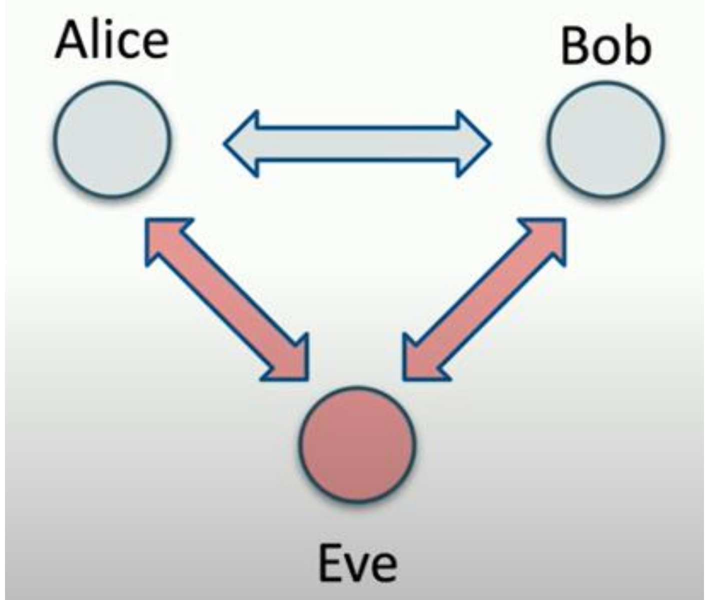
- So, what is monogamy of entanglement? This has already been shown in a previous lesson.
- Monogamy of entanglement is a very fundamental property of quantum states, and it constrains how correlated multiple qubits can be.
- In particular, if Alice and Bob share a *maximally entangled state*, then we are **guaranteed** that they **cannot share** any correlations with a **third party**, such as Eve.
- So, in terms of security this is very important because if Alice and Bob can demonstrate and verify that they have a maximally entangled state, they are automatically demonstrating that whatever key they establish is secure and Eve does not have any information about their secret key.

E91 QKD Protocol

- In general, there is a trade-off
- If Alice and Bob share some entanglement, but **not** a maximally entangled state, they can still share some correlations with Eve
- The stronger the entanglement that they share, the less correlated they are with Eve, until the point where they are maximally entangled, and therefore they share no correlations with Eve.

↓

A stronger entanglement between Alice and Bob implies a more secure key between Alice and Bob



CHSH Inequality

- So how do we verify that Alice and Bob are sharing a **maximally entangled** key?
- We use something known as *CHSH* inequality
- *CHSH* stands for John **C**lauser, Michael **H**orne, Abner **S**himony, and Richard **H**olt, who described it in a much-cited paper published in 1969
- It is part of a larger set of inequalities known generically as **Bell inequalities** since the first was found by John Bell

CHSH Inequality

- Imagine the following scenario
- Alice and Bob, our two characters with a predilection for wacky experiments, are equipped with appropriate measuring devices and sent to two distant locations
- Assume that Alice and Bob each have a choice of ***two*** observables that they can measure, each with well defined values +1 and −1
- Let’s say that Alice can choose between observables A_1 and A_2, and Bob between B_1 and B_2

Alice

$A_1 = \pm 1$

$A_2 = \pm 1$

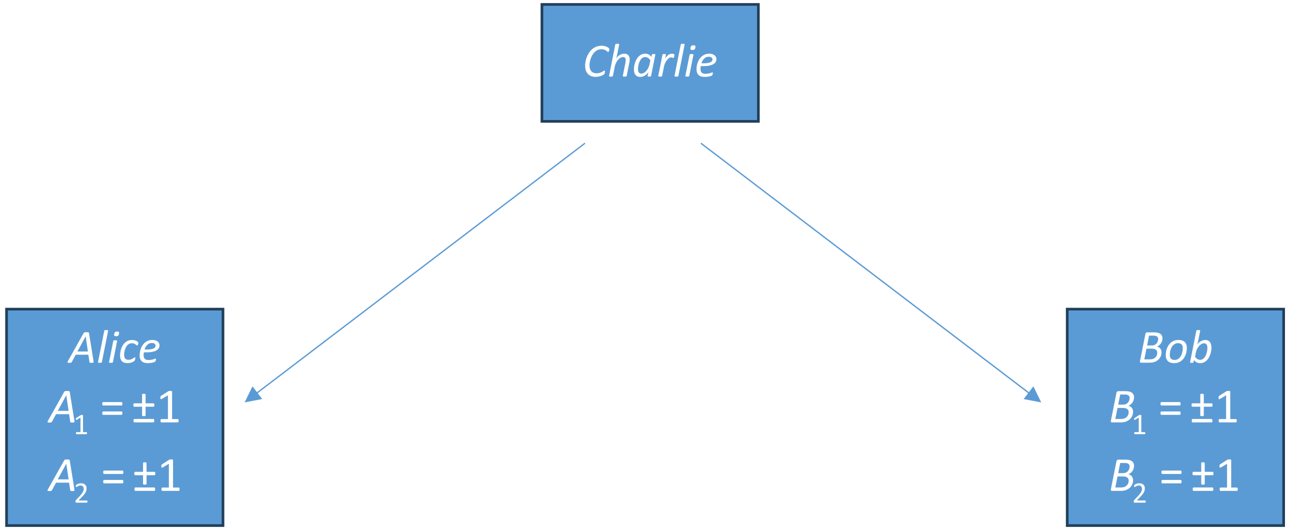
Bob

$B_1 = \pm 1$

$B_2 = \pm 1$

CHSH Inequality

- Now, somewhere in between them there is a source (Charlie) that emits **pairs** of particles that fly apart, one towards Alice and one towards Bob

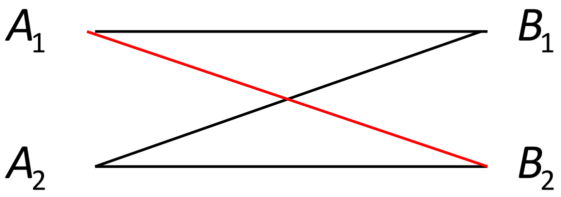


- For each incoming particle, Alice and Bob choose randomly (e.g., they can toss a coin), and independently from each other, which particular **observable** will be measured

CHSH Inequality

- This means we can think of the observables as random variables A_k, B_k (for k = 1,2) that take values 1 or -1
- Using these, we can define a new random variable

$$A_1 B_1 - A_1 B_2 + A_2 B_1 + A_2 B_2 = A_1(B_1 - B_2) + A_2(B_1 + B_2)$$



The red line represents -1

By a case-by-case analysis of the four possible outcomes for the pair (B_1, B_2), we see that one of the terms $B_1 \pm B_2$ must be equal to zero and the other to ± 2 (basically depending on if $B_1 = B_2$ or not), and so (looking at the four possible outcomes for the pair (A_1, A_2)) we see that $A_1(B_1 - B_2) + A_2(B_1 + B_2) = \pm 2$

E91 QKD Protocol

- Suppose next that $p(a_1, a_2, b_1, b_2)$ is the probability that, before the measurements are performed, the system is in a state where

$$A_1 = a_1,\ A_2 = a_2,\ B_1 = b_1 \text{ and } B_2 = b_2$$

- These probabilities may depend on how Charlie performs his preparation, and on experimental noise
- Letting $\langle\cdot\rangle$ denote the mean value of a quantity, we have

$$\left\langle A_1B_1 - A_1B_2 + A_2B_1 + A_2B_2 \right\rangle = \sum_{\substack{a_1,\, a_2 \\ b_1,\, b_2}} p\left(a_1,\, a_2,\, b_1,\, b_2\right)\left(a_1b_1 - a_1b_2 + a_2b_1 + a_2b_2\right)$$

$$\leq \sum_{\substack{a_1,\, a_2 \\ b_1,\, b_2}} p\left(a_1, a_2, b_1, b_2\right) \times 2 = 2 \qquad [1]$$

E91 QKD Protocol

- Since $A_1B_1 - A_1B_2 + A_2B_1 + A_2B_2 = \pm 2$ we can also write

$$\left\langle A_1B_1 - A_1B_2 + A_2B_1 + A_2B_2 \right\rangle = \sum_{\substack{a_1, a_2 \\ b_1, b_2}} p\left(a_1, a_2, b_1, b_2\right)\left(a_1b_1 - a_1b_2 + a_2b_1 + a_2b_2\right)$$

$$\geq \sum_{\substack{a_1, a_2 \\ b_1, b_2}} p\left(a_1, a_2, b_1, b_2\right) \times \left(-2\right) = -2$$

[2]

E91 QKD Protocol

- Also

$$\left\langle A_1B_1 - A_1B_2 + A_2B_1 + A_2B_2 \right\rangle = \sum_{\substack{a_1,\, a_2 \\ b_1,\, b_2}} p\left(a_1,\, a_2,\, b_1,\, b_2\right) a_1 b_1 - \sum_{\substack{a_1,\, a_2 \\ b_1,\, b_2}} p\left(a_1,\, a_2,\, b_1,\, b_2\right) a_1 b_2$$

$$+ \sum_{\substack{a_1,\, a_2 \\ b_1,\, b_2}} p\left(a_1,\, a_2,\, b_1,\, b_2\right) a_2 b_1 + \sum_{\substack{a_1,\, a_2 \\ b_1,\, b_2}} p\left(a_1,\, a_2,\, b_1,\, b_2\right) a_2 b_2$$

$$= \sum_{a_1,\, b_1} p\left(a_1,\, b_1\right) a_1 b_1 - \sum_{a_1,\, b_2} p\left(a_1,\, b_2\right) a_1 b_2$$

$$+ \sum_{a_2,b_1} p\left(a_2,\, b_1\right) a_2 b_1 + \sum_{a_2,b_2} p\left(a_2,\, b_2\right) a_2 b_2$$

$$= \left\langle A_1B_1 \right\rangle - \left\langle A_1B_2 \right\rangle + \left\langle A_2B_1 \right\rangle + \left\langle A_2B_2 \right\rangle$$

[3]

E91 QKD Protocol

- Comparing [1], [2] and [3] we obtain

$$-2 \leq \left\langle A_1 B_1 \right\rangle - \left\langle A_1 B_2 \right\rangle + \left\langle A_2 B_1 \right\rangle + \left\langle A_2 B_2 \right\rangle \leq 2 \qquad [4]$$

E91 QKD Protocol

- The *CHSH inequality* [4] can be synthesized as

$$\boxed{S = \left| \langle A_1 B_1 \rangle - \langle A_1 B_2 \rangle + \langle A_2 B_1 \rangle + \langle A_2 B_2 \rangle \right| \leq 2}$$ [5]

- By repeating the experiment many times, Alice and Bob can determine each quantity on the left-hand side of the *CHSH inequality* that we have denoted by S
- For example, after finishing a set of experiments, Alice and Bob get together to analyze their data
- They look at all the experiments where Alice measured A_1 and Bob measured B_2

E91 QKD Protocol

- By multiplying the results of their experiments together, they get a sample of values for $A_1 B_2$
- By averaging over this sample, they can estimate $\langle A_1 B_2 \rangle$ to an accuracy only limited by the number of experiments that they perform
- Similarly, they can estimate all the other quantities on the left-hand side of the *CHSH inequality*, and thus check to see whether it is obeyed in a real experiment
- To conclude, the **classical system** previously described must meet the constraint of the *CHSH inequality*

E91 QKD Protocol

- There is absolutely *no quantum theory involved* in the *CHSH* inequality

$$S \leq 2$$

because the *CHSH* inequality is not specific to quantum theory: it does not really matter what kind of physical process is behind the appearance of binary values of A_1, A_2, B_1, and B_2; it is merely a statement about correlations, and for all classical correlations we must have

$$S = \left| \langle A_1 B_1 \rangle - \langle A_1 B_2 \rangle + \langle A_2 B_1 \rangle + \langle A_2 B_2 \rangle \right| \leq 2$$

(which is just another way of phrasing the *CHSH* inequality)

E91 QKD Protocol

- What happens in the quantum case?
- We can consider A_1, A_2, B_1, and B_2 to be **observables** which provides outcomes ±1 when state $|\psi\rangle$ is measured in a certain basis
- Just as a reminder, the expectation value of an observable where Alice measures observable A_1 and Bob measures observable B_1 is given by the expression

$$\langle A_1 B_1 \rangle = \langle \psi | A_1 \otimes B_1 | \psi \rangle$$

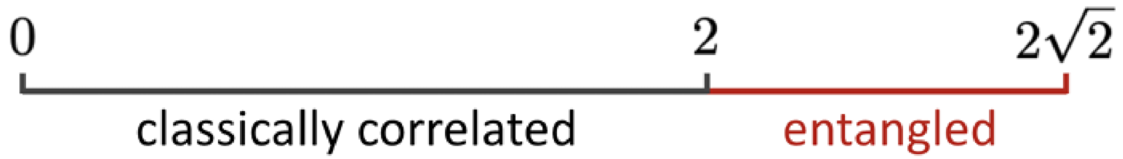
- Given that the measurement outcomes are still ±1, we might expect that the *CHSH* inequality in equation [5] applies to the quantum case too

E91 QKD Protocol

- Amazingly, **for some quantum states**, we can **violate** the *CHSH* inequality
- By “violating”, we mean that we can obtain a value *S* that is larger than 2
- In particular, in an experiment where we measure and compute these four expectation values and then we sum them up in this manner, if we obtain a *CHSH* expression which is less than two, then we can say ***maybe*** the states are classically correlated

E91 QKD Protocol

- But, if we measure a *CHSH* expression which is **larger than two**, then we can say that definitely these states are entangled
- In quantum mechanics, *S* can go all the way up to a value of $2\sqrt{2}$, which happens for maximally entangled states



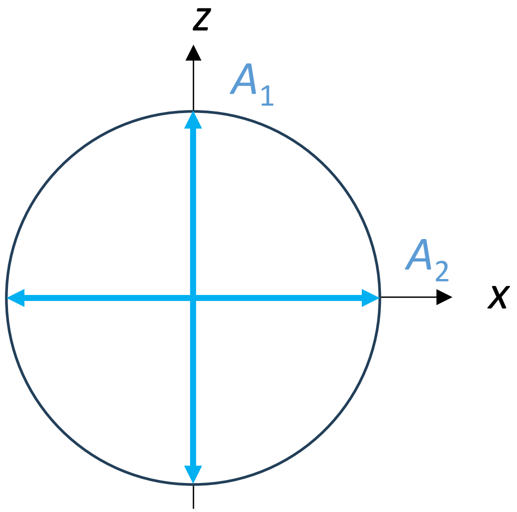
E91 QKD Protocol

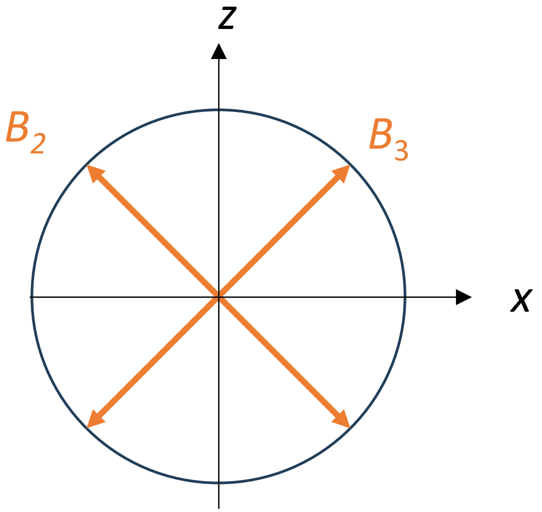
- Let's consider a particular example
- Take one of the Bell pairs,

$$\left|\Psi^{+}\right\rangle_{AB} = \frac{1}{\sqrt{2}}\left(\left|01\right\rangle_{AB} + \left|10\right\rangle_{AB}\right)$$

- For the **CHSH measurement settings**, we consider the following **observables**:

Alice	*Bob*
$A_1 = Z$	$B_2 = \frac{1}{\sqrt{2}}(Z - X)$
$A_2 = X$	$B_3 = \frac{1}{\sqrt{2}}(Z + X)$





E91 QKD Protocol

- We can go through the algebra of computing the four expectation values

$$\langle A_1 B_2 \rangle,\ \langle A_1 B_3 \rangle,\ \langle A_2 B_2 \rangle,\ \langle A_2 B_3 \rangle$$

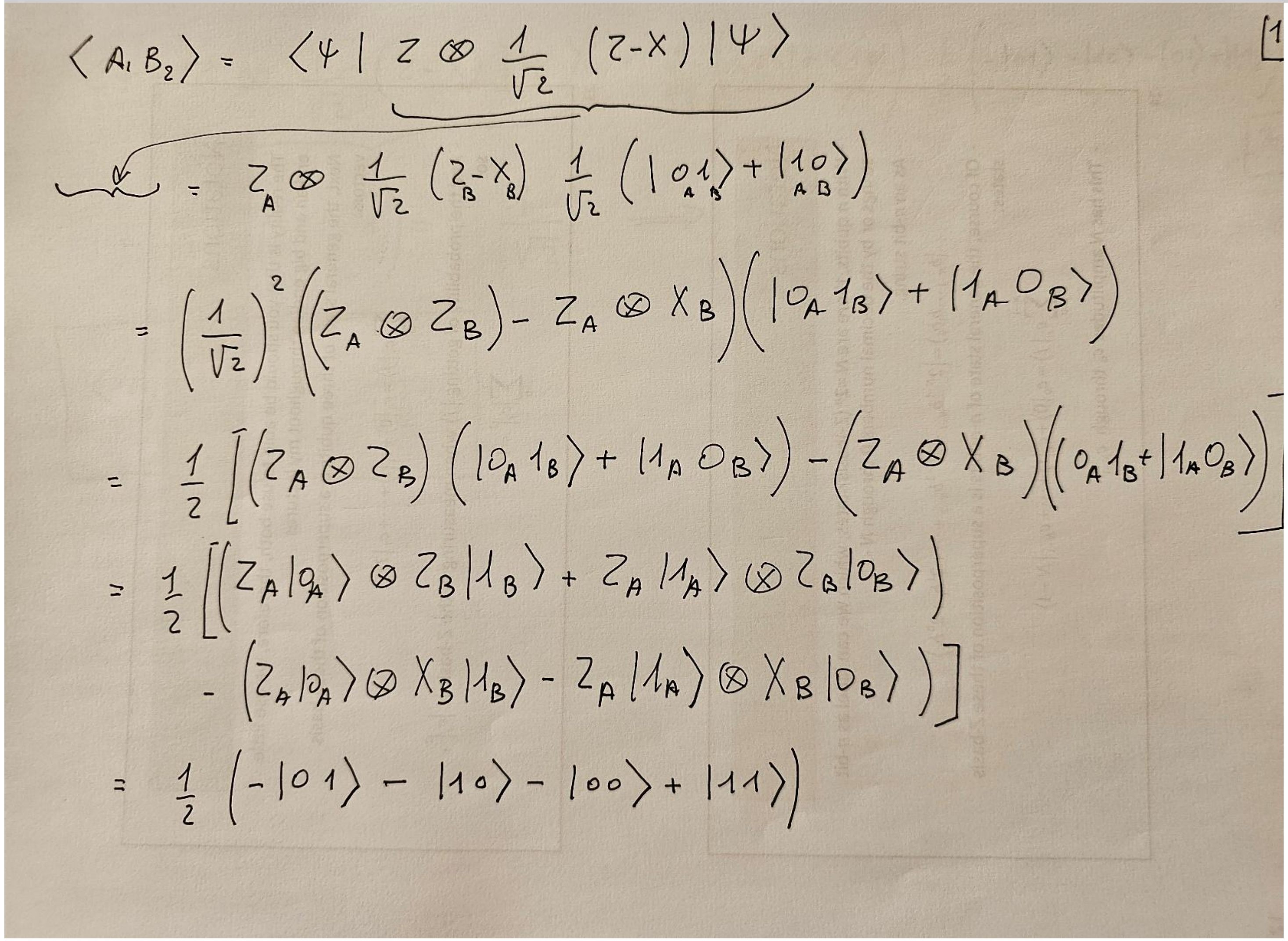
for a maximally entangled state

$$\left|\Psi^+\right\rangle_{AB} = \frac{1}{\sqrt{2}}\left(\left|01\right\rangle_{AB} + \left|10\right\rangle_{AB}\right)$$

and then *S*

$$S = \left|\langle A_1 B_2 \rangle + \langle A_1 B_3 \rangle + \langle A_2 B_2 \rangle - \langle A_2 B_3 \rangle\right|$$

E91 QKD Protocol



$$\langle A_1 B_2 \rangle = \langle \Psi | \underbrace{Z \otimes \frac{1}{\sqrt{2}} (Z - X) | \Psi \rangle}$$

$$\underbrace{\quad} = Z_A \otimes \frac{1}{\sqrt{2}} (Z_B - X_B) \; \frac{1}{\sqrt{2}} \left(|01\rangle_{AB} + |10\rangle_{AB} \right)$$

$$= \left(\frac{1}{\sqrt{2}} \right)^2 \left((Z_A \otimes Z_B) - Z_A \otimes X_B \right) \left(|0_A 1_B\rangle + |1_A 0_B\rangle \right)$$

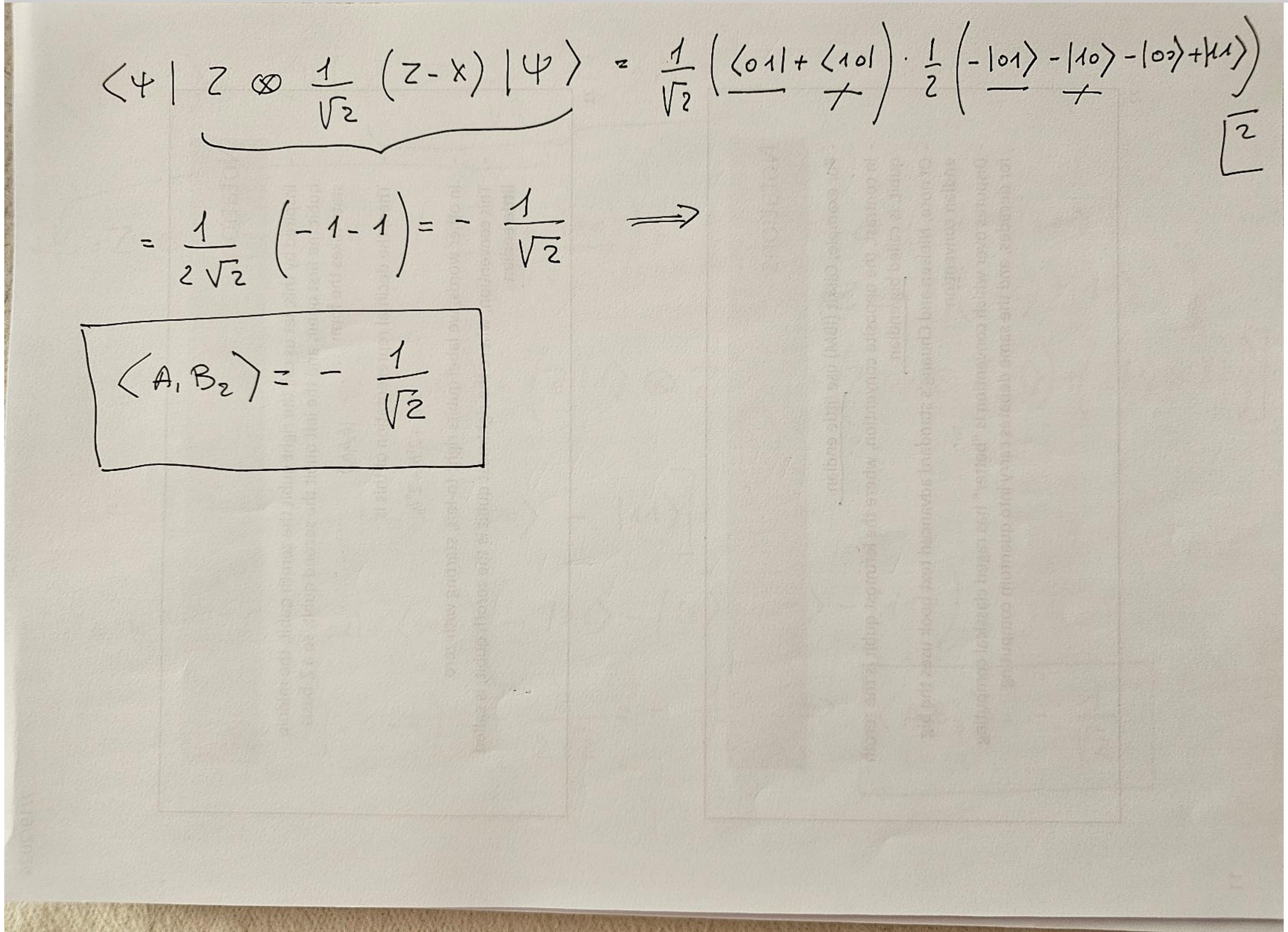
$$= \frac{1}{2} \left[(Z_A \otimes Z_B) \left(|0_A 1_B\rangle + |1_A 0_B\rangle \right) - (Z_A \otimes X_B) \left((0_A 1_B + |1_A 0_B\rangle \right) \right]$$

$$= \frac{1}{2} \Big[\left(Z_A |0_A\rangle \otimes Z_B |1_B\rangle + Z_A |1_A\rangle \otimes Z_B |0_B\rangle \right)$$

$$- \left(Z_A |0_A\rangle \otimes X_B |1_B\rangle - Z_A |1_A\rangle \otimes X_B |0_B\rangle \right) \Big) \Big]$$

$$= \frac{1}{2} \left(-|01\rangle - |10\rangle - |00\rangle + |11\rangle \right)$$

E91 QKD Protocol

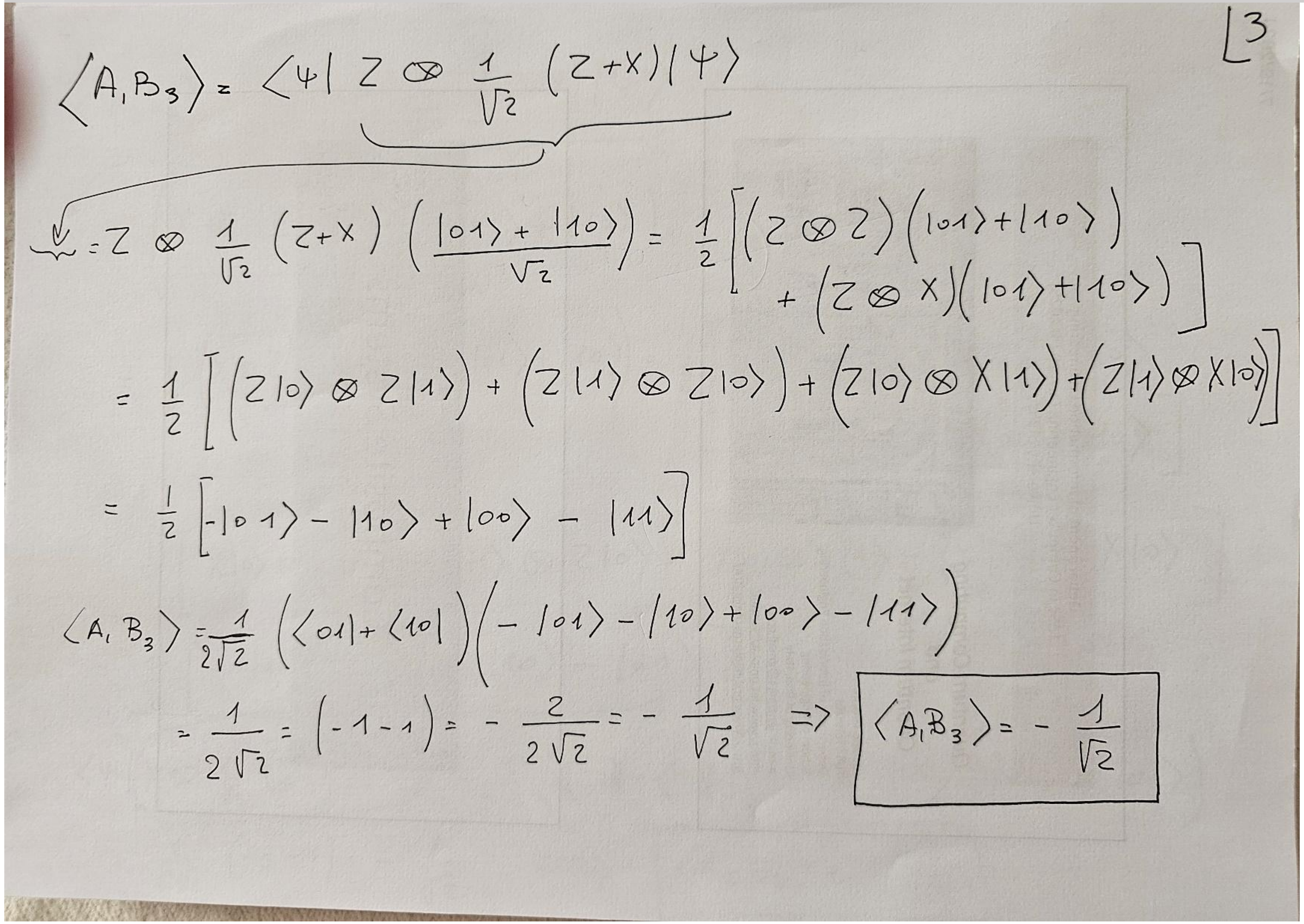


$$\langle \psi | \underbrace{Z \otimes \frac{1}{\sqrt{2}} (Z - X)}_{} | \psi \rangle = \frac{1}{\sqrt{2}} \left(\underline{\langle 01|} + \underset{+}{\langle 10|} \right) \cdot \frac{1}{2} \left(- \underline{|01\rangle} - \underset{+}{|10\rangle} - |00\rangle + |11\rangle \right) \sqrt{2}$$

$$= \frac{1}{2\sqrt{2}} \left(-1 - 1 \right) = - \frac{1}{\sqrt{2}} \implies$$

$$\boxed{\langle A_1 B_2 \rangle = - \frac{1}{\sqrt{2}}}$$

E91 QKD Protocol



3

$$\langle A_1 B_3 \rangle = \langle \psi | \underbrace{Z \otimes \frac{1}{\sqrt{2}} (Z+X) | \psi \rangle}$$

$$= Z \otimes \frac{1}{\sqrt{2}} (Z+X) \left(\frac{|01\rangle + |10\rangle}{\sqrt{2}} \right) = \frac{1}{2} \Big[(Z \otimes Z)\big(|01\rangle + |10\rangle\big) + (Z \otimes X)\big(|01\rangle + |10\rangle\big) \Big]$$

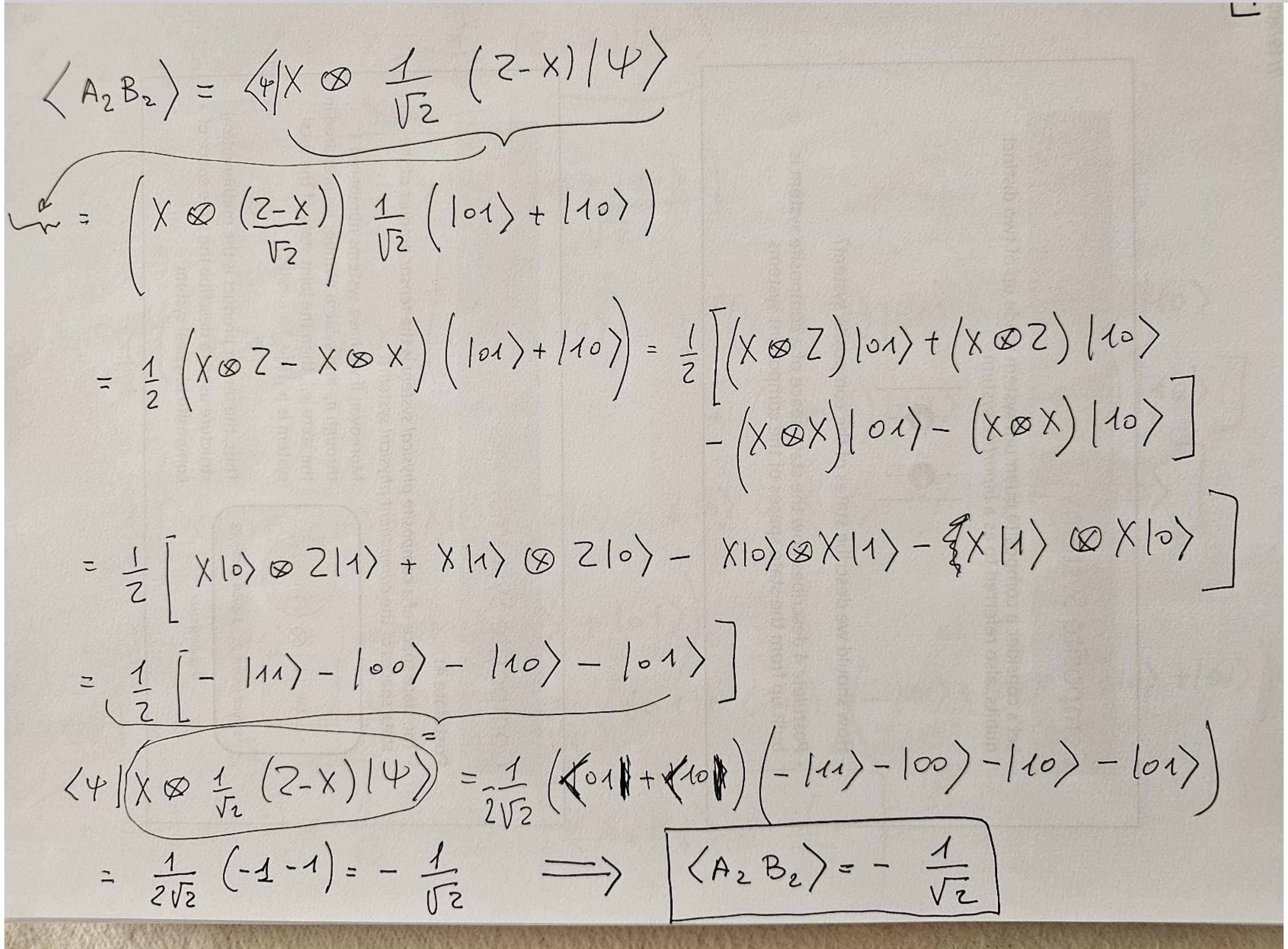
$$= \frac{1}{2} \Big[\big(Z|0\rangle \otimes Z|1\rangle\big) + \big(Z|1\rangle \otimes Z|0\rangle\big) + \big(Z|0\rangle \otimes X|1\rangle\big) + \big(Z|1\rangle \otimes X|0\rangle\big) \Big]$$

$$= \frac{1}{2} \Big[-|01\rangle - |10\rangle + |00\rangle - |11\rangle \Big]$$

$$\langle A_1 B_3 \rangle = \frac{1}{2\sqrt{2}} \big(\langle 01| + \langle 10| \big) \big(-|01\rangle - |10\rangle + |00\rangle - |11\rangle \big)$$

$$= \frac{1}{2\sqrt{2}} = (-1-1) = -\frac{2}{2\sqrt{2}} = -\frac{1}{\sqrt{2}} \Rightarrow \boxed{\langle A_1 B_3 \rangle = -\frac{1}{\sqrt{2}}}$$

E91 QKD Protocol



$$\langle A_2 B_2 \rangle = \langle \psi | \underbrace{X \otimes \frac{1}{\sqrt{2}} (Z - X) | \psi \rangle}$$

$$= \left(X \otimes \frac{(Z-X)}{\sqrt{2}} \right) \frac{1}{\sqrt{2}} \left(|01\rangle + |10\rangle \right)$$

$$= \frac{1}{2} \left(X \otimes Z - X \otimes X \right) \left(|01\rangle + |10\rangle \right) = \frac{1}{2} \Big[(X \otimes Z) |01\rangle + (X \otimes Z) |10\rangle - (X \otimes X) |01\rangle - (X \otimes X) |10\rangle \Big]$$

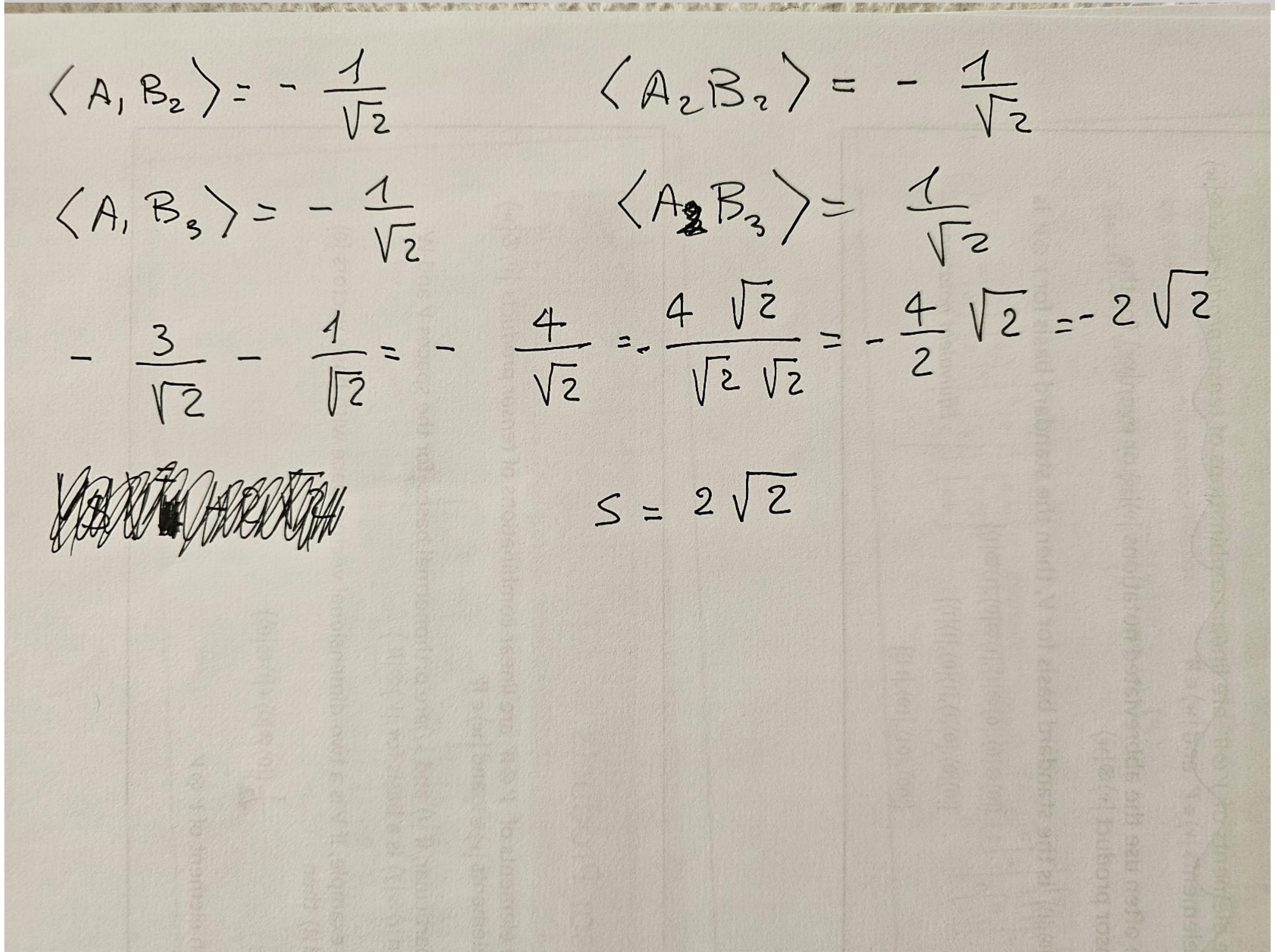
$$= \frac{1}{2} \Big[X|0\rangle \otimes Z|1\rangle + X|1\rangle \otimes Z|0\rangle - X|0\rangle \otimes X|1\rangle - X|1\rangle \otimes X|0\rangle \Big]$$

$$= \underbrace{\frac{1}{2} \Big[-|11\rangle - |00\rangle - |10\rangle - |01\rangle \Big]}_{=}$$

$$\langle \psi | \left(X \otimes \frac{1}{\sqrt{2}} (Z - X) | \psi \rangle \right) = \frac{1}{2\sqrt{2}} \left(\langle 01| + \langle 10| \right) \left(-|11\rangle - |00\rangle - |10\rangle - |01\rangle \right)$$

$$= \frac{1}{2\sqrt{2}} (-1 - 1) = -\frac{1}{\sqrt{2}} \implies \boxed{\langle A_2 B_2 \rangle = -\frac{1}{\sqrt{2}}}$$

E91 QKD Protocol



$\langle A_1 B_2 \rangle = -\frac{1}{\sqrt{2}}$ $\langle A_2 B_2 \rangle = -\frac{1}{\sqrt{2}}$

$\langle A_1 B_3 \rangle = -\frac{1}{\sqrt{2}}$ $\langle A_2 B_3 \rangle = \frac{1}{\sqrt{2}}$

$$-\frac{3}{\sqrt{2}} - \frac{1}{\sqrt{2}} = -\frac{4}{\sqrt{2}} = -\frac{4\sqrt{2}}{\sqrt{2}\sqrt{2}} = -\frac{4}{2}\sqrt{2} = -2\sqrt{2}$$

$S = 2\sqrt{2}$

E91 QKD Protocol

- Hold on! We learned back in [5] that the absolute value of the average value $\langle A_1 B_2 \rangle$ plus the average value $\langle A_1 B_3 \rangle$ plus the average value $\langle A_2 B_2 \rangle$ minus the average $\langle A_2 B_3 \rangle$ value **can never exceed two**
- Yet here, **quantum mechanics** predicts that this sum of averages yields $2\sqrt{2}$!
- Fortunately, we can ask **Nature** to resolve the apparent paradox for us
- Clever experiments using photons have been done to check the prediction [6] of quantum mechanics versus the CHSH inequality [5] which we were led to by our common-sense reasoning

E91 QKD Protocol

- The details of the experiments are outside the scope of the course, but the results were resoundingly in favor of the quantum mechanical prediction
- The *CHSH* inequality [5] is not obeyed by Nature
- What does this mean? It means that **one or more of the assumptions** that went into the derivation of the Bell inequality **must be incorrect**
- The analysis of these assumptions is outside the scope of the course

E91 QKD Protocol

- Now it's time to put together, in a quantum mechanics picture, the two basic ingredients of the E91 protocol, namely,
  - the *monogamy of entanglement*, and
  - the *CHSH inequality*
- Imagine we perform the following quantum mechanical experiment
- Charlie prepares a quantum system of two qubits in the maximum entangled state

$$\left|\Psi^{+}\right\rangle_{AB} = \frac{1}{\sqrt{2}}\left(\left|01\right\rangle_{AB} + \left|10\right\rangle_{AB}\right)$$

and passes the first qubit to Alice, and the second qubit to Bob

E91 QKD Protocol

- Then, Alice and Bob **randomly choose**, from the following **three** measurement bases, a measurement basis in which they measure their qubits

	Alice	Bob
	$A_1 = Z$	$B_1 = Z$
	$A_2 = X$	$B_2 = \frac{1}{\sqrt{2}}(Z - X)$
	$A_3 = \frac{1}{\sqrt{2}}(Z + X)$	$B_3 = \frac{1}{\sqrt{2}}(Z + X)$

E91 QKD Protocol

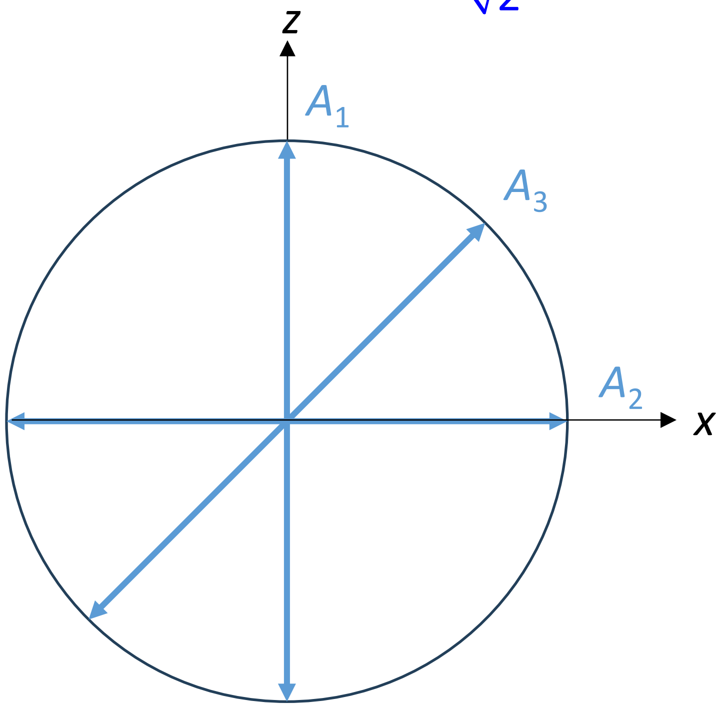
The *x*-*z* plane of the Block sphere is where Alice and Bob's bases can be displayed

Alice

$A_1 = Z$

$A_2 = X$

$A_3 = \frac{1}{\sqrt{2}}(Z + X)$

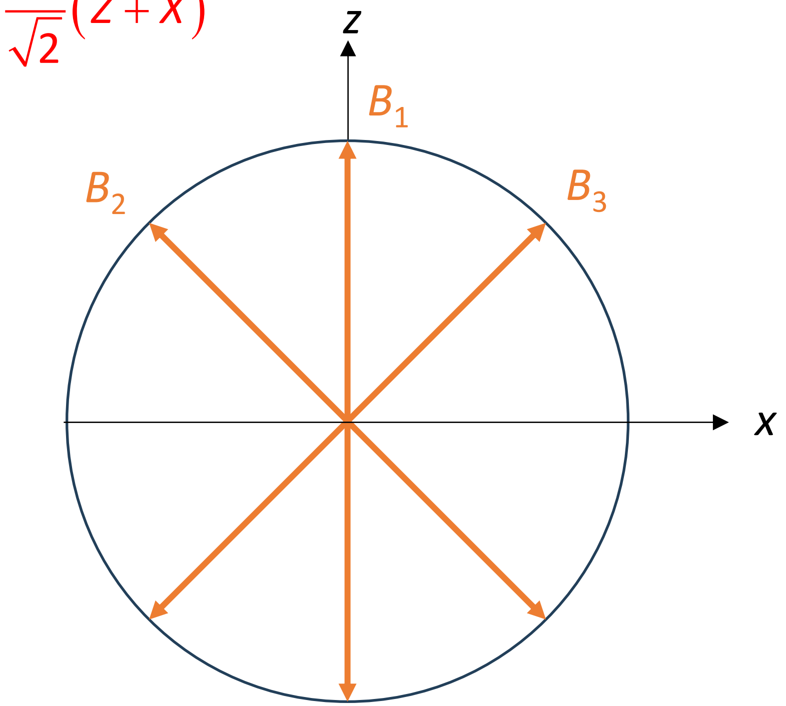


Bob

$B_1 = Z$

$B_2 = \frac{1}{\sqrt{2}}(Z - X)$

$B_3 = \frac{1}{\sqrt{2}}(Z + X)$



E91 QKD Protocol

- Bob can measure in the Z basis, given by B_1, or in the rotated basis
  - > $B_2 = \frac{1}{\sqrt{2}}(Z - X)$, which is proportional to Z minus X, or in the basis
  - > $B_3 = \frac{1}{\sqrt{2}}(Z + X)$, which is proportional to Z plus X

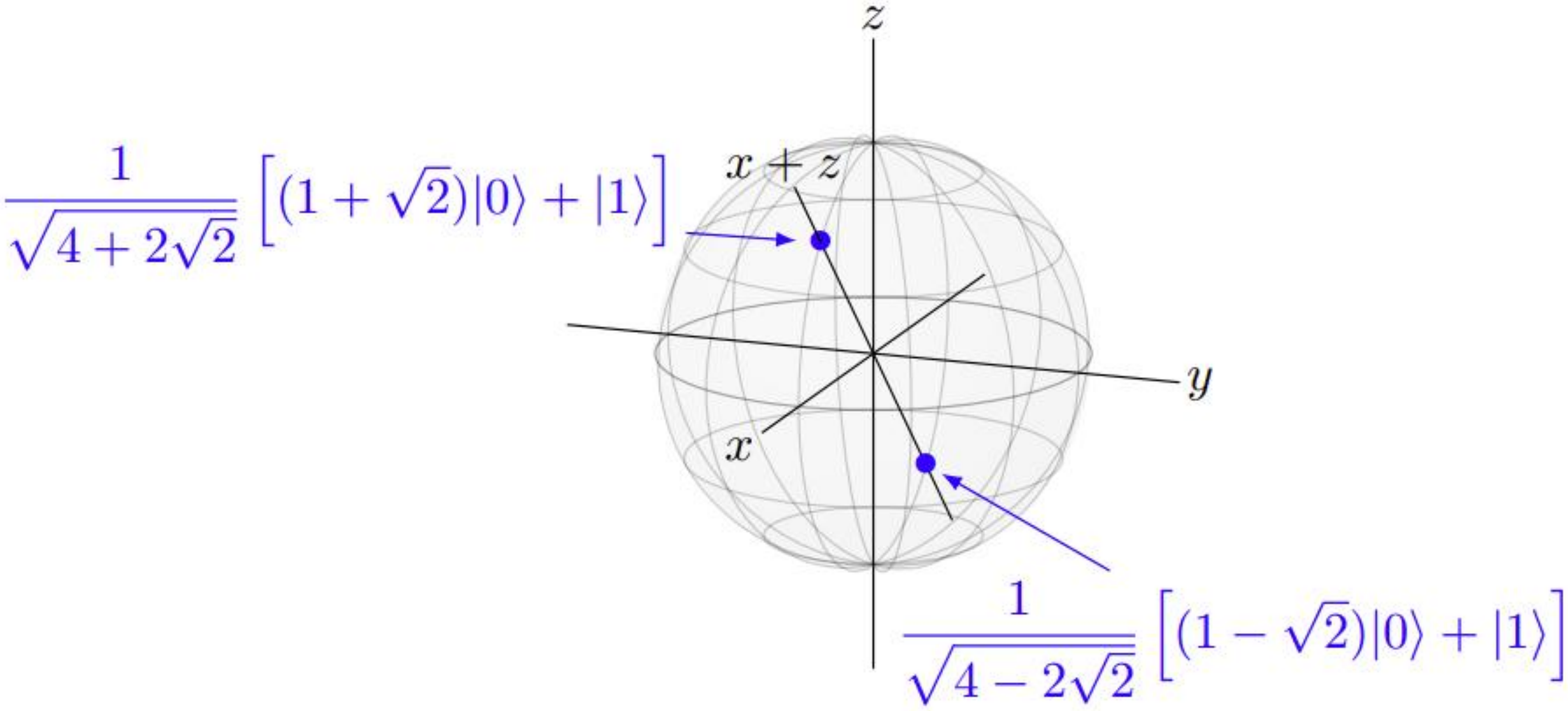
- B_3 basis contains the following two vectors

$$\left\{ \frac{1}{\sqrt{4+2\sqrt{2}}}\left[\left(1+\sqrt{2}\right)|0\rangle + |1\rangle\right], \frac{1}{\sqrt{4-2\sqrt{2}}}\left[\left(1-\sqrt{2}\right)|0\rangle + |1\rangle\right] \right\},$$

which are the eigenvectors of $\frac{1}{\sqrt{2}}(Z+X)$ corresponding to eigenvalues +1 and -1

E91 QKD Protocol

- The eigenvectors above appear on the Bloch sphere on the *x* + *z* axis



$$\frac{1}{\sqrt{4+2\sqrt{2}}}\left[(1+\sqrt{2})|0\rangle + |1\rangle\right]$$

$$\frac{1}{\sqrt{4-2\sqrt{2}}}\left[(1-\sqrt{2})|0\rangle + |1\rangle\right]$$

E91 QKD Protocol

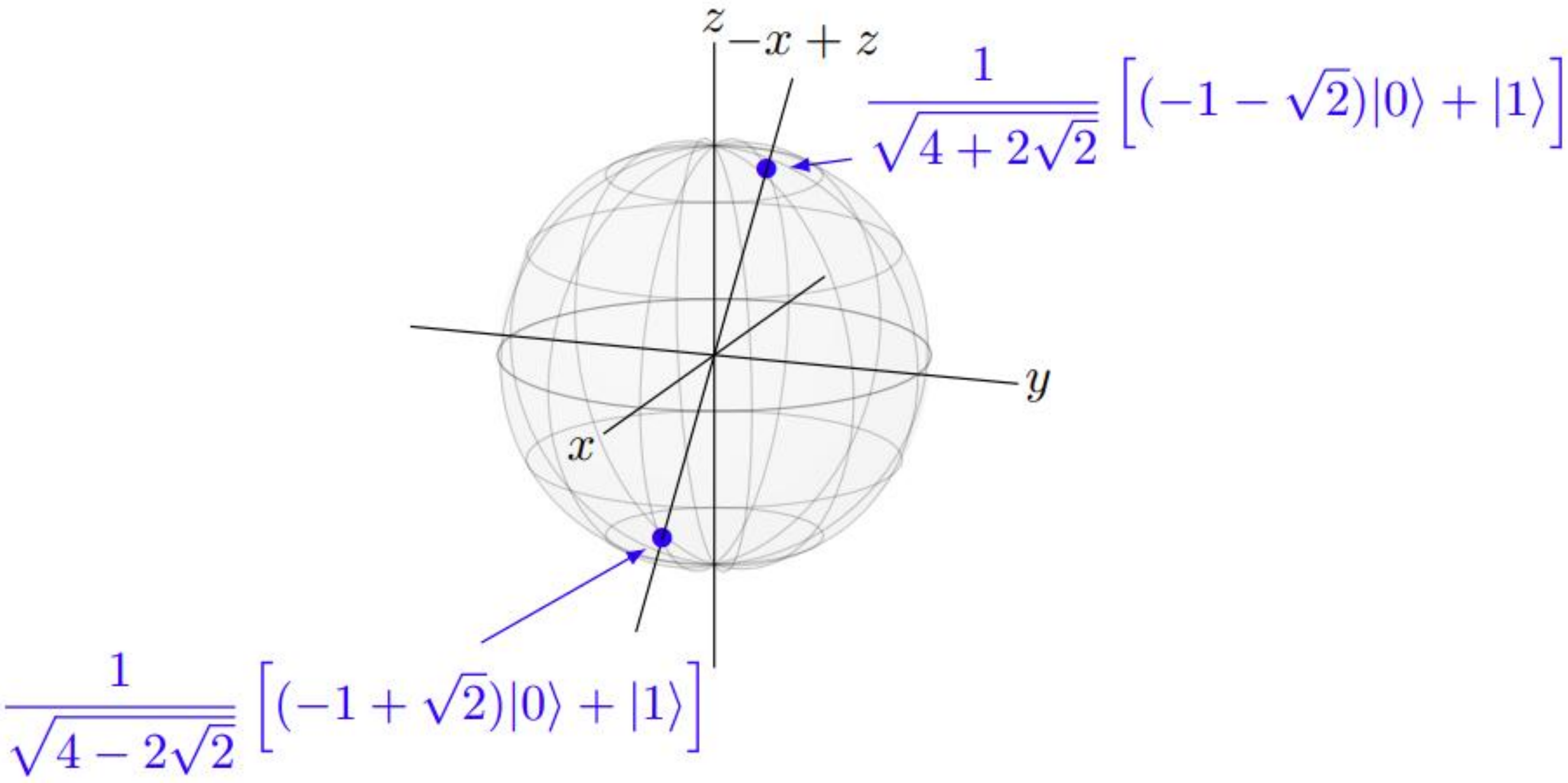
- B_2 basis, i.e., the other basis for Bob, contains the following two vectors:

$$\left\{ \frac{1}{\sqrt{4+2\sqrt{2}}}\left[\left(-1-\sqrt{2}\right)|0\rangle + |1\rangle\right], \frac{1}{\sqrt{4-2\sqrt{2}}}\left[\left(-1+\sqrt{2}\right)|0\rangle + |1\rangle\right] \right\},$$

which are the eigenvectors of $\frac{1}{\sqrt{2}}(Z-X)$ corresponding to eigenvalues +1 and -1

E91 QKD Protocol

- The eigenvectors above appear on the Bloch sphere on the *-x+z* axis


z
$-x+z$
$\frac{1}{\sqrt{4+2\sqrt{2}}}\left[(-1-\sqrt{2})|0\rangle+|1\rangle\right]$
y
x
$\frac{1}{\sqrt{4-2\sqrt{2}}}\left[(-1+\sqrt{2})|0\rangle+|1\rangle\right]$

E91 QKD Protocol

- **Question:** why do we have **three** different measurements for Alice and **three** different measurements for Bob rather than two as we had in the previous protocol *BB84*?
- Notice that some of these measurements are overlapping

Alice	Bob
$A_1 = Z$	$B_1 = Z$
$A_2 = X$	$B_2 = \frac{1}{\sqrt{2}}(Z - X)$
$A_3 = \frac{1}{\sqrt{2}}(Z + X)$	$B_3 = \frac{1}{\sqrt{2}}(Z + X)$

E91 QKD Protocol

- Remember, we said that if both Alice and Bob measure the entangled state on the same basis, they can use the classical outcomes, to generate and establish a classical correlated random key
- This follows similar logic to *BB84*
- Data from the basis choices (A_1, B_1) or (A_3, B_3) can be used for key generation

	Alice	Bob
	$A_1 = Z$	$B_1 = Z$
	$A_3 = \frac{1}{\sqrt{2}}(Z + X)$	$B_3 = \frac{1}{\sqrt{2}}(Z + X)$

E91 QKD Protocol

- On the other hand, we need some **rotated bases** to compute the *CHSH* expression, *S*, and see if it violates the classical *CHSH inequality* to establish that Alice and Bob are really sharing an entangled state
- For this calculation, we use the basis choices

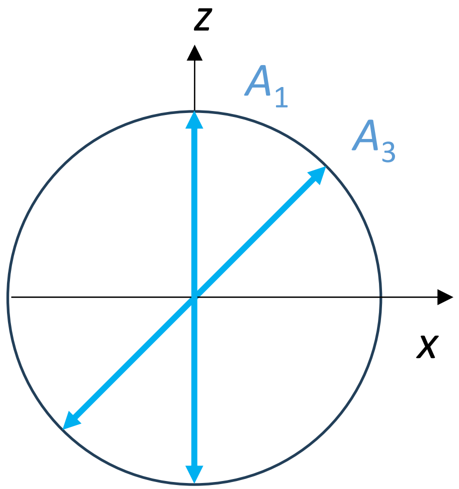
$$(A_1, B_3), (A_1, B_2), (A_2, B_2), (A_2, B_3)$$

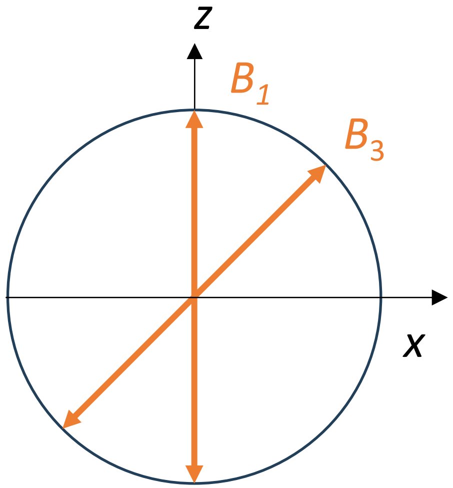
which we visualize by the following picture

$$\begin{tikzcd}
A_1 \arrow[r, blue] \arrow[dr, blue] & B_3 \\
A_2 \arrow[r, red] \arrow[ur, red] & B_2
\end{tikzcd}$$

E91 QKD Protocol

- To establish the key, Alice measures either in A_1 or A_3 and Bob measures accordingly in B_1 or B_3
- They *randomly* measure their multiple copies of entangled states provided by Charlie, and then they exchange information about the basis of their measurements





E91 QKD Protocol

- As an example, Alice and Bob made the following random choices regarding their measurement bases

Alice's Basis	A_1	A_3	A_1	A_2	A_3	A_3	A_1	A_3
Bob's Basis	B_2	B_3	B_1	B_2	B_1	B_2	B_1	B_3

E91 QKD Protocol

- *They exchange information about these bases,* and they look at the places where their *measurement basis choice coincide*

Alice's Basis	A_1	A_3	A_1	A_2	A_3	A_3	A_1	A_3
Bob's Basis	B_2	B_3	B_1	B_2	B_1	B_2	B_1	B_3

- Here, Alice measures A_1 and Bob measures B_1, meaning both of them measured in the Z basis
- If they do that, as we saw, they get anti-correlated outcomes, which they can use to generate a correlated classical key

E91 QKD Protocol

Alice's Basis	A_1	A_3	A_1	A_2	A_3	A_3	A_1	A_3
Bob's Basis	B_2	B_3	B_1	B_2	B_1	B_2	B_1	B_3

- Over here, they measure both in the rotated A_3 and B_3 basis
- The outcomes of Alice's and Bob's measurements reported in the red colored columns, will contribute to the generation of the key

E91 QKD Protocol

Alice’s Basis	A_1	A_3	A_1	A_2	A_3	A_3	A_1	A_3
Bob’s Basis	B_2	B_3	B_1	B_2	B_1	B_2	B_1	B_3

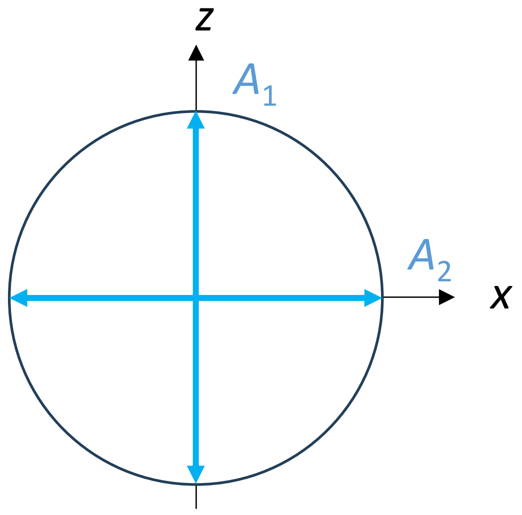
- The red cases where Alice and Bob chose the same measurement basis take care of generating the key
- In some other cases, they will not measure in bases that coincide
- They don’t discard these results, but instead use them to compute the *CHSH* expression and check for a violation of the classical bound on the *CHSH* inequality

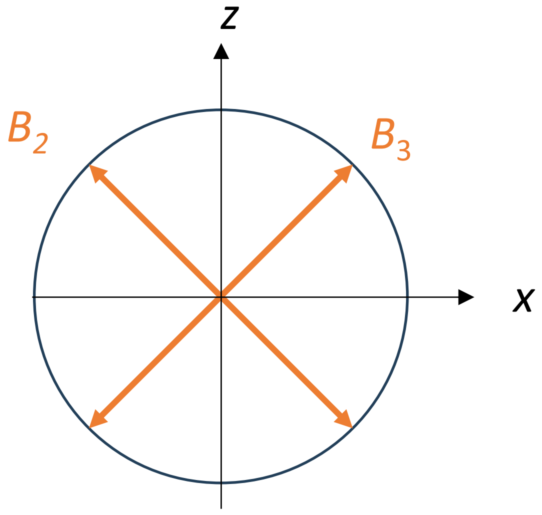
E91 QKD Protocol

- In particular, they look for scenarios where both of them measure

$$(A_1, B_2), (A_1, B_3), (A_2, B_2), (A_2, B_3)$$

- Visually it does correspond to Alice looking for cases where she measures in the Z basis and the X basis, and Bob measures in these rotated bases B_2 and B_3





E91 QKD Protocol

- Then they use those measurement results to compute the following expression

$$S = \left| \langle A_1 B_2 \rangle + \langle A_1 B_3 \rangle + \langle A_2 B_2 \rangle - \langle A_2 B_3 \rangle \right|$$

  which is just the sum of expectation values where Alice measured A_1 and Bob measured B_2, Alice measured A_1 and Bob measured B_3, and so on

- Therefore, Alice and Bob don't need to discard any information like in BB84, but they get to use it to calculate either the *secret correlated key* or the *CHSH violation*

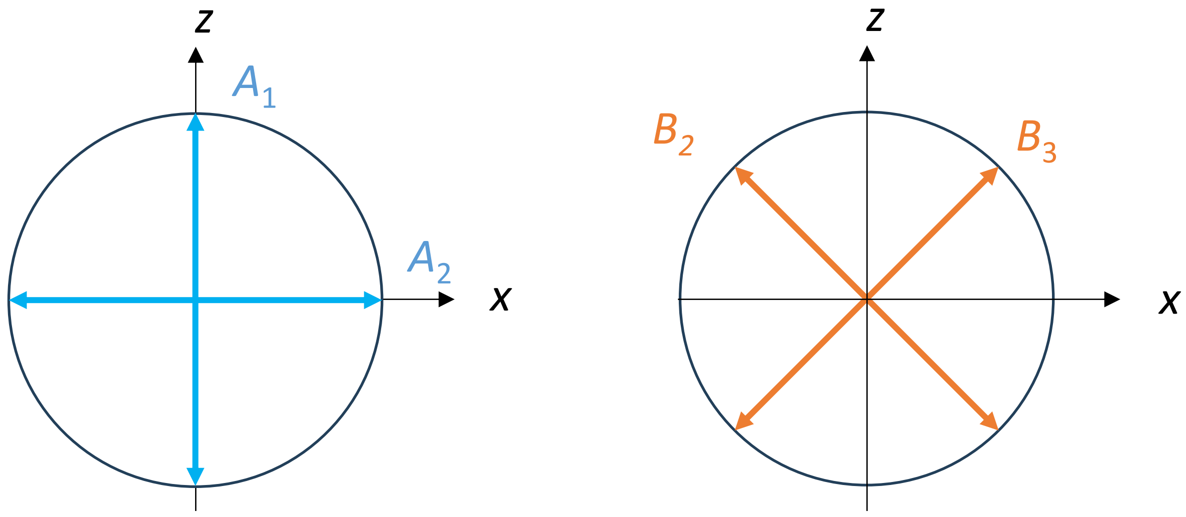
- If Alice and Bob obtain a *CHSH* expression of less or equal to two, they say *"Okay, we cannot conclude that we have an entangled state or not, but it's safer to just abort"*

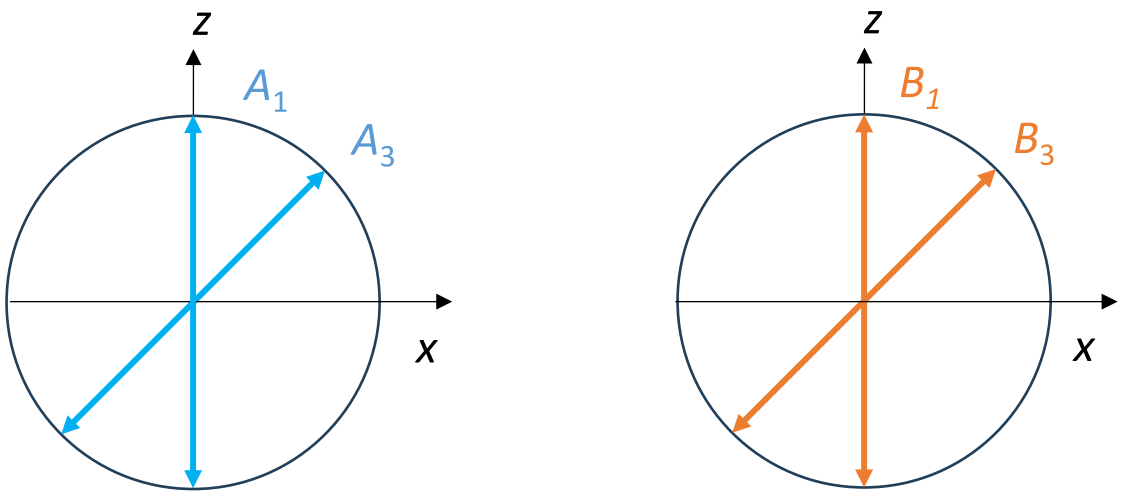
E91 QKD Protocol

- Remember, we said that *monogamy of entanglement* ensures that if Alice and Bob have an entangled state, then Eve is not strongly correlated with either of them
- In particular, if they have a *maximally entangled state*, then Eve is not correlated with Alice and Bob at all, so they are looking for as strong a violation as they can get
- Therefore, if they have a *CHSH* expression larger than two, then they conclude, *“Yes, we are sharing an entangled state, therefore we can proceed with the protocol"*

E91 QKD Protocol

- The discussion above can be summarized as follows





The basis choices (A_1, B_3), (A_1, B_2), (A_2, B_2), (A_2, B_3) to compute the *CHSH* expression

$$S = \left| \langle A_1 B_2 \rangle + \langle A_1 B_3 \rangle + \langle A_2 B_2 \rangle - \langle A_2 B_3 \rangle \right|$$

If $S \le 2$, ABORT!

If $S > 2$, Proceed.

The basis choices (A_1, B_1) or (A_3, B_3) used for key generation

E91 QKD Protocol

- So far, we have considered the case where everything was ideal, with no noise
- But what happens in the real life, where noise is always present? How does noise affect the E91 protocol?
- In real life, the CHSH value **will not equal exactly** $\mathbf{2\sqrt{2}}$
- In real life Alice and Bob will not be able to generate a perfectly correlated key, meaning that either **noise** or the **tinkering of Eve** will introduce some inconsistencies into the key, and therefore the keys constructed by Alice and Bob will be nearly identical

E91 QKD Protocol

- Even if Eve is not trying to actively eavesdrop and disrupt the protocol, still due to inherent noise in the system, these keys will not be perfectly correlated
- Alice and Bob have to decide on the acceptable security risk even if the keys are not perfectly correlated
- They have to agree "okay, if the correlation is not one hundred percent, but it's very, we can still use this to do something useful, and use it for secret communication"
- If they agree to this principle, then they have to engage in two more protocols

E91 QKD Protocol

- One is called the ***information reconciliation***, which takes the initial secret key that is not perfectly correlated and produces a more correlated key
- It increases the correlation between the secret bit strings obtained by Alice and Bob.
- As cryptosystems are generally designed so that a single bit difference in the keys changes half of the bits in the encrypted message (A characteristic sometimes called the avalanche effect or strict avalanche criterion by cryptographers.), they require that exactly the same key be used at both ends.

E91 QKD Protocol

- Alice and Bob can also perform something known as ***privacy amplification***, where they take their generated secret key and produce a shorter, more secure key
- Privacy amplification is a procedure that attempts to eliminate any possible correlation with Eve