08. Quantum Information Theory, Part I.

I. Qubits.

1. C-bits vs. Qubits

- *Classical Information Theory*

  C-bit = a state of a *classical* 2-state system: either "0" or "1".

  Physical examples:

  - The state of a mechanical on/off switch.
  - The state of an electronic device capable of distinguishing a voltage difference.

- *Quantum Information Theory*

  Qubit = a state of a *quantum* 2-state system: $|0\rangle$, $|1\rangle$, or $a|0\rangle + b|1\rangle$.

  Physical example:

  - The state of an electron in a spin basis (e.g.,$|hard\rangle$, $|soft\rangle$, or $a|hard\rangle + b|soft\rangle$).

***General form of a qubit*:**

$|Q\rangle = a|0\rangle + b|1\rangle, \quad \text{where } |a|^2 + |b|^2 = 1$

According to the Eigenvalue-eigenvector Rule:

- $|Q\rangle$ has no determinate value (of Hardness, say).
- It's value only becomes determinate (0 or 1; *hard* or *soft*) when we measure it.
- All we can say about $|Q\rangle$ is:
  (a) $\Pr(\textit{value of } |Q\rangle \text{ is } 0) = |a|^2$.
  (b) $\Pr(\textit{value of } |Q\rangle \text{ is } 1) = |b|^2$.

- *Common Claim*: A qubit $|Q\rangle = a|0\rangle + b|1\rangle$ encodes an arbitrarily large amount of information, but at most only one classical bit's worth of information in a qubit is *accessible*.

Why?

- a and b encode an arbitrarily large amount of information.
- But the outcome of a measurement performed on $|Q\rangle$ is its collapse to either $|0\rangle$ or $|1\rangle$, which each encode just one classical bit.

2. Transformations on Single Qubits

- Let $|0\rangle$ and $|1\rangle$ be given the matrix representations: $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ $\quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

- Define the following operators that act on $|0\rangle$ and $|1\rangle$:

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad Y = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Identity   *Negation*   *Negation/Phase-change*   *Phase-change*

$$I|0\rangle = |0\rangle \qquad X|0\rangle = |1\rangle \qquad Y|0\rangle = -|1\rangle \qquad Z|0\rangle = |0\rangle$$
$$I|1\rangle = |1\rangle \qquad X|1\rangle = |0\rangle \qquad Y|1\rangle = |0\rangle \qquad Z|1\rangle = -|1\rangle$$

$$H = \begin{pmatrix} \sqrt{\frac{1}{2}} & \sqrt{\frac{1}{2}} \\ \sqrt{\frac{1}{2}} & \sqrt{\frac{1}{2}} \end{pmatrix} \qquad \begin{aligned} H|0\rangle &= \sqrt{\tfrac{1}{2}}\big(|0\rangle + |1\rangle\big) \\ H|1\rangle &= \sqrt{\tfrac{1}{2}}\big(|0\rangle - |1\rangle\big) \end{aligned}$$

Hadamard operator: *Takes a basis qubit and outputs a superposition*

3. Transformations on Two Qubits

- Let $\{|0\rangle_1, |1\rangle_1\}$, $\{|0\rangle_2, |1\rangle_2\}$ be bases for the single qubit state spaces $\mathcal{H}_1$, $\mathcal{H}_2$.
- <u>*Then*</u>: A basis for the 2-qubit state space $\mathcal{H}_1 \otimes \mathcal{H}_2$ is given by

$$\{|0\rangle_1|0\rangle_2,\ |0\rangle_1|1\rangle_2,\ |1\rangle_1|0\rangle_2,\ |1\rangle_1|1\rangle_2\}$$

- Let these basis vectors be given the following matrix representations:

$$|0\rangle_1|0\rangle_2 = \begin{pmatrix}1\\0\\0\\0\end{pmatrix} \qquad |0\rangle_1|1\rangle_2 = \begin{pmatrix}0\\1\\0\\0\end{pmatrix} \qquad |1\rangle_1|0\rangle_2 = \begin{pmatrix}0\\0\\1\\0\end{pmatrix} \qquad |1\rangle_1|1\rangle_2 = \begin{pmatrix}0\\0\\0\\1\end{pmatrix}$$

- The *Controlled-NOT* 2-qubit operator is then defined by:

$$C_{NOT} = \begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}$$

$$C_{NOT}|0\rangle_1|0\rangle_2 = |0\rangle_1|0\rangle_2 \quad C_{NOT}|1\rangle_1|0\rangle_2 = |1\rangle_1|1\rangle_2$$
$$C_{NOT}|0\rangle_1|1\rangle_2 = |0\rangle_1|1\rangle_2 \quad C_{NOT}|1\rangle_1|1\rangle_2 = |1\rangle_1|0\rangle_2$$

Acts on two basis qubits.

- *Changes the second if the first is* $|1\rangle$.
- *Leaves the second unchanged otherwise.*

4. The No-Cloning Theorem

Claim: Unknown qubits cannot be "cloned".

- In particular, there is no (unitary, linear) operator U such that $U|v\rangle_1|0\rangle_2 = |v\rangle_1|v\rangle_2$, where $|v\rangle_1$ is an arbitrary qubit.

Proof: Suppose there is such a U.

- *Then*: $U|a\rangle_1|0\rangle_2 = |a\rangle_1|a\rangle_2$ and $U|b\rangle_1|0\rangle_2 = |b\rangle_1|b\rangle_2$, for qubits $|a\rangle_1$, $|b\rangle_1$.
- *Now*: Consider a qubit $|c\rangle_1 = \alpha|a\rangle_1 + \beta|b\rangle_1$. Since U is linear,

$$\begin{aligned} U|c\rangle_1|0\rangle_2 &= U(\alpha|a\rangle_1|0\rangle_2 + \beta|b\rangle_1|0\rangle_2) \\ &= (\alpha U|a\rangle_1|0\rangle_2 + \beta U|b\rangle_1|0\rangle_2) \\ &= \alpha|a\rangle_1|a\rangle_2 + \beta|b\rangle_1|b\rangle_2 \end{aligned}$$

- *But*: By definition, U acts on $|c\rangle_1$ according to:
$$U|c\rangle_1|0\rangle_2 = |c\rangle_1|c\rangle_2 = \alpha^2|a\rangle_1|a\rangle_2 + \alpha\beta|a\rangle_1|b\rangle_2 + \beta\alpha|b\rangle_1|a\rangle_2 + \beta^2|b\rangle_1|b\rangle_2.$$
- *So*: There cannot be such a U.

- *Note*: *Known* qubits (like $|1\rangle_1$) *can* be cloned (*ex*: $C_{NOT}|1\rangle_1|0\rangle_2 = |1\rangle_1|1\rangle_2$).

II. Quantum Cryptography.

Cryptography Basics

- *plaintext* = message to be encoded. (Private)
- *cryptotext* = encoded message. (Public)
- *encoding/decoding procedure* = procedure used to encode plaintext and decode cryptotext. (Public)
- *key* = device required to implement encoding/decoding procedure. (Private)

Example: One-time pad (Vernam 1917)

A	***B***	***C***	***D***	***E***	**...**	***X***	***Y***	***Z***	**?**	**,**	**.**	
00	01	02	03	04	...	23	24	25	26	27	28	29

alphanumeric convention

plaintext (private)

S H A K E N N O T S T I R R E D

18 07 00 10 04 13 26 13 14 19 26 18 19 08 17 17 04 03

key (private)

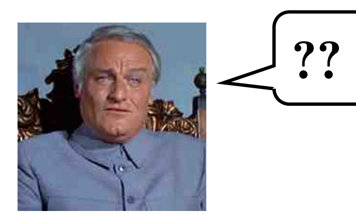
15 04 28 13 14 06 21 11 23 18 09 11 14 01 19 05 22 07

encoding/decoding procedure (public)

Add plaintext to key and take remainder after division by 30.

cryptotext (public)

03 11 28 23 18 19 17 24 07 07 05 29 03 09 06 22 26 10



- *Technical Result (Shannon 1949)*: One-time pad is guaranteed secure, as long as the key is completely *random*, has same length as plaintext, is never reused, and *is not intercepted by a third party*.

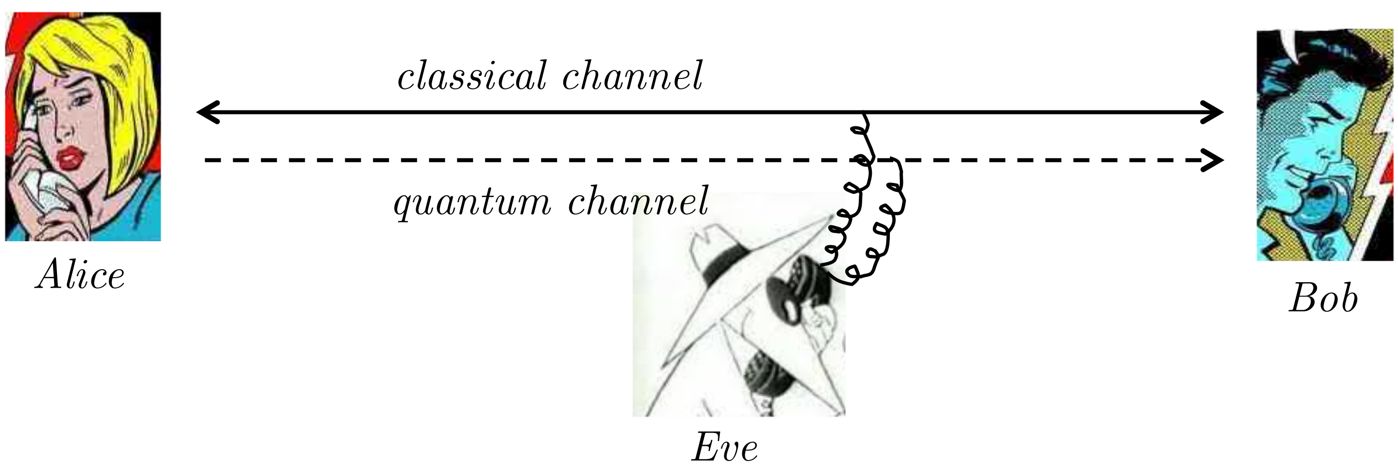
Quantum Key Distribution via Non-orthogonal States

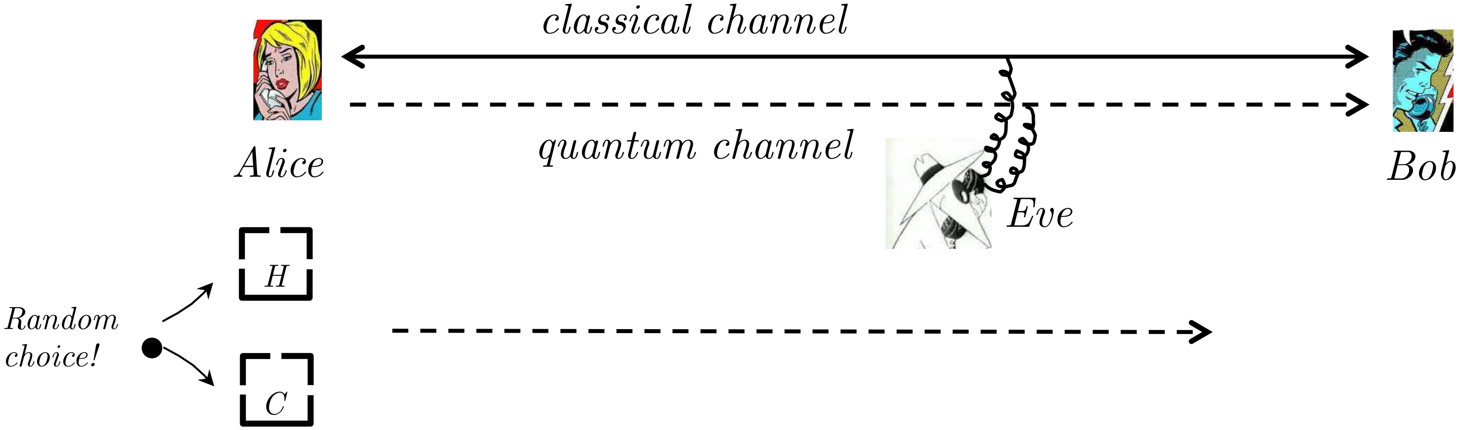
- *Goal*: To transmit a private key on possibly insecure channels.

- *Set-up:* Alice and Bob communicate through 2 public (insecure) channels:

  (i) A 2-way *classical channel* through which they exchange classical bits.

  (ii) A 1-way *quantum channel* through which Alice sends Bob qubits.





Protocol:

1. (a) Alice encodes a *random* sequence of bits as the *Color* or *Hardness* states of electrons: For each electron, she *randomly* picks a *Color* or *Hardness* box to put it through, and then selects the bit according to a public encryption chart.

   (b) Alice then generates a private list of the *value* of each electron and the correponding bit, and a public list of just the *property* of each electron.

   (c) Alice then sends her electrons to Bob *via* the quantum channel.

Public encryption chart

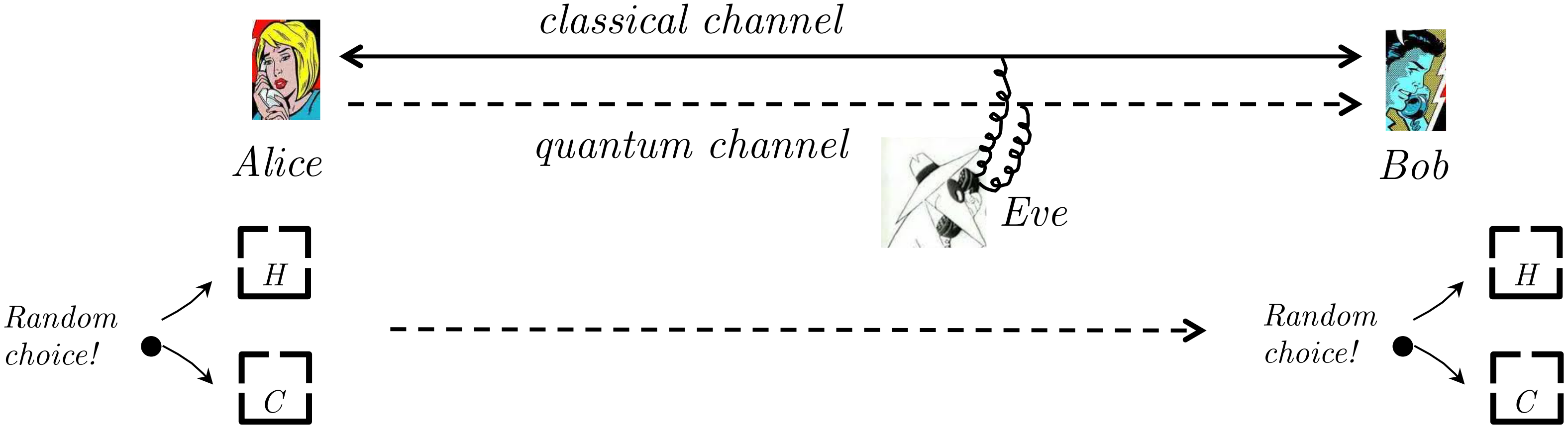
Hardness		*Color*	
$\vert hard\rangle$	$\Leftrightarrow$ 0	$\vert black\rangle$	$\Leftrightarrow$ 0
$\vert soft\rangle$	$\Leftrightarrow$ 1	$\vert white\rangle$	$\Leftrightarrow$ 1

Alice's private list

electron 1:	*hard*, 0
electron 2:	*black*, 0
etc...	

Alice's public list

electron 1: definite H-value
electron 2: definite C-value
etc...



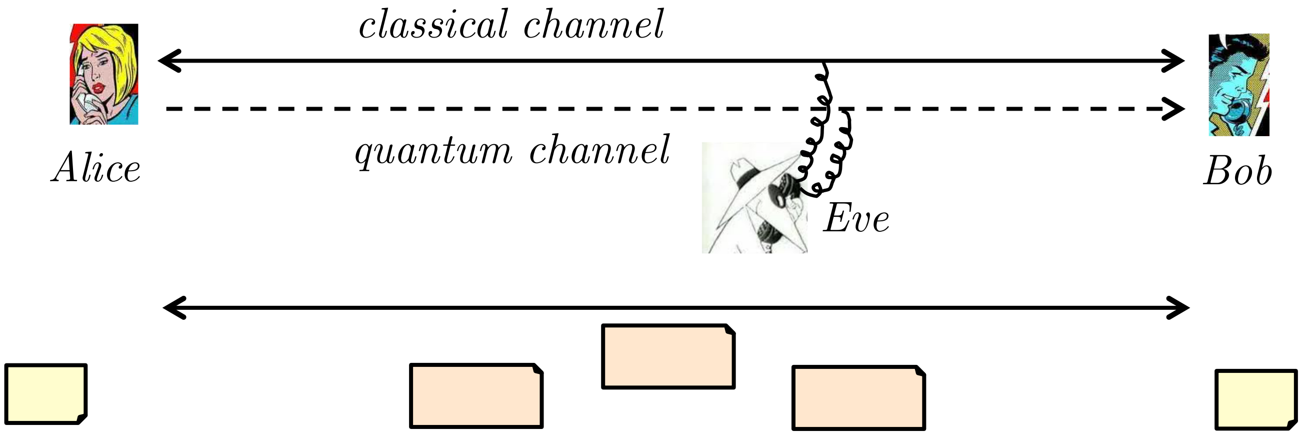
***Protocol*:**

2. (a) Upon reception of an electron, Bob *randomly* picks a *Color* box or a *Hardness* box to send it through.

   (b) Bob then generates a private list of the value of each electron received; and a public list of the property of each electron received.

Bob's private list	
electron 1:	*white*
electron 2:	*black*
etc...	

Bob's public list	
electron 1:	definite C-value
electron 2:	definite C-value
etc...	



Protocol:

3. After all electrons have been transmitted, Alice and Bob use the classical channel to exchange the Encryption chart and their *public* lists.

4. (a) Alice and Bob use their public lists to identify those electrons that did not get their properties disrupted by Bob.

   (b) They then use the Encrpytion chart, and their private lists, to identify the bits associated with these electrons. These bits are used to construct a key.

Alice's public list
electron 1: definite *H*-value
electron 2: definite *C*-value
etc...

Bob's public list
electron 1: definite *C*-value
electron 2: definite *C*-value
etc...

Public encryption chart

Hardness		*Color*	
$\vert hard\rangle$	$\Leftrightarrow$ 0	$\vert black\rangle$	$\Leftrightarrow$ 0
$\vert soft\rangle$	$\Leftrightarrow$ 1	$\vert white\rangle$	$\Leftrightarrow$ 1

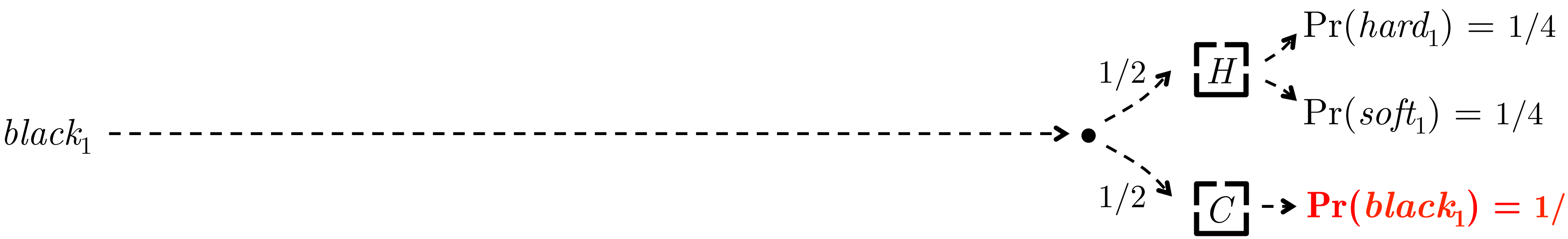
Alice's private list
electron 1: *hard*, 0
electron 2: *black*, 0
etc...

Bob's private list
electron 1: *white*
electron 2: *black*
etc...

Example:
- *electron* 1: *no matchup!*
- *electron* 2: *matchup!*
- *Bob and Alice now privately share a "0" bit!*

- *Claim*: Any attempt by Eve to intercept the key will be detectable.

Case 1: No Eve

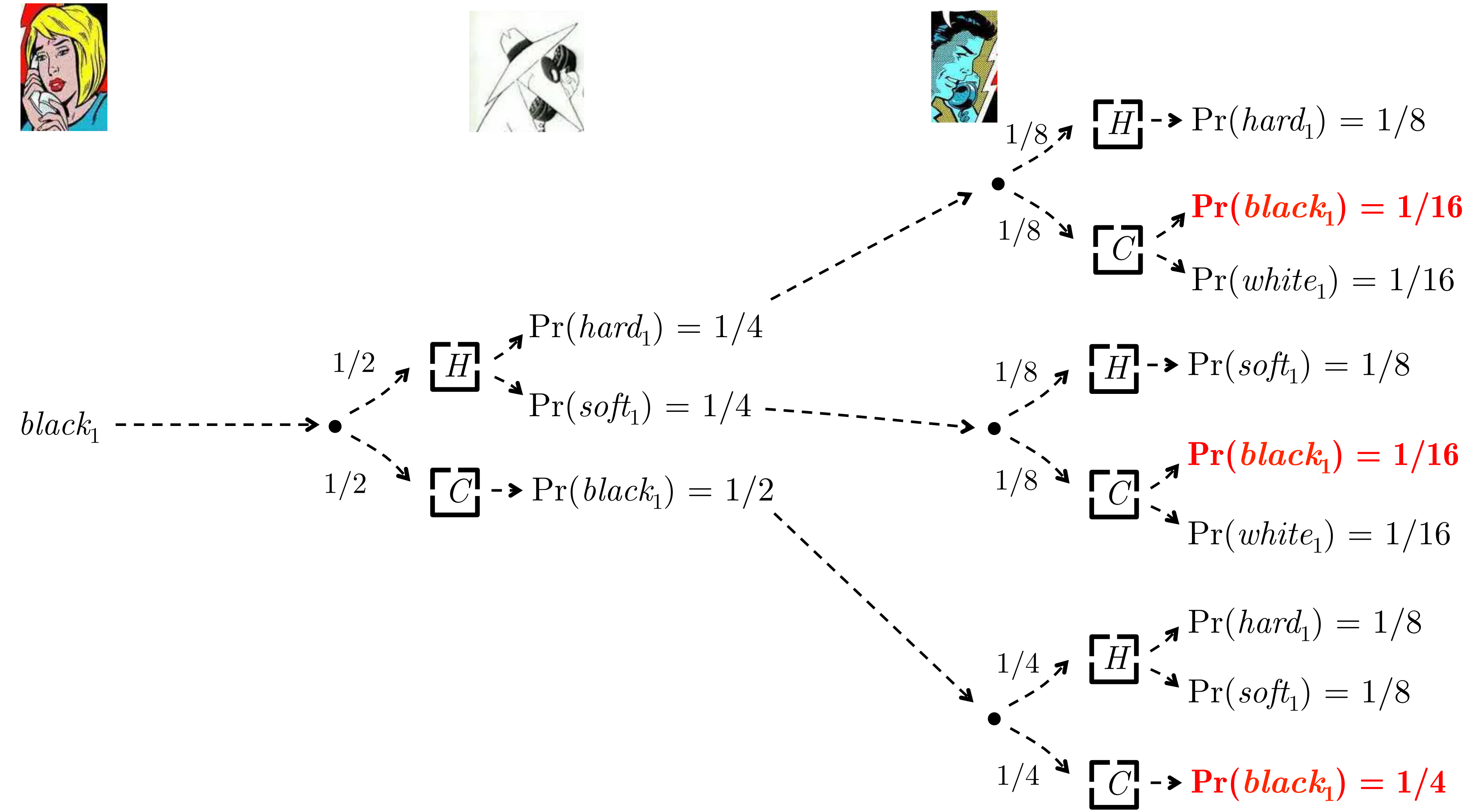


- *Suppose:* Electron 1 sent by Alice is black.
- What's the probability that Bob measures it as black?
- The probability that Bob measures its Color is 1/2; and when a black electron is measured for Color, it will register as black (of course).
- *So*: Without Eve present, $\Pr(\textit{Bob gets electron}_1 \textit{ right}) = 1/2$.

$$\begin{aligned} \Pr(hard_1) &= \Pr(\textit{black}_1 \textit{ measured for Hardness}) \times \Pr(\textit{black}_1 \textit{ is hard}/\textit{black}_1 \textit{ measured for Hardness}) \\ &= 1/2 \times 1/2 = 1/4 \end{aligned}$$

- *Claim*: Any attempt by Eve to intercept the key will be detectable.

Case 2: Eve Present



- With Eve, $\Pr(\mathit{Bob\ gets\ electron_1\ right}) = 1/16 + 1/16 + 1/4 = 3/8$.

- *So:* If Alice sends $2n$ electrons, without Eve, on average Bob will get $1/2 \times 2n = n$ right.
- *And:* With Eve present, on average Bob will get $3/8 \times 2n = 3n/4$ right.
- *So*: With Eve present, on average Bob gets $1/4$ wrong that he would have gotten right.

To detect Eve:

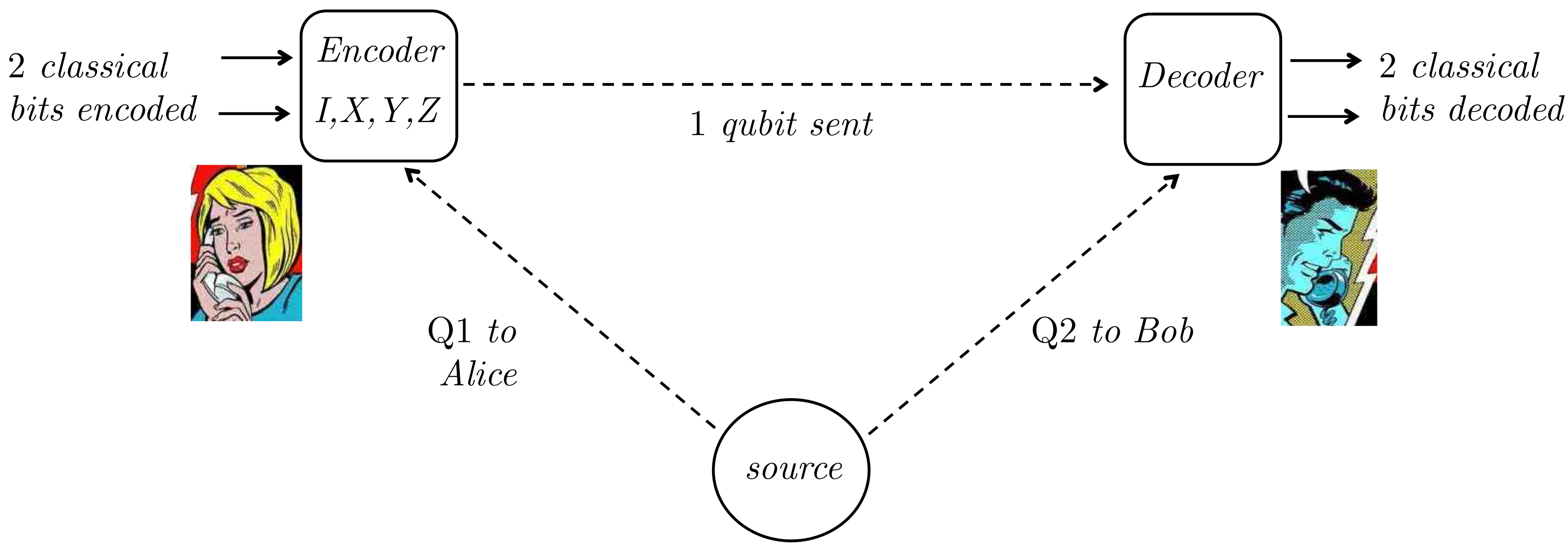
- Alice and Bob randomly choose half of the electrons Bob got right and now compare their *values* of Color/Hardness (recorded in their private lists).
- If these values all agree, then the probability that Eve is present is extremely *low*. They can now use the other electrons Bob got right as the key.
- If these values do not all agree, then it's probable that Eve is present and is disrupting the flow.

III. Quantum Dense Coding

- *Goal*: To use one qubit to transmit two classical bits.
- *But*: One qubit (supposedly) only contains one classical bit's worth of information!
- *So*: How can we send 2 classical bits using just one qubit?
- *Answer*: Use entangled states!

Set-Up:

- Prepare two qubits Q1, Q2 in an entangled state $|\Psi^+\rangle = \sqrt{\tfrac{1}{2}}\left(|0\rangle_1|0\rangle_2 + |1\rangle_1|1\rangle_2\right)$.
- Alice gets Q1, Bob gets Q2.
- Alice manipulates her Q1 so that it steers Bob's Q2 into a state from which he can read off the 2 classical bits Alice desires to send. All he needs to do this is the post-manipulated Q1 that Alice sends to him.



$$|\Psi^+\rangle = \sqrt{\tfrac{1}{2}}\left(|0\rangle_1|0\rangle_2 + |1\rangle_1|1\rangle_2\right).$$

Protocol

1. Alice has a pair of classical bits: either 00, 01, 10, or 11. She first encodes it in Q1 by acting on Q1 with one of $\{I, X, Y, Z\}$ according to:

pair:	transform:	new state:
00	$(I_1 \otimes I_2)\|\Psi^+\rangle$	$\sqrt{\frac{1}{2}}\left(\|0\rangle_1\|0\rangle_2 + \|1\rangle_1\|1\rangle_2\right)$
01	$(X_1 \otimes I_2)\|\Psi^+\rangle$	$\sqrt{\frac{1}{2}}\left(\|1\rangle_1\|0\rangle_2 + \|0\rangle_1\|1\rangle_2\right)$
10	$(Y_1 \otimes I_2)\|\Psi^+\rangle$	$\sqrt{\frac{1}{2}}\left(-\|1\rangle_1\|0\rangle_2 + \|0\rangle_1\|1\rangle_2\right)$
11	$(Z_1 \otimes I_2)\|\Psi^+\rangle$	$\sqrt{\frac{1}{2}}\left(\|0\rangle_1\|0\rangle_2 - \|1\rangle_1\|1\rangle_2\right)$

- *Let* Q1 *and* Q2 *be electrons in Hardness states.*
- *Let* $|0\rangle$ *be* $|soft\rangle$ *and* $|1\rangle$ *be* $|hard\rangle$.

2. Alice now sends Q1 to Bob.

3. After reception of Q1, Bob first applies a C_{NOT} transformation to both Q1 and Q2:

pair:	transform:	new state:	Apply C_{NOT}:
00	$(I_1 \otimes I_2)\|\Psi^+\rangle$	$\sqrt{\frac{1}{2}}\left(\|0\rangle_1\|0\rangle_2 + \|1\rangle_1\|1\rangle_2\right)$	$\sqrt{\frac{1}{2}}\left(\|0\rangle_1 + \|1\rangle_1\right)\|0\rangle_2$
01	$(X_1 \otimes I_2)\|\Psi^+\rangle$	$\sqrt{\frac{1}{2}}\left(\|1\rangle_1\|0\rangle_2 + \|0\rangle_1\|1\rangle_2\right)$	$\sqrt{\frac{1}{2}}\left(\|1\rangle_1 + \|0\rangle_1\right)\|1\rangle_2$
10	$(Y_1 \otimes I_2)\|\Psi^+\rangle$	$\sqrt{\frac{1}{2}}\left(-\|1\rangle_1\|0\rangle_2 + \|0\rangle_1\|1\rangle_2\right)$	$\sqrt{\frac{1}{2}}\left(-\|1\rangle_1 + \|0\rangle_1\right)\|1\rangle_2$
11	$(Z_1 \otimes I_2)\|\Psi^+\rangle$	$\sqrt{\frac{1}{2}}\left(\|0\rangle_1\|0\rangle_2 - \|1\rangle_1\|1\rangle_2\right)$	$\sqrt{\frac{1}{2}}\left(\|0\rangle_1 - \|1\rangle_1\right)\|0\rangle_2$

- *Note*: According to the EE Rule, Q1 still has no definite value, but Q2 now does!

Protocol

4. Bob now applies a Hadamard transformation to Q1:

pair:	*transform:*	*new state:*	*Apply C_{NOT}:*	*Now Apply H_1:*
00	$(I_1 \otimes I_2)\lvert\Psi^+\rangle$	$\sqrt{\frac{1}{2}}\left(\lvert 0\rangle_1\lvert 0\rangle_2 + \lvert 1\rangle_1\lvert 1\rangle_2\right)$	$\sqrt{\frac{1}{2}}\left(\lvert 0\rangle_1 + \lvert 1\rangle_1\right)\lvert 0\rangle_2$	$\lvert 0\rangle_1\lvert 0\rangle_2$
01	$(X_1 \otimes I_2)\lvert\Psi^+\rangle$	$\sqrt{\frac{1}{2}}\left(\lvert 1\rangle_1\lvert 0\rangle_2 + \lvert 0\rangle_1\lvert 1\rangle_2\right)$	$\sqrt{\frac{1}{2}}\left(\lvert 1\rangle_1 + \lvert 0\rangle_1\right)\lvert 1\rangle_2$	$\lvert 0\rangle_1\lvert 1\rangle_2$
10	$(Y_1 \otimes I_2)\lvert\Psi^+\rangle$	$\sqrt{\frac{1}{2}}\left(-\lvert 1\rangle_1\lvert 0\rangle_2 + \lvert 0\rangle_1\lvert 1\rangle_2\right)$	$\sqrt{\frac{1}{2}}\left(-\lvert 1\rangle_1 + \lvert 0\rangle_1\right)\lvert 1\rangle_2$	$\lvert 1\rangle_1\lvert 1\rangle_2$
11	$(Z_1 \otimes I_2)\lvert\Psi^+\rangle$	$\sqrt{\frac{1}{2}}\left(\lvert 0\rangle_1\lvert 0\rangle_2 - \lvert 1\rangle_1\lvert 1\rangle_2\right)$	$\sqrt{\frac{1}{2}}\left(\lvert 0\rangle_1 - \lvert 1\rangle_1\right)\lvert 0\rangle_2$	$\lvert 1\rangle_1\lvert 0\rangle_2$

- *Note*: According to the EE Rule, Q1 and Q2 now *both* have definite values.

5. Bob now measures Q1 and Q2 to determine the number Alice sent!

   (a) $(Q1 = 0,\ Q2 = 0) \Rightarrow 00$

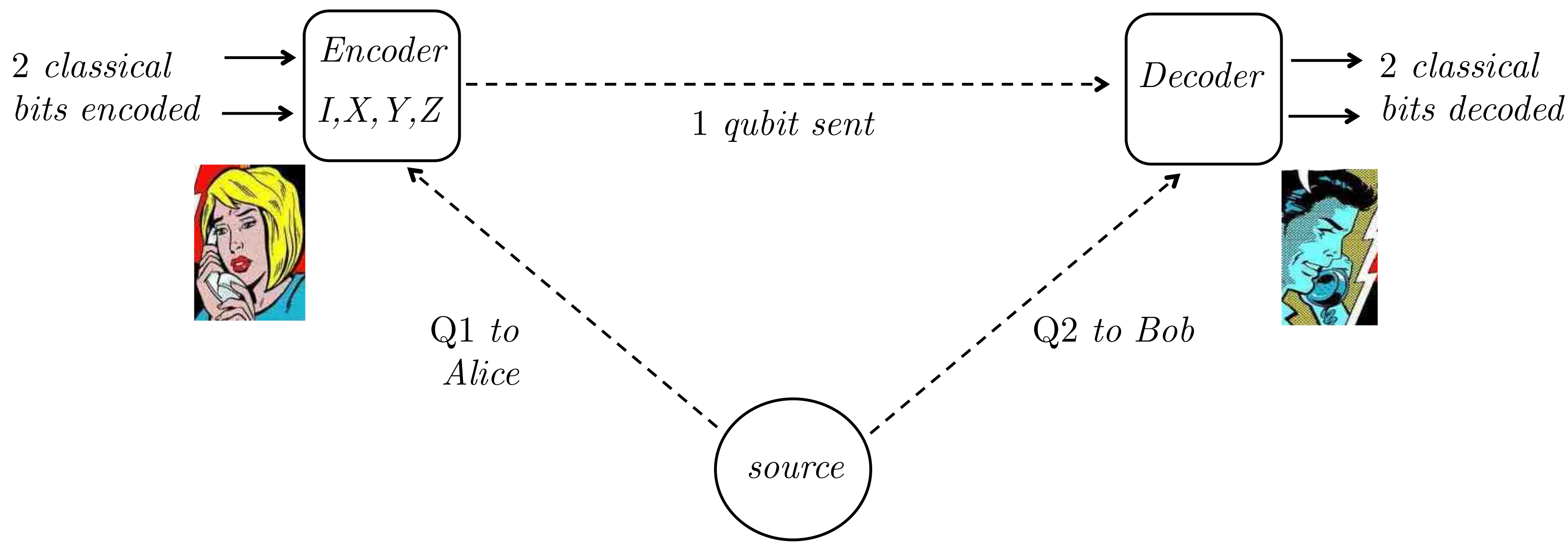
   (b) $(Q1 = 0,\ Q2 = 1) \Rightarrow 01$

   (c) $(Q1 = 1,\ Q2 = 0) \Rightarrow 10$

   (d) $(Q1 = 1,\ Q2 = 1) \Rightarrow 11$

Question: How are the 2 classical bits transferred from Alice to Bob?

- *Not* transferred *via* the single qubit.
- Transferred by the *correlations* present in the 2-qubit entangled state $|\Psi^+\rangle$.
- In order to convey information between Alice and Bob, it need *not* be physically transported from Alice to Bob across the intervening spatial distance.
- The *only* thing required to convey information is to set up a correlation between the sender's data and the receiver's data.



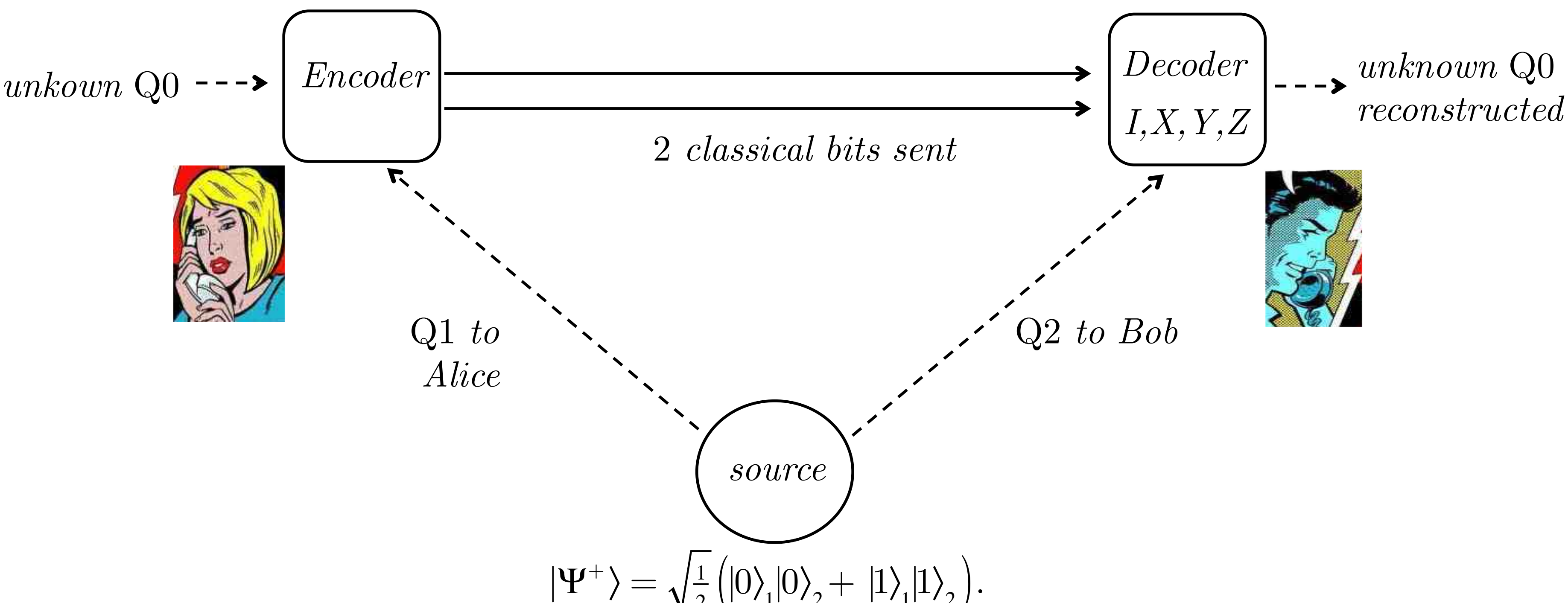
$$|\Psi^+\rangle = \sqrt{\tfrac{1}{2}}\left(|0\rangle_1|0\rangle_2 + |1\rangle_1|1\rangle_2\right).$$

IV. Quantum Teleportation

- *Goal*: To transmit an unknown quantum state using classical bits and to reconstruct the exact quantum state at the receiver.
- *But*: How can this avoid the No-Cloning Theorem?
- *Answer*: Use entangled states!

Set-Up:

- Alice has an unknown Q0, $|Q\rangle_0 = a|0\rangle_0 + b|1\rangle_0$, and wants to send it to Bob.
- Q1 and Q2 are prepared in an entangled state $|\Psi^+\rangle = \sqrt{\frac{1}{2}}\left(|0\rangle_1|0\rangle_2 + |1\rangle_1|1\rangle_2\right)$. Alice gets Q1, Bob gets Q2.
- Alice manipulates Q0 and Q1 so that they steer Bob's Q2 into the unknown state of Q0. Bob then reconstructs it using the 2 classical bits sent by Alice.



Protocol

1. Alice starts with a 3-qubit system (Q0, Q1, Q2) in the state:

$$|Q\rangle_0|\Psi^+\rangle = \sqrt{\tfrac{1}{2}}\left(a|0\rangle_0|0\rangle_1|0\rangle_2 + a|0\rangle_0|1\rangle_1|1\rangle_2 + b|1\rangle_0|0\rangle_1|0\rangle_2 + b|1\rangle_0|1\rangle_1|1\rangle_2\right)$$

Alice now applies C_{NOT} on Q0 & Q1, and then a Hadamard transformation on Q0:

First C_{NOT} on Q0 & Q1:

$$(C_{NOT_{01}} \otimes I_2)|Q\rangle_0|\Psi^+\rangle = \sqrt{\tfrac{1}{2}}\left(a|0\rangle_0|0\rangle_1|0\rangle_2 + a|0\rangle_0|1\rangle_1|1\rangle_2 + b|1\rangle_0|1\rangle_1|0\rangle_2 + b|1\rangle_0|0\rangle_1|1\rangle_2\right)$$

Then H on Q0:

$$(H_0 \otimes I_1 \otimes I_2)('''') = \tfrac{1}{2}|0\rangle_0|0\rangle_1\left(a|0\rangle_2 + b|1\rangle_2\right) + \tfrac{1}{2}|0\rangle_0|1\rangle_1\left(a|1\rangle_2 + b|0\rangle_2\right) +$$
$$\tfrac{1}{2}|1\rangle_0|0\rangle_1\left(a|0\rangle_2 - b|1\rangle_2\right) + \tfrac{1}{2}|1\rangle_0|1\rangle_1\left(a|1\rangle_2 - b|0\rangle_2\right)$$

EE Rule: *Each of the terms represents a state in which* Q0 *and* Q1 *have definite values, but* Q2 *does not.*

2. Alice now measures Q0 and Q1:

If measurement outcome is:	*...Q2 is now in state:*
$\|0\rangle_0\|0\rangle_1$	$a\|0\rangle_2 + b\|1\rangle_2$
$\|0\rangle_0\|1\rangle_1$	$a\|1\rangle_2 + b\|0\rangle_2$
$\|1\rangle_0\|0\rangle_1$	$a\|0\rangle_2 - b\|1\rangle_2$
$\|1\rangle_0\|1\rangle_1$	$a\|1\rangle_2 - b\|0\rangle_2$

Protocol

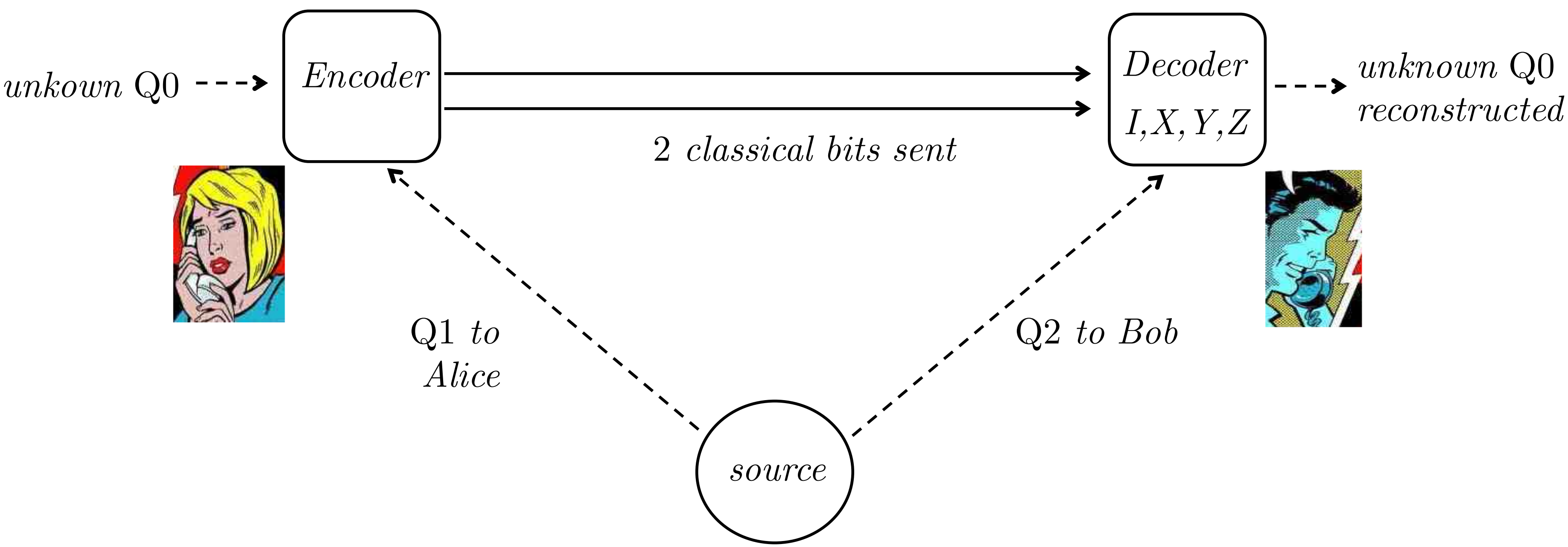
If measurement outcome is:	*...Q2 is now in state:*
$\lvert 0\rangle_0 \lvert 0\rangle_1$	$a\lvert 0\rangle_2 + b\lvert 1\rangle_2$
$\lvert 0\rangle_0 \lvert 1\rangle_1$	$a\lvert 1\rangle_2 + b\lvert 0\rangle_2$
$\lvert 1\rangle_0 \lvert 0\rangle_1$	$a\lvert 0\rangle_2 - b\lvert 1\rangle_2$
$\lvert 1\rangle_0 \lvert 1\rangle_1$	$a\lvert 1\rangle_2 - b\lvert 0\rangle_2$

3. Alice sends the result of her measurement to Bob in the form of 2 classical bits: 00, 01, 10, or 11.

4. Depending on what he receives, Bob performs one of $\{I, X, Y, Z\}$ on Q2. This allows him to turn it into (reconstruct) the unknown Q0.

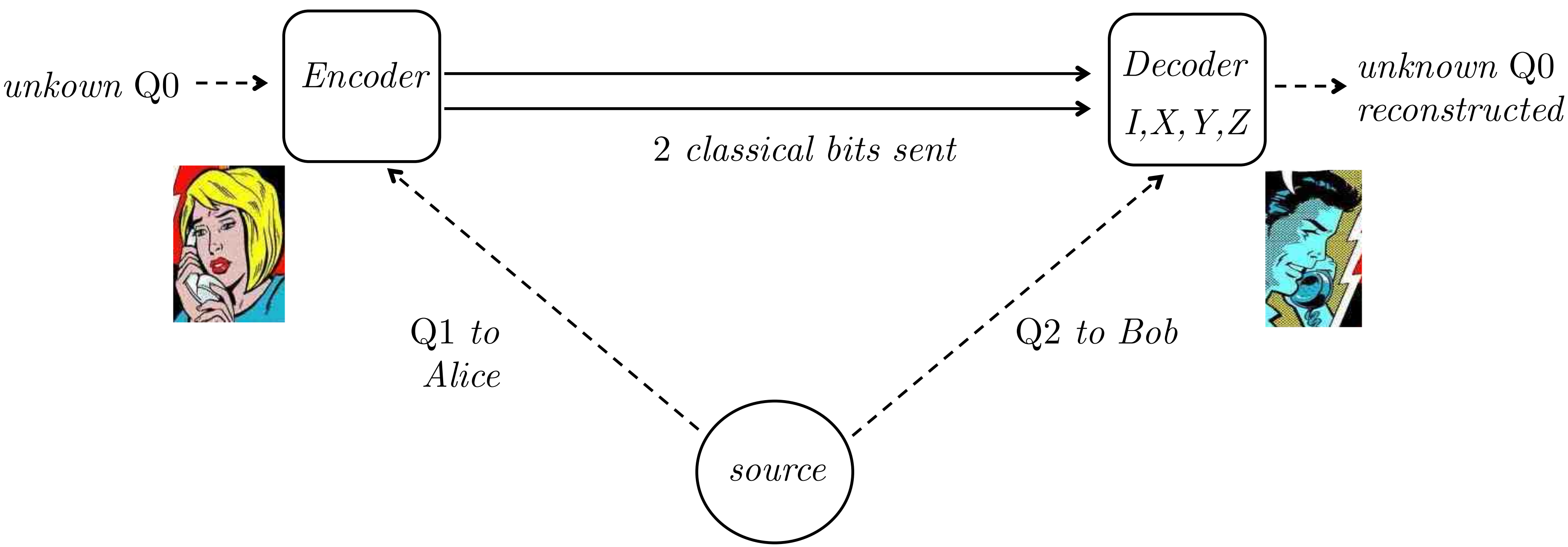
If bits received are:	*...then Q2 is now in state:*	*...so to reconstruct Q0, use:*
00	$a\lvert 0\rangle_2 + b\lvert 1\rangle_2$	I_2
01	$a\lvert 1\rangle_2 + b\lvert 0\rangle_2$	X_2
10	$a\lvert 0\rangle_2 - b\lvert 1\rangle_2$	Z_2
11	$a\lvert 1\rangle_2 - b\lvert 0\rangle_2$	Y_2

- *Question 1*: Does Bob violate the *No-Cloning Theorem*? Doesn't he construct a copy of the unknown Q0?
- *No violation occurs.*
- Bob *does* construct a copy: Q2 has become an exact duplicate of Q0.
- *But*: After Alice is through transforming Q0 and Q1, the original Q0 has now collapsed to either $|0\rangle_0$ or $|1\rangle_0$! Alice destroys Q0 in the process of conveying the information contained in it to Bob!



$$|\Psi^+\rangle = \sqrt{\tfrac{1}{2}}\left(|0\rangle_1|0\rangle_2 + |1\rangle_1|1\rangle_2\right).$$

- *<u>Question 2</u>*: How does Bob reconstruct the unknown Q0 (that encodes an arbitrarily large amount of information) from just 2 classical bits?
- Information to reconstruct Q0 is transferred by the correlations present in the entangled state $|\Psi^{+}\rangle$, *in addition* to the 2 classical bits.
- The 2 classical bits are used simply to determine the appropriate transformation on Q2, *after* it has been "steered" into the appropriate state by Alice.



$$|\Psi^{+}\rangle = \sqrt{\tfrac{1}{2}}\left(|0\rangle_1|0\rangle_2 + |1\rangle_1|1\rangle_2\right).$$