07. Quantum Information Theory (QIT), Part I.

1. C-bits vs. Qubits

- *Classical Information Theory*

  Bit = a state of a *classical* 2-state system.

  - *Represented by 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.
  - *Must be capable of being in two distinguishable states (in physical realizations, require sufficiently large energy barrier to separate states).*

- *Quantum Information Theory*

  Qubit = a state of a *quantum* 2-state system.

  - *Represented by either* $|0\rangle$, $|1\rangle$, *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. Single Qubit Transformations

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

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

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

$$\mathfrak{H} = \begin{pmatrix}\sqrt{1/2} & \sqrt{1/2}\\ \sqrt{1/2} & -\sqrt{1/2}\end{pmatrix}$$

Hadamard operator

$$\mathfrak{H}|0\rangle = \sqrt{1/2}\,(|0\rangle + |1\rangle)$$

$$\mathfrak{H}|1\rangle = \sqrt{1/2}\,(|0\rangle - |1\rangle)$$

Takes a basis qubit and outputs a superposition

3. Multi-Qubits Transformations

- Let $\{|0\rangle_1, |1\rangle_1\}$, $\{|0\rangle_2, |1\rangle_2\}$ be bases for the single qubit state spaces $\mathcal{H}^{(1)}, \mathcal{H}^{(2)}$.

- *Then*: A basis for the 2-qubit state space $\mathcal{H}^{(1)} \otimes \mathcal{H}^{(2)}$ is given by

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

- *Aside*: *Another* basis for $\mathcal{H}^{(1)} \otimes \mathcal{H}^{(2)}$ is given by

$$\{|\Psi^+\rangle, |\Psi^-\rangle, |\Phi^+\rangle, |\Phi^-\rangle\},$$

where:

$$\left.\begin{aligned} |\Psi^+\rangle &= \sqrt{1/2}\,(|0\rangle_1|0\rangle_2 + |1\rangle_1|1\rangle_2) \\ |\Psi^-\rangle &= \sqrt{1/2}\,(|0\rangle_1|0\rangle_2 - |1\rangle_1|1\rangle_2) \\ |\Phi^+\rangle &= \sqrt{1/2}\,(|1\rangle_1|0\rangle_2 + |0\rangle_1|1\rangle_2) \\ |\Phi^-\rangle &= \sqrt{1/2}\,(-|1\rangle_1|0\rangle_2 + |0\rangle_1|1\rangle_2) \end{aligned}\right\}$$

The "Bell basis" for $\mathcal{H}^{(1)} \otimes \mathcal{H}^{(2)}$.
Each basis vector is an entangled state!

- Let $|0\rangle_1|0\rangle_2$, $|0\rangle_1|1\rangle_2$, $|1\rangle_1|0\rangle_2$, $|1\rangle_1|1\rangle_2$ be given the matrix representations:

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

- Define the 2-qubit "Controlled-NOT" operator by:

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

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

Acts on two 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

$$U|v\rangle_1|0\rangle_2 = |v\rangle_1|v\rangle_2, \quad \text{where } |v\rangle_1 \text{ is an unknown qubit.}$$

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 unknown qubits $|a\rangle_1$, $|b\rangle_1$.
- *Let*: $|c\rangle_1 = \alpha|a\rangle_1 + \beta|b\rangle_1$, where $|\alpha|^2 + |\beta|^2 = 1$
- *Then*: $U|c\rangle_1|0\rangle_2 = U(\alpha|a\rangle_1|0\rangle_2 + \beta|b\rangle_1|0\rangle_2)$

$$= (\alpha U|a\rangle_1|0\rangle_2 + \beta U|b\rangle_1|0\rangle_2), \quad \textit{since } U \textit{ is linear}$$

$$= \alpha|a\rangle_1|a\rangle_2 + \beta|b\rangle_1|b\rangle_2$$

- *But*: By definition, U acts on $|c\rangle_1$ according to:

$$\begin{aligned} U|c\rangle_1|0\rangle_2 &= |c\rangle_1|c\rangle_2 \\ &= (\alpha|a\rangle_1 + \beta|b\rangle_1)(\alpha|a\rangle_2 + \beta|b\rangle_2) \\ &= \alpha^2|a\rangle_1|a\rangle_2 + \alpha\beta|a\rangle_1|b\rangle_2 + \beta\alpha|b\rangle_1|a\rangle_2 + \beta^2|b\rangle_1|b\rangle_2. \end{aligned}$$

- *So*: There can be no such U.

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

5. 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)

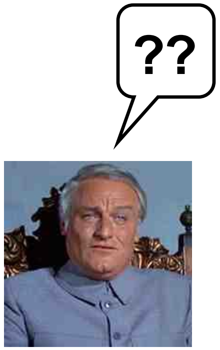
S	***H***	***A***	***K***	***E***	***N***		***N***	***O***	***T***		***S***	***T***	***I***	***R***	***R***	***E***	***D***
18	07	00	10	04	13	29	13	14	19	29	18	19	08	17	17	04	03

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)

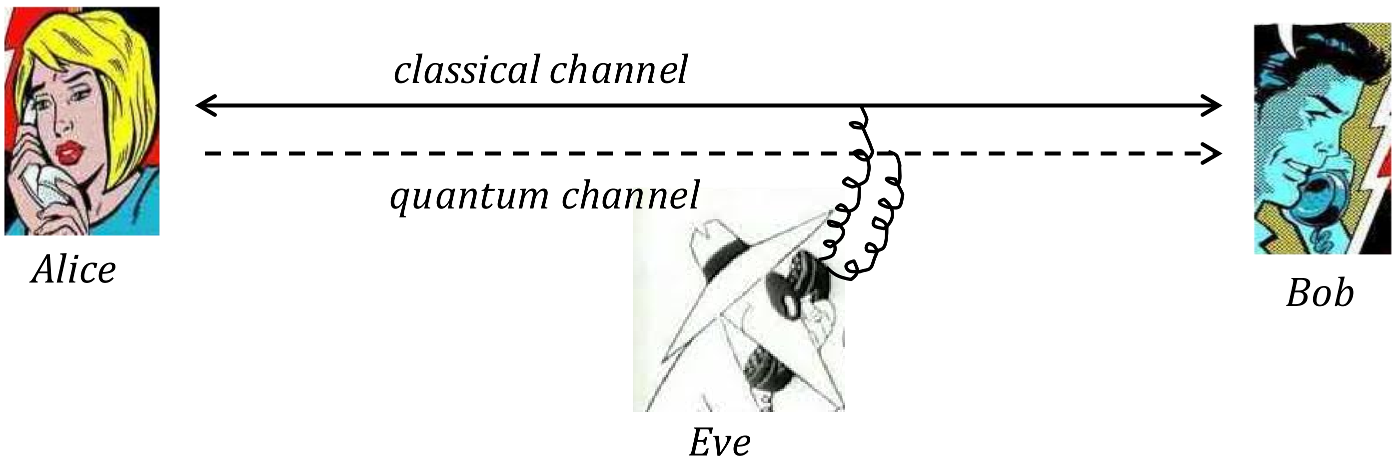
03	11	28	23	18	19	20	24	07	07	08	29	03	09	06	22	26	10

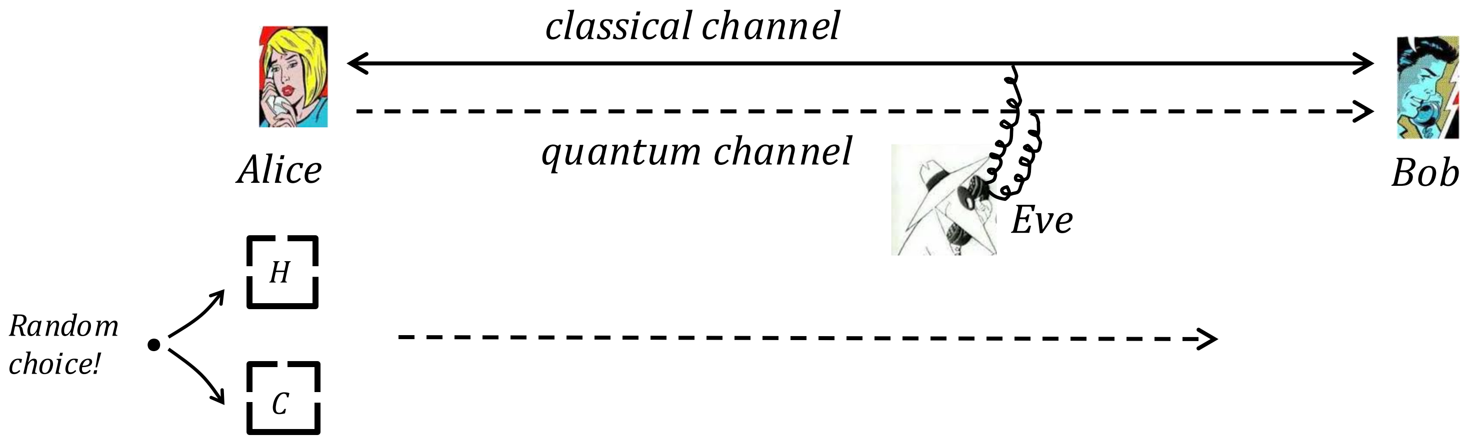
- *Technical Result (Shannon 1949)*: One-time pad is guaranteed secure, as long as the key is completely *random*, has same length as plaintext, is never reused, and *is not intercepted by a third party*.

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

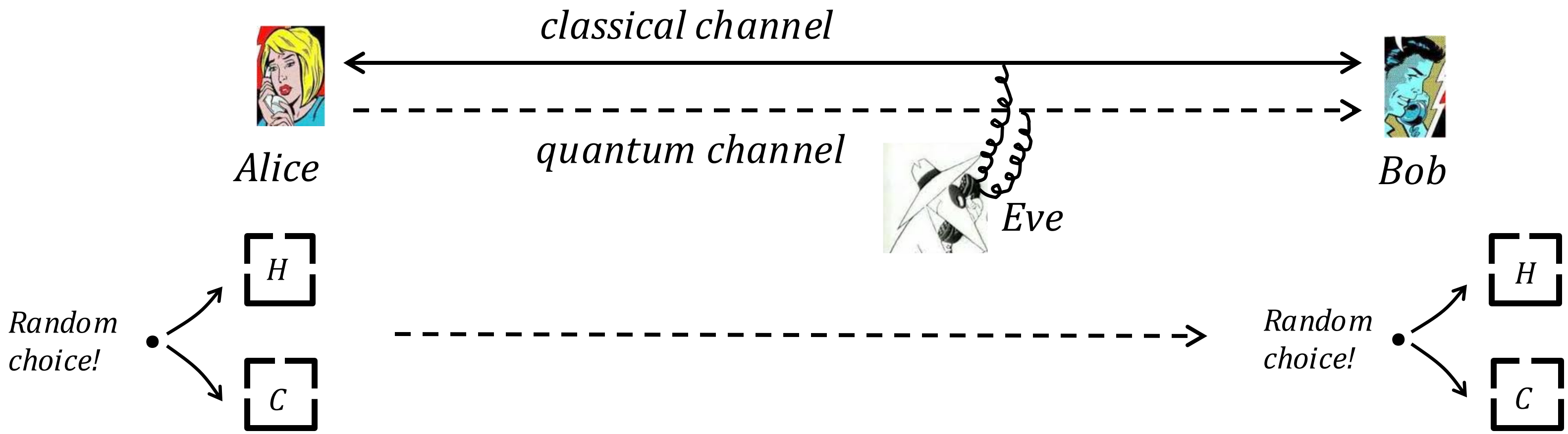
Hardness	*Color*
$\lvert hard\rangle \Leftrightarrow 0$	$\lvert black\rangle \Leftrightarrow 0$
$\lvert soft\rangle \Leftrightarrow 1$	$\lvert white\rangle \Leftrightarrow 1$

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...



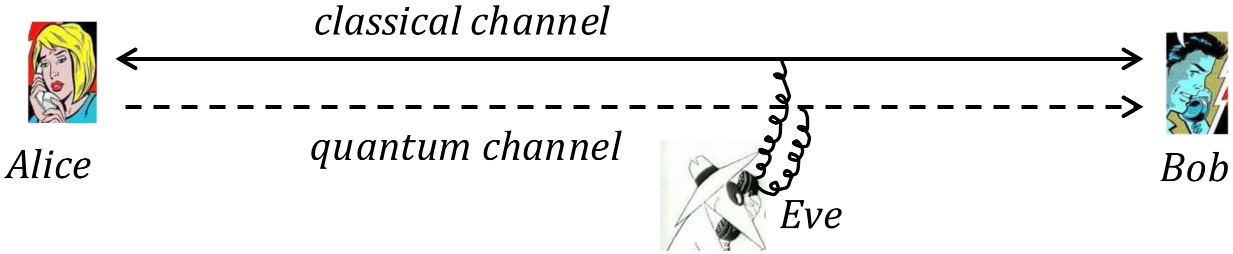
<u>*Protocol*</u>:

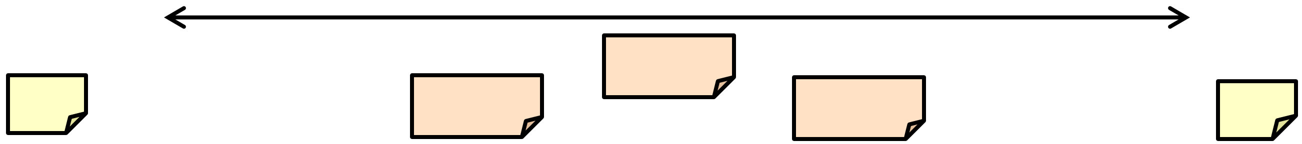
2. (a) Upon reception of an electron, Bob *randomly* picks a *Color* box or a *Hardness* box to send it through.

   (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...





<u>Protocol</u>:

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

4. (a) Alice and Bob use their public records to identify those electrons that did not get their properties disrupted by Bob.
   (b) They then use the Encrpytion chart, and their private charts, 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

<u>*Hardness*</u>	<u>*Color*</u>
$\|hard\rangle \Leftrightarrow 0$	$\|black\rangle \Leftrightarrow 0$
$\|soft\rangle \Leftrightarrow 1$	$\|white\rangle \Leftrightarrow 1$

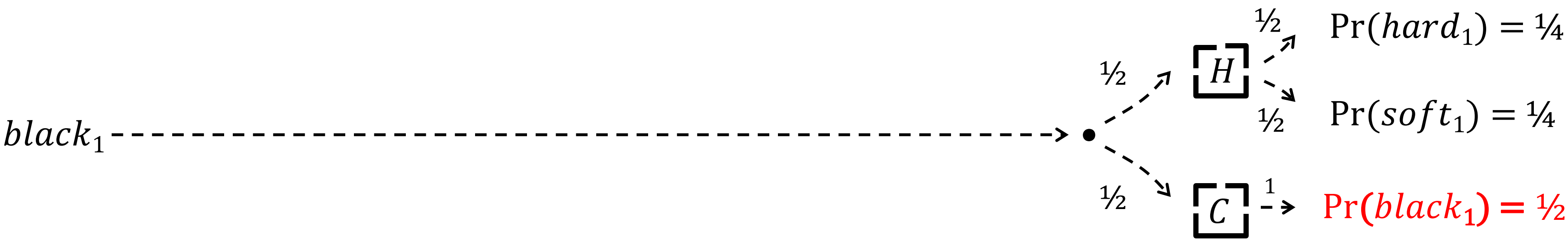
Alice's private list
electron 1: *hard*, 0
electron 2: *black*, 0
etc...

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

<u>Example</u>:
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



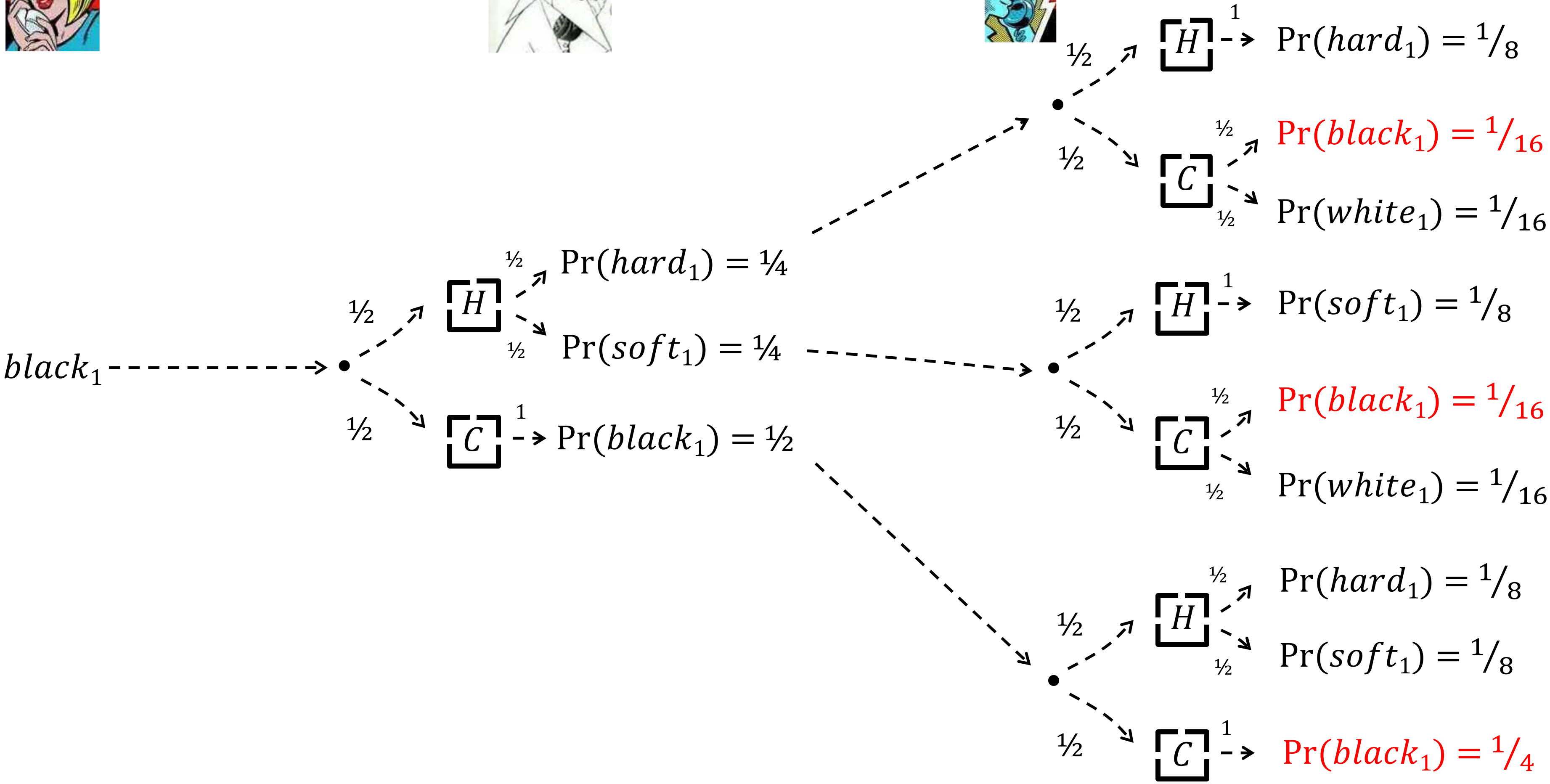
- *Suppose*: Electron 1 sent by Alice is black.
- What's the probability that Bob measures it as black?
- The probability that Bob measures its Color is ½; and when a black electron is measured for Color, it will register as black (of course).
- *So*: Without Eve present, Pr(*Bob gets electron*$_1$ *right*) = ½.

Ex: $\Pr(hard_1) = \Pr(black_1 \textit{ measured for Hardness}) \times \Pr(black_1 \textit{ is hard} \mid black_1 \textit{ measured for Hardness})$

$= ½ \times ½ = ¼$

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

Case 2: Eve Present



- With Eve, $\Pr(Bob\ gets\ electron_1\ right) = {}^1/_{16} + {}^1/_{16} + {}^1/_4 = {}^3/_8$

Claim: With Eve, Bob gets wrong $1/4$ of the electrons he got right without Eve.

Check: Suppose Alice sends n electrons.

- Without Eve, Bob gets $n/2$ right, and $n/2$ wrong.
- With Eve, Bob gets $3n/8$ right, and $5n/8$ wrong.
- *So*: With Eve, Bob gets $(n/2 - 3n/8) = n/8$ more electrons wrong than without Eve.
- *And*: $n/8 = 1/4 \times n/2$.

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 Eve is present and is disrupting the flow*.