Quantum Computation (CO484)

Quantum Cryptography with No Cloning

Herbert Wiklicky

herbert@doc.ic.ac.uk

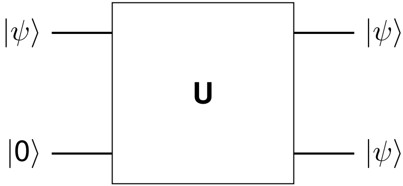
Autumn 2017

Cloning of Qubits?

Is it possible to create a second copy of a general qubit $|\psi\rangle$ using a unitary operation **U**.

Cloning of Qubits?

Is it possible to create a second copy of a general qubit $|\psi\rangle$ using a unitary operation **U**.



Theorem (No Cloning Theorem)

The exists no unitary transformation **U** *such that*

$$\mathbf{U}\,|\psi\rangle\,|0\rangle = |\psi\rangle\,|\psi\rangle$$

for all qubits $|\psi\rangle \in \mathbb{C}^2$.

Argument

Consider **two** qubits $|\psi\rangle$ and $|\phi\rangle$.

Argument

Consider **two** qubits $|\psi\rangle$ and $|\phi\rangle$.Then by linearity:

$$\begin{aligned} \mathbf{U}(\alpha\,|\psi\rangle + \beta\,|\phi\rangle)\,|0\rangle &= \alpha\mathbf{U}(|\psi\rangle)\,|0\rangle + \beta\mathbf{U}(|\phi\rangle)\,|0\rangle \\ &= \alpha\,|\psi\rangle\,|\psi\rangle + \beta\,|\phi\rangle\,|\phi\rangle \end{aligned}$$

Argument

Consider **two** qubits $|\psi\rangle$ and $|\phi\rangle$.Then by linearity:

$$\begin{aligned}\mathbf{U}(\alpha|\psi\rangle+\beta|\phi\rangle)|0\rangle &= \alpha\mathbf{U}(|\psi\rangle)|0\rangle+\beta\mathbf{U}(|\phi\rangle)|0\rangle \\ &= \alpha|\psi\rangle|\psi\rangle+\beta|\phi\rangle|\phi\rangle\end{aligned}$$

but also if **U** is a cloning operator:

$$\begin{aligned}\mathbf{U}(\alpha|\psi\rangle+\beta|\phi\rangle)|0\rangle &= (\alpha|\psi\rangle+\beta|\phi\rangle)(\alpha|\psi\rangle+\beta|\phi\rangle) \\ &= \alpha^2|\psi\rangle|\psi\rangle+\beta^2|\phi\rangle|\phi\rangle \\ &\quad +\alpha\beta|\psi\rangle|\phi\rangle+\alpha\beta|\phi\rangle|\psi\rangle\end{aligned}$$

Argument

Consider **two** qubits $|\psi\rangle$ and $|\phi\rangle$.Then by linearity:

$$\begin{aligned}\mathbf{U}(\alpha|\psi\rangle+\beta|\phi\rangle)|0\rangle &= \alpha\mathbf{U}(|\psi\rangle)|0\rangle+\beta\mathbf{U}(|\phi\rangle)|0\rangle\\ &= \alpha|\psi\rangle|\psi\rangle+\beta|\phi\rangle|\phi\rangle\end{aligned}$$

but also if **U** is a cloning operator:

$$\begin{aligned}\mathbf{U}(\alpha|\psi\rangle+\beta|\phi\rangle)|0\rangle &= (\alpha|\psi\rangle+\beta|\phi\rangle)(\alpha|\psi\rangle+\beta|\phi\rangle)\\ &= \alpha^2|\psi\rangle|\psi\rangle+\beta^2|\phi\rangle|\phi\rangle\\ &\quad+\alpha\beta|\psi\rangle|\phi\rangle+\alpha\beta|\phi\rangle|\psi\rangle\end{aligned}$$

Only for $\alpha = 0$ or $\beta = 0$ we have

$$\begin{aligned}\alpha|\psi\rangle|\psi\rangle+\beta|\phi\rangle|\phi\rangle &= \alpha^2|\psi\rangle|\psi\rangle+\beta^2|\phi\rangle|\phi\rangle\\ &\quad+\alpha\beta|\psi\rangle|\phi\rangle+\alpha\beta|\phi\rangle|\psi\rangle\end{aligned}$$

Approximate Cloning?

Is it not even possible to **approximately** clone a qubit.

Approximate Cloning?

Is it not even possible to **approximately** clone a qubit.

Consider **two** qubits $|\psi\rangle$ and $|\phi\rangle$ with $0 < \langle\psi|\phi\rangle < 1$ such that

$$\mathbf{U}(|\psi\rangle \otimes |0\rangle) \approx |\psi\rangle \otimes |\psi\rangle \quad \text{and} \quad \mathbf{U}(|\phi\rangle \otimes |0\rangle) \approx |\phi\rangle \otimes |\phi\rangle$$

Approximate Cloning?

Is it not even possible to **approximately** clone a qubit.

Consider **two** qubits $|\psi\rangle$ and $|\phi\rangle$ with $0 < \langle\psi|\phi\rangle < 1$ such that

$$\mathbf{U}(|\psi\rangle \otimes |0\rangle) \approx |\psi\rangle \otimes |\psi\rangle \quad \text{and} \quad \mathbf{U}(|\phi\rangle \otimes |0\rangle) \approx |\phi\rangle \otimes |\phi\rangle$$

By unitarity – **U** preserving inner products – we get

$$(|\psi\rangle\,|0\rangle)^{\dagger}(|\phi\rangle\,|0\rangle) = \langle\psi|\phi\rangle\,\langle 0|0\rangle = \langle\psi|\phi\rangle \approx \langle\psi|\phi\rangle^{2}$$

Approximate Cloning?

Is it not even possible to **approximately** clone a qubit.

Consider **two** qubits $|\psi\rangle$ and $|\phi\rangle$ with $0 < \langle\psi|\phi\rangle < 1$ such that

$$\mathbf{U}(|\psi\rangle \otimes |0\rangle) \approx |\psi\rangle \otimes |\psi\rangle \quad \text{and} \quad \mathbf{U}(|\phi\rangle \otimes |0\rangle) \approx |\phi\rangle \otimes |\phi\rangle$$

By unitarity – **U** preserving inner products – we get

$$(|\psi\rangle\,|0\rangle)^{\dagger}(|\phi\rangle\,|0\rangle) = \langle\psi|\phi\rangle\,\langle 0|0\rangle = \langle\psi|\phi\rangle \approx \langle\psi|\phi\rangle^{2}$$

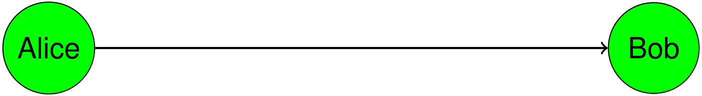
Thus $\langle\psi|\phi\rangle \approx 0$ or $\langle\psi|\phi\rangle \approx 1$.

Communication on Insecure Channels

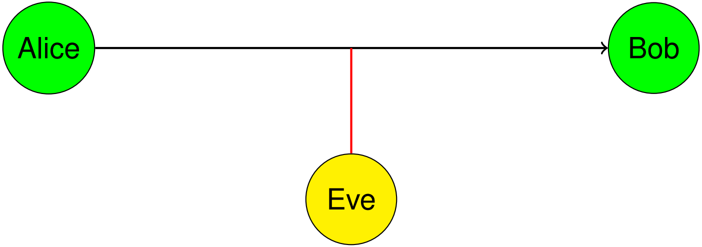
Alice

Bob

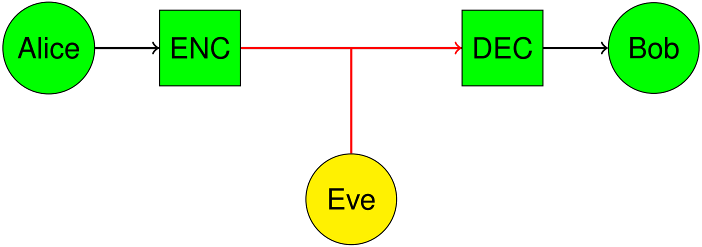
Communication on Insecure Channels



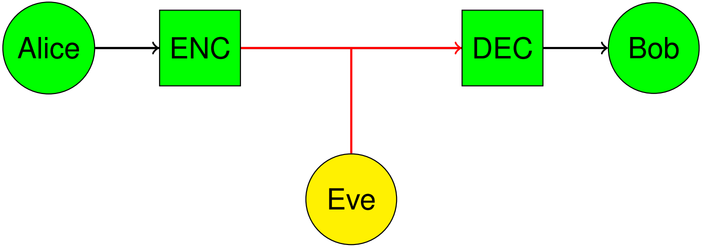
Communication on Insecure Channels



Communication on Insecure Channels



Communication on Insecure Channels



$$\begin{aligned} ENC(T, K_A) &= M \\ DEC(M, K_B) &= T \\ DEC(ENC(T, K_A), K_B) &= T \end{aligned}$$

One-Time-Pad or Vernam Cipher

Gilbert Sandford Vernam, 1917

Step 0. Alice and Bob share a common, random key K.

One-Time-Pad or Vernam Cipher

Gilbert Sandford Vernam, 1917

Step 0. Alice and Bob share a common, random key K.

Step 1. Alice calculates $M = T \oplus K$.

One-Time-Pad or Vernam Cipher

Gilbert Sandford Vernam, 1917

Step 0. Alice and Bob share a common, random key K.

Step 1. Alice calculates $M = T \oplus K$.

Step 2. Message M is sent along the insecure channel.

One-Time-Pad or Vernam Cipher

Gilbert Sandford Vernam, 1917

Step 0. Alice and Bob share a common, random key K.
Step 1. Alice calculates $M = T \oplus K$.
Step 2. Message M is sent along the insecure channel.
Step 3. Bob retrieves plain text $T = M \oplus K$.

One-Time-Pad or Vernam Cipher

Gilbert Sandford Vernam, 1917

Step 0. Alice and Bob share a common, random key K.
Step 1. Alice calculates $M = T \oplus K$.
Step 2. Message M is sent along the insecure channel.
Step 3. Bob retrieves plain text $T = M \oplus K$.

$$K = K_A = K_B$$

$$ENC(T, K) = DEC(T, K) = T \oplus K.$$

One-Time-Pad or Vernam Cipher

Gilbert Sandford Vernam, 1917

- Step 0. Alice and Bob share a common, random key K.
- Step 1. Alice calculates $M = T \oplus K$.
- Step 2. Message M is sent along the insecure channel.
- Step 3. Bob retrieves plain text $T = M \oplus K$.

$$K = K_A = K_B$$

$$ENC(T, K) = DEC(T, K) = T \oplus K.$$

Caveat: Never ever reuse random key K!

Example

T	0	1	1	0	1	1

Example

$$\begin{array}{cccccccc} T & & 0 & 1 & 1 & 0 & 1 & 1 \\ K & \oplus & 1 & 1 & 1 & 0 & 1 & 0 \end{array}$$

Example

$$\begin{array}{cccccccc}
T & & 0 & 1 & 1 & 0 & 1 & 1 \\
K & \oplus & 1 & 1 & 1 & 0 & 1 & 0 \\
\hline
M & & 1 & 0 & 0 & 0 & 0 & 1 \\
\\
 & & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\
\\
M & & 1 & 0 & 0 & 0 & 0 & 1
\end{array}$$

Example

$$\begin{array}{llcccccc}
T & & 0 & 1 & 1 & 0 & 1 & 1 \\
K & \oplus & 1 & 1 & 1 & 0 & 1 & 0 \\
\hline
M & & 1 & 0 & 0 & 0 & 0 & 1
\end{array}$$

$$\begin{array}{llcccccc}
 & & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow
\end{array}$$

$$\begin{array}{llcccccc}
M & & 1 & 0 & 0 & 0 & 0 & 1 \\
K & \oplus & 1 & 1 & 1 & 0 & 1 & 0
\end{array}$$

Example

$$\begin{array}{cccccccc}
T & & 0 & 1 & 1 & 0 & 1 & 1 \\
K & \oplus & 1 & 1 & 1 & 0 & 1 & 0 \\
\hline
M & & 1 & 0 & 0 & 0 & 0 & 1
\end{array}$$

$$\begin{array}{cccccccc}
 & & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow
\end{array}$$

$$\begin{array}{cccccccc}
M & & 1 & 0 & 0 & 0 & 0 & 1 \\
K & \oplus & 1 & 1 & 1 & 0 & 1 & 0 \\
\hline
T & & 0 & 1 & 1 & 0 & 1 & 1
\end{array}$$

Quantum Key Distribution

The **problem** with One-Time-Pads is **Key Distribution.**

Quantum Key Distribution

The **problem** with One-Time-Pads is **Key Distribution.**

Quantum Key Distribution aims to exploit quantum features in order to protect the keys, utilising:

Quantum Key Distribution

The **problem** with One-Time-Pads is **Key Distribution.**

Quantum Key Distribution aims to exploit quantum features in order to protect the keys, utilising:

No-Cloning. The message cannot be duplicated.

Quantum Key Distribution

The **problem** with One-Time-Pads is **Key Distribution.**

Quantum Key Distribution aims to exploit quantum features in order to protect the keys, utilising:

No-Cloning. The message cannot be duplicated.

Measurement. Observing the message changes it.

Quantum Key Distribution

The **problem** with One-Time-Pads is **Key Distribution.**

Quantum Key Distribution aims to exploit quantum features in order to protect the keys, utilising:

No-Cloning. The message cannot be duplicated.

Measurement. Observing the message changes it.

These quantum techniques aim in addressing two security aims:

Quantum Key Distribution

The **problem** with One-Time-Pads is **Key Distribution.**

Quantum Key Distribution aims to exploit quantum features in order to protect the keys, utilising:

No-Cloning. The message cannot be duplicated.

Measurement. Observing the message changes it.

These quantum techniques aim in addressing two security aims:

Authentication. Is sender really Alice?

Quantum Key Distribution

The **problem** with One-Time-Pads is **Key Distribution.**

Quantum Key Distribution aims to exploit quantum features in order to protect the keys, utilising:

No-Cloning. The message cannot be duplicated.

Measurement. Observing the message changes it.

These quantum techniques aim in addressing two security aims:

Authentication. Is sender really Alice?

Intrusion Detection. Is Eve eavesdropping?

BB84

Charles Bennett and Gilles Brassard 1984

The aim is to exchange a key K (e.g. a One-Time-Pad).

BB84

Charles Bennett and Gilles Brassard 1984

The aim is to exchange a key K (e.g. a One-Time-Pad).
Alice and Bob communicate over two insecure channels: a **quantum** channel and a **classical** one.

BB84

Charles Bennett and Gilles Brassard 1984

The aim is to exchange a key K (e.g. a One-Time-Pad).
Alice and Bob communicate over two insecure channels: a **quantum** channel and a **classical** one.
The protocol is based on the use of two (computational) bases:

$$\leftrightarrow\!\!\!\!\!\!\!\updownarrow\;=\{\left|\updownarrow\right\rangle,|\leftrightarrow\rangle\}=\{(1,0)^T,(0,1)^T\}$$

$$\nwarrow\!\!\!\!\searrow\!\!\!\!\!\!\!\swarrow\!\!\!\!\nearrow\;=\{|\searrow\rangle,|\nearrow\rangle\}=\{\frac{1}{\sqrt{2}}(-1,1)^T,\frac{1}{\sqrt{2}}(1,1)^T\}$$

BB84

Charles Bennett and Gilles Brassard 1984

The aim is to exchange a key *K* (e.g. a One-Time-Pad).
Alice and Bob communicate over two insecure channels: a **quantum** channel and a **classical** one.
The protocol is based on the use of two (computational) bases:

$$\updownarrow\!\!\!\!\leftrightarrow \; = \{\left|\updownarrow\right\rangle, |\leftrightarrow\rangle\} = \{(1,0)^T, (0,1)^T\}$$

$$\nwsearrow\!\!\!\!\neswarrow \; = \{|\nwsearrow\rangle, |\neswarrow\rangle\} = \{\frac{1}{\sqrt{2}}(-1,1)^T, \frac{1}{\sqrt{2}}(1,1)^T\}$$

Interpretation of messages in both basis

M	$\updownarrow\!\!\!\!\leftrightarrow$	$\nwsearrow\!\!\!\!\neswarrow$
0	$\lvert\leftrightarrow\rangle$	$\lvert\neswarrow\rangle$
1	$\left\lvert\updownarrow\right\rangle$	$\lvert\nwsearrow\rangle$

Measuring in Wrong Base

As long as Alice and Bob send and receive qubits in the same basis, Bob will always measure the same qubit Alice has sent.

Measuring in Wrong Base

As long as Alice and Bob send and receive qubits in the same basis, Bob will always measure the same qubit Alice has sent.

However, if they don't agree on the measurement base, Bob will make the wrong assumption of what Alice has sent.

Measuring in Wrong Base

As long as Alice and Bob send and receive qubits in the same basis, Bob will always measure the same qubit Alice has sent.

However, if they don't agree on the measurement base, Bob will make the wrong assumption of what Alice has sent.

Assume that Alice sends 0 encoded as $|⤢\rangle$ in the ⤧ basis but Bob uses ✥ to measure it:

Measuring in Wrong Base

As long as Alice and Bob send and receive qubits in the same basis, Bob will always measure the same qubit Alice has sent.

However, if they don't agree on the measurement base, Bob will make the wrong assumption of what Alice has sent.

Assume that Alice sends 0 encoded as |⤢⟩ in the ⤫ basis but Bob uses ✛ to measure it: In this case he will measure $|\updownarrow\rangle$ or $|\leftrightarrow\rangle$ with 50% chance, i.e. concludes with a 50:50 chance that Alice intended to send 0 or 1 respectively.

Measuring in Wrong Base

As long as Alice and Bob send and receive qubits in the same basis, Bob will always measure the same qubit Alice has sent.

However, if they don't agree on the measurement base, Bob will make the wrong assumption of what Alice has sent.

Assume that Alice sends 0 encoded as $|\neswarrow\rangle$ in the $\neswarrow\!\!\!\!\!\nwsearrow$ basis but Bob uses $\updownarrow\!\!\!\!\leftrightarrow$ to measure it: In this case he will measure $|\updownarrow\rangle$ or $|\leftrightarrow\rangle$ with 50% chance, i.e. concludes with a 50:50 chance that Alice intended to send 0 or 1 respectively.
This is due to the following obvious facts that:

$$\begin{aligned} |\nwsearrow\rangle &= \tfrac{1}{\sqrt{2}}(|\updownarrow\rangle - |\leftrightarrow\rangle) & \qquad |\updownarrow\rangle &= \tfrac{1}{\sqrt{2}}(|\neswarrow\rangle + |\nwsearrow\rangle) \\ |\neswarrow\rangle &= \tfrac{1}{\sqrt{2}}(|\updownarrow\rangle + |\leftrightarrow\rangle) & \qquad |\leftrightarrow\rangle &= \tfrac{1}{\sqrt{2}}(|\neswarrow\rangle - |\nwsearrow\rangle) \end{aligned}$$

BB84 Protocol

Step 1.a Alice chooses n random bits to send (e.g. to be used as One-Time-Pad).

BB84 Protocol

Step 1.a Alice chooses n random bits to send (e.g. to be used as One-Time-Pad).

Step 1.b Alice randomly chooses n times whether to use ✛ or ⤢ to encode each bit.

BB84 Protocol

Step 1.a Alice chooses *n* random bits to send (e.g. to be used as One-Time-Pad).

Step 1.b Alice randomly chooses *n* times whether to use + or × to encode each bit.

Step 2.a Alice encodes the bits accordingly in the bases and sends the qubits to Bob.

BB84 Protocol

Step 1.a Alice chooses *n* random bits to send (e.g. to be used as One-Time-Pad).

Step 1.b Alice randomly chooses *n* times whether to use + or × to encode each bit.

Step 2.a Alice encodes the bits accordingly in the bases and sends the qubits to Bob.

Step 2.b Bob randomly chooses *n* times whether to use + or × to measure the qubits he got and measures them.

BB84 Protocol

Step 1.a Alice chooses *n* random bits to send (e.g. to be used as One-Time-Pad).

Step 1.b Alice randomly chooses *n* times whether to use $+$ or $\times$ to encode each bit.

Step 2.a Alice encodes the bits accordingly in the bases and sends the qubits to Bob.

Step 2.b Bob randomly chooses *n* times whether to use $+$ or $\times$ to measure the qubits he got and measures them.

Step 3. Over the classical channel Alice and Bob compare which basis they used for each bit. If they agree they keep it otherwise they drop it.

BB84 Protocol

Step 1.a Alice chooses *n* random bits to send (e.g. to be used as One-Time-Pad).

Step 1.b Alice randomly chooses *n* times whether to use ✛ or ⤨ to encode each bit.

Step 2.a Alice encodes the bits accordingly in the bases and sends the qubits to Bob.

Step 2.b Bob randomly chooses *n* times whether to use ✛ or ⤨ to measure the qubits he got and measures them.

Step 3. Over the classical channel Alice and Bob compare which basis they used for each bit. If they agree they keep it otherwise they drop it.

Step 4.a Bob choose a part (e.g. half) of the transmitted bits (drops them) and compares them openly with Alice.

BB84 Protocol

- **Step 1.a** Alice chooses *n* random bits to send (e.g. to be used as One-Time-Pad).
- **Step 1.b** Alice randomly chooses *n* times whether to use ✛ or ✕ to encode each bit.
- **Step 2.a** Alice encodes the bits accordingly in the bases and sends the qubits to Bob.
- **Step 2.b** Bob randomly chooses *n* times whether to use ✛ or ✕ to measure the qubits he got and measures them.
- **Step 3.** Over the classical channel Alice and Bob compare which basis they used for each bit. If they agree they keep it otherwise they drop it.
- **Step 4.a** Bob choose a part (e.g. half) of the transmitted bits (drops them) and compares them openly with Alice.
- **Step 4.b** If these test bits do not agree (subject to transmission errors) Alice and Bob conclude that Eve was eavesdropping and abandon

Example

K_A	0	1	1	0	1	1	1	0	1	0	1	0

Example

K_A	0	1	1	0	1	1	1	0	1	0	1	0
B_A	+	+	×	+	+	+	×	+	×	×	×	+

Example

K_A	0	1	1	0	1	1	1	0	1	0	1	0
B_A	✛	✛	✕	✛	✛	✛	✕	✛	✕	✕	✕	✛
	↔	↕	⤡	↔	↕	↕	⤡	↔	⤡	⤢	⤡	↔

Example

K_A	0	1	1	0	1	1	1	0	1	0	1	0
B_A	✛	✛	✕	✛	✛	✛	✕	✛	✕	✕	✕	✛
	↔	↕	⤡	↔	↕	↕	⤡	↔	⤡	⤢	⤡	↔
	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
B_B	✕	✛	✕	✕	✛	✕	✛	✛	✕	✕	✕	✛

Example

K_A	0	1	1	0	1	1	1	0	1	0	1	0
B_A	✛	✛	✕	✛	✛	✛	✕	✛	✕	✕	✕	✛
	↔	↕	⤡	↔	↕	↕	⤡	↔	⤡	⤢	⤡	↔
	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
B_B	✕	✛	✕	✕	✛	✕	✛	✛	✕	✕	✕	✛
obs	⤢	↕	⤡	⤡	↕	⤢	↕	↔	⤡	⤢	⤡	↔

Example

K_A	0	1	1	0	1	1	1	0	1	0	1	0
B_A	✛	✛	✕	✛	✛	✛	✕	✛	✕	✕	✕	✛
	↔	↕	⤡	↔	↕	↕	⤡	↔	⤡	⤢	⤡	↔
	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
B_B	✕	✛	✕	✕	✛	✕	✛	✛	✕	✕	✕	✛
obs	⤢	↕	⤡	⤡	↕	⤢	↕	↔	⤡	⤢	⤡	↔
K_B	0	1	1	1	1	0	1	0	1	0	1	0

Example

K_A	0	1	1	0	1	1	1	0	1	0	1	0
B_A	✛	✛	✕	✛	✛	✛	✕	✛	✕	✕	✕	✛
	↔	↕	⤡	↔	↕	↕	⤡	↔	⤡	⤢	⤡	↔
	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
B_B	✕	✛	✕	✕	✛	✕	✛	✛	✕	✕	✕	✛
obs	⤢	↕	⤡	⤡	↕	⤢	↕	↔	⤡	⤢	⤡	↔
K_B	0	1	1	1	1	0	1	0	1	0	1	0
		√	√		√			√	√	√	√	√

Example

K_A	0	1	1	0	1	1	1	0	1	0	1	0
B_A	+	+	×	+	+	+	×	+	×	×	×	+
	↔	↕	⤡	↔	↕	↕	⤡	↔	⤡	⤢	⤡	↔
	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
B_B	×	+	×	×	+	×	+	+	×	×	×	+
obs	⤢	↕	⤡	⤡	↕	⤢	↕	↔	⤡	⤢	⤡	↔
K_B	0	1	1	1	1	0	1	0	1	0	1	0
		√	√		√			√	√	√	√	√
K		1	1		1			0	1	0	1	0

B92

Charles Bennett 1992

The idea is to use a **non-orthogonal** basis to encode 0 and 1, e.g.

$$B = \{|\leftrightarrow\rangle, |\swarrow\!\!\nearrow\rangle\} = \{(1,0)^T, \frac{1}{\sqrt{2}}(1,1)^T\}$$

B92

Charles Bennett 1992

The idea is to use a **non-orthogonal** basis to encode 0 and 1, e.g.

$$B = \{|\leftrightarrow\rangle, |\swarrow\!\!\!\nearrow\rangle\} = \{(1,0)^T, \frac{1}{\sqrt{2}}(1,1)^T\}$$

Step 1. Alice chooses n random bits and encodes them, e.g. $0 \equiv |\leftrightarrow\rangle$ and $1 \equiv |\swarrow\!\!\!\nearrow\rangle$ and send these qubits to Bob.

B92

Charles Bennett 1992

The idea is to use a **non-orthogonal** basis to encode 0 and 1, e.g.

$$B = \{|\leftrightarrow\rangle, |\swarrow\!\!\!\!\nearrow\rangle\} = \{(1,0)^T, \frac{1}{\sqrt{2}}(1,1)^T\}$$

Step 1. Alice chooses *n* random bits and encodes them, e.g. $0 \equiv |\leftrightarrow\rangle$ and $1 \equiv |\swarrow\!\!\!\!\nearrow\rangle$ and send these qubits to Bob.

Step 2. Bob measures these qubits in randomly chosen base $\leftrightarrow\!\!\!\!\!\!\updownarrow$ or $\nwarrow\!\!\!\!\nearrow\!\!\!\!\!\!\swarrow\!\!\!\!\searrow$.

B92

Charles Bennett 1992

The idea is to use a **non-orthogonal** basis to encode 0 and 1, e.g.

$$B = \{ |\leftrightarrow\rangle, |\text{⤢}\rangle \} = \{(1,0)^T, \frac{1}{\sqrt{2}}(1,1)^T\}$$

Step 1. Alice chooses n random bits and encodes them, e.g. $0 \equiv |\leftrightarrow\rangle$ and $1 \equiv |\text{⤢}\rangle$ and send these qubits to Bob.

Step 2. Bob measures these qubits in randomly chosen base $\leftrightarrow\!\!\!\!\!\updownarrow$ or ⤡⤢ .

Step 3. Bob tells Alice over an open classical which qubits he considers **ambiguous** in order to drop them.

B92

Charles Bennett 1992

The idea is to use a **non-orthogonal** basis to encode 0 and 1, e.g.

$$B = \{|\leftrightarrow\rangle, |\swarrow\!\!\!\!\!\nearrow\rangle\} = \{(1,0)^T, \frac{1}{\sqrt{2}}(1,1)^T\}$$

Step 1. Alice chooses n random bits and encodes them, e.g. $0 \equiv |\leftrightarrow\rangle$ and $1 \equiv |\swarrow\!\!\!\!\!\nearrow\rangle$ and send these qubits to Bob.

Step 2. Bob measures these qubits in randomly chosen base $\leftrightarrow\!\!\!\!\!\!\updownarrow$ or $\swarrow\!\!\!\!\!\nearrow\!\!\!\!\!\nwarrow\!\!\!\!\!\searrow$.

Step 3. Bob tells Alice over an open classical which qubits he considers **ambiguous** in order to drop them.

Again – as in BB84 – some bits can be sacrificed to see if an extensive number of “transmission errors” indicates that Eve was eavesdropping and abandon transmission.

Ambiguous Bits

When Bob measures the qubits received from Alice he will conclude that certain observations are inconclusive.

Ambiguous Bits

When Bob measures the qubits received from Alice he will conclude that certain observations are inconclusive.

Using ✥. If Bob observes

Ambiguous Bits

When Bob measures the qubits received from Alice he will conclude that certain observations are inconclusive.

Using $\leftrightarrow\!\!\!\!\!\updownarrow$. If Bob observes

$|\updownarrow\rangle$ Bob knows that Alice sent 1 $\equiv |⤢\rangle$.

Ambiguous Bits

When Bob measures the qubits received from Alice he will conclude that certain observations are inconclusive.

Using $\leftrightarrow\!\!\!\!\!\!\updownarrow$. If Bob observes

$|\updownarrow\rangle$ Bob knows that Alice sent $1 \equiv |\nearrow\!\!\!\!\!\swarrow\rangle$.

$|\leftrightarrow\rangle$ Bob drops this bit.

Ambiguous Bits

When Bob measures the qubits received from Alice he will conclude that certain observations are inconclusive.

Using ✛. If Bob observes

- $|\updownarrow\rangle$ Bob knows that Alice sent $1 \equiv |⤢\rangle$.
- $|\leftrightarrow\rangle$ Bob drops this bit.

Using ⤧. If Bob observes

Ambiguous Bits

When Bob measures the qubits received from Alice he will conclude that certain observations are inconclusive.

Using ↕↔. If Bob observes

|↕⟩ Bob knows that Alice sent 1 ≡ |⤢⟩.
|↔⟩ Bob drops this bit.

Using ⤢⤡. If Bob observes

|⤡⟩ Bob knows that Alice sent 0 ≡ |↔⟩.

Ambiguous Bits

When Bob measures the qubits received from Alice he will conclude that certain observations are inconclusive.

Using ✥. If Bob observes

$|\updownarrow\rangle$ Bob knows that Alice sent $1 \equiv |⤢\rangle$.
$|\leftrightarrow\rangle$ Bob drops this bit.

Using ⤫. If Bob observes

$|⤡\rangle$ Bob knows that Alice sent $0 \equiv |\leftrightarrow\rangle$.
$|⤢\rangle$ Bob drops this bit.

Ambiguous Bits

When Bob measures the qubits received from Alice he will conclude that certain observations are inconclusive.

Using +. If Bob observes

- |↕⟩ Bob knows that Alice sent 1 ≡ |⤢⟩.
- |↔⟩ Bob drops this bit.

Using ×. If Bob observes

- |⤡⟩ Bob knows that Alice sent 0 ≡ |↔⟩.
- |⤢⟩ Bob drops this bit.

In the average three quarters of the qubits have to be discarded.

Example

K_A	0	0	1	0	1	0	1	0	1	1	1	0

Example

K_A	0	0	1	0	1	0	1	0	1	1	1	0
	↔	↔	⤢	↔	⤢	↔	⤢	↔	⤢	⤢	⤢	↔

Example

K_A	0	0	1	0	1	0	1	0	1	1	1	0
	↔	↔	⤢	↔	⤢	↔	⤢	↔	⤢	⤢	⤢	↔
	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓

Example

K_A	0	0	1	0	1	0	1	0	1	1	1	0
	↔	↔	⤢	↔	⤢	↔	⤢	↔	⤢	⤢	⤢	↔
	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
B_B	⤫	✥	⤫	⤫	✥	⤫	✥	✥	⤫	✥	⤫	✥

Example

K_A	0	0	1	0	1	0	1	0	1	1	1	0
	↔	↔	⤢	↔	⤢	↔	⤢	↔	⤢	⤢	⤢	↔
	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
B_B	✕	✛	✕	✕	✛	✕	✛	✛	✕	✛	✕	✛
obs	⤡	↔	⤢	⤡	↕	⤡	↔	↔	⤢	↕	⤢	↔

Example

K_A	0	0	1	0	1	0	1	0	1	1	1	0
	↔	↔	⤢	↔	⤢	↔	⤢	↔	⤢	⤢	⤢	↔
	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
B_B	✕	✛	✕	✕	✛	✕	✛	✛	✕	✛	✕	✛
obs	⤡	↔	⤢	⤡	↕	⤡	↔	↔	⤢	↕	⤢	↔
K_B	0	?	?	0	1	0	?	?	?	1	?	?

Example

K_A	0	0	1	0	1	0	1	0	1	1	1	0
	↔	↔	⤢	↔	⤢	↔	⤢	↔	⤢	⤢	⤢	↔
	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
B_B	✕	✛	✕	✕	✛	✕	✛	✛	✕	✛	✕	✛
obs	⤡	↔	⤢	⤡	↕	⤡	↔	↔	⤢	↕	⤢	↔
K_B	0	?	?	0	1	0	?	?	?	1	?	?
	√			√	√	√				√		

Example

K_A	0	0	1	0	1	0	1	0	1	1	1	0
	↔	↔	⤢	↔	⤢	↔	⤢	↔	⤢	⤢	⤢	↔
	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
B_B	×	+	×	×	+	×	+	+	×	+	×	+
obs	⤡	↔	⤢	⤡	↕	⤡	↔	↔	⤢	↕	⤢	↔
K_B	0	?	?	0	1	0	?	?	?	1	?	?
	√			√	√	√				√		
K	0			0	1	0				1		

EPR

Artur Ekert 1991

The idea is to distribute a key K via pairs of entangled states, for example the **Bell states**:

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

EPR

Artur Ekert 1991

The idea is to distribute a key K via pairs of entangled states, for example the **Bell states**:

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

The key K is effectively generated only after the distribution of these states to Alice and Bob. They do this independently but entanglement guarantees they obtain the same key.

EPR

Artur Ekert 1991

The idea is to distribute a key K via pairs of entangled states, for example the **Bell states**:

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

The key K is effectively generated only after the distribution of these states to Alice and Bob. They do this independently but entanglement guarantees they obtain the same key.

This protocol is inspired by the Einstein-Podolsky-Rosen (EPR, 1935) Gedanken-Experiment.

EPR Protocol

EPR Protocol

Step 1. A random sequence of entangled 2-qubit states – e.g. $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ – is created.
For each such state one of the qubits is given to Alice and Bob, respectively.

EPR Protocol

Step 1. A random sequence of entangled 2-qubit states – e.g. $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ – is created.
For each such state one of the qubits is given to Alice and Bob, respectively.

Step 2. Bob and Alice measure each of their qubits in a randomly chosen base ✛ or ⤧ .

EPR Protocol

Step 1. A random sequence of entangled 2-qubit states – e.g. $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ – is created.
For each such state one of the qubits is given to Alice and Bob, respectively.

Step 2. Bob and Alice measure each of their qubits in a randomly chosen base ✥ or ⤫ .

Step 3. Over the classical channel Alice and Bob compare which basis they used for each bit. If they agree they keep it otherwise they drop it.

EPR Protocol

Step 1. A random sequence of entangled 2-qubit states – e.g. $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ – is created.
For each such state one of the qubits is given to Alice and Bob, respectively.

Step 2. Bob and Alice measure each of their qubits in a randomly chosen base ✛ or ✕ .

Step 3. Over the classical channel Alice and Bob compare which basis they used for each bit. If they agree they keep it otherwise they drop it.

As in BB84 too many “transmission errors” indicate that Eve was eavesdropping and the transmission is abandoned.

EPR Protocol

Step 1. A random sequence of entangled 2-qubit states – e.g. $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ – is created.
For each such state one of the qubits is given to Alice and Bob, respectively.

Step 2. Bob and Alice measure each of their qubits in a randomly chosen base ✥ or ⤫ .

Step 3. Over the classical channel Alice and Bob compare which basis they used for each bit. If they agree they keep it otherwise they drop it.

As in BB84 too many “transmission errors” indicate that Eve was eavesdropping and the transmission is abandoned. Ekert proposed a more sophisticated eavesdropping detection (Bell’s theorem).

Example

B_A	×	×	+	+	×	+	×	+	+	×	+	×

Example

B_A	⤫	⤫	✥	✥	⤫	✥	⤫	✥	✥	⤫	✥	⤫
obs	⤢	⤡	↔	↕	⤢	↔	⤡	↔	↔	⤢	↔	⤢

Example

B_A	$\times$	$\times$	$+$	$+$	$\times$	$+$	$\times$	$+$	$+$	$\times$	$+$	$\times$
obs	⤢	⤡	↔	↕	⤢	↔	⤡	↔	↔	⤢	↔	⤢
K_A	0	1	0	1	0	0	1	0	0	0	0	0

Example

B_A	×	×	+	+	×	+	×	+	+	×	+	×
obs	⤢	⤡	↔	↕	⤢	↔	⤡	↔	↔	⤢	↔	⤢
K_A	0	1	0	1	0	0	1	0	0	0	0	0
B_B	×	+	+	×	×	+	+	+	+	×	×	+

Example

B_A	✕	✕	✛	✛	✕	✛	✕	✛	✛	✕	✛	✕
obs	⤢	⤡	↔	↕	⤢	↔	⤡	↔	↔	⤢	↔	⤢
K_A	0	1	0	1	0	0	1	0	0	0	0	0
B_B	✕	✛	✛	✕	✕	✛	✛	✛	✛	✕	✕	✛
obs	⤢	↔	↔	⤢	⤢	↔	↕	↔	↔	⤢	⤡	↔

Example

B_A	×	×	+	+	×	+	×	+	+	×	+	×
obs	⤢	⤡	↔	↕	⤢	↔	⤡	↔	↔	⤢	↔	⤢
K_A	0	1	0	1	0	0	1	0	0	0	0	0

B_B	×	+	+	×	×	+	+	+	+	×	×	+
obs	⤢	↔	↔	⤢	⤢	↔	↕	↔	↔	⤢	⤡	↔
K_B	0	0	0	0	0	0	1	0	0	0	1	0

Example

B_A	$\times$	$\times$	$+$	$+$	$\times$	$+$	$\times$	$+$	$+$	$\times$	$+$	$\times$
obs	⤢	⤡	↔	↕	⤢	↔	⤡	↔	↔	⤢	↔	⤢
K_A	0	1	0	1	0	0	1	0	0	0	0	0
B_B	$\times$	$+$	$+$	$\times$	$\times$	$+$	$+$	$+$	$+$	$\times$	$\times$	$+$
obs	⤢	↔	↔	⤢	⤢	↔	↕	↔	↔	⤢	⤡	↔
K_B	0	0	0	0	0	0	1	0	0	0	1	0
	$\surd$		$\surd$		$\surd$	$\surd$		$\surd$	$\surd$	$\surd$		

Example

B_A	×	×	+	+	×	+	×	+	+	×	+	×
obs	⤢	⤡	↔	↕	⤢	↔	⤡	↔	↔	⤢	↔	⤢
K_A	0	1	0	1	0	0	1	0	0	0	0	0
B_B	×	+	+	×	×	+	+	+	+	×	×	+
obs	⤢	↔	↔	⤢	⤢	↔	↕	↔	↔	⤢	⤡	↔
K_B	0	0	0	0	0	0	1	0	0	0	1	0
	√		√		√	√		√	√	√		
K	0		0		0	0		0	0	0		