

# CS 258: Quantum Cryptography

**Mark Zhandry**

Previously...

# Bra-Ket Notation

Column vector

$$|\psi\rangle = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \end{pmatrix}$$

Row vector

$$\langle\psi| = (|\psi\rangle)^\dagger$$

Inner products:

$$\langle\psi|\phi\rangle = \langle\psi| \cdot |\phi\rangle$$

$$||\psi\rangle| = \sqrt{\langle\psi|\psi\rangle}$$

A quantum transformation is a unitary transformation:

$$|\psi\rangle \longrightarrow U|\psi\rangle$$

A unitary matrix  $U$  is square and satisfies  $U^\dagger U = \mathbf{I}$

Or equivalently  $U^{-1} = U^\dagger$

In particular, the inverse always exists

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \longrightarrow \boxed{\text{meter symbol}} \longrightarrow \begin{array}{l} 0 \text{ w/ probability } |\alpha|^2 \\ 1 \text{ w/ probability } |\beta|^2 \end{array}$$

Normalization ensures valid probability distribution, and squaring matches the relationship between underlying wave and observed intensity/probability

$$\text{In general: } |\psi\rangle \longrightarrow \boxed{\text{meter symbol}} \longrightarrow i \text{ w/ probability } |\langle i|\psi\rangle|^2$$

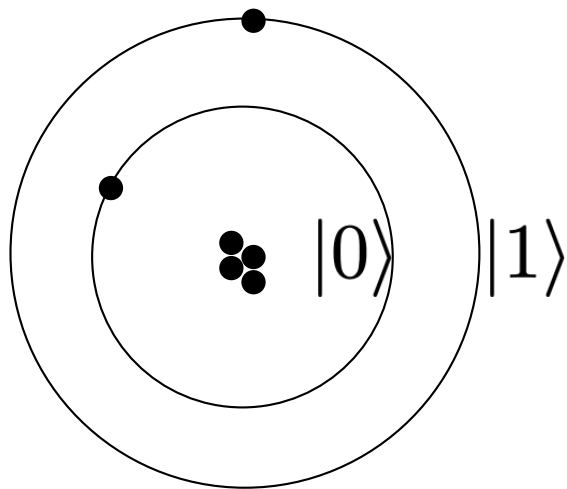
# Post-measurement state of system

Rather than a measurement destroying the state, we will usually think of it as simply “collapsing” the state to be at a given location; the state can then be further acted on

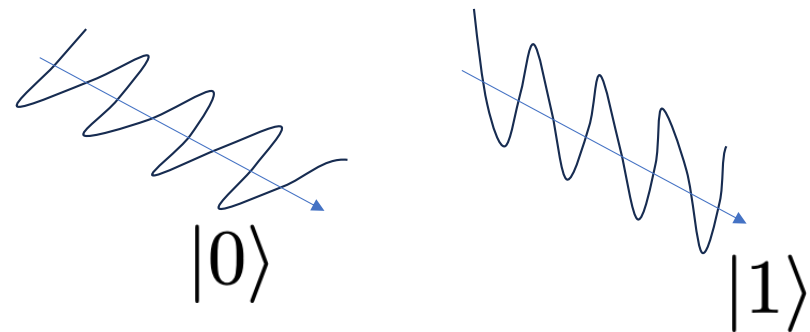
$$|\psi\rangle \longrightarrow \boxed{\text{meter symbol}} \longrightarrow i \text{ w/ probability } |\langle i|\psi\rangle|^2$$

Then state collapses to  $|i\rangle$

We used the double slit experiment as a motivation, but the mathematical framework of quantum mechanics is an abstraction describing many possible systems



Atomic orbitals



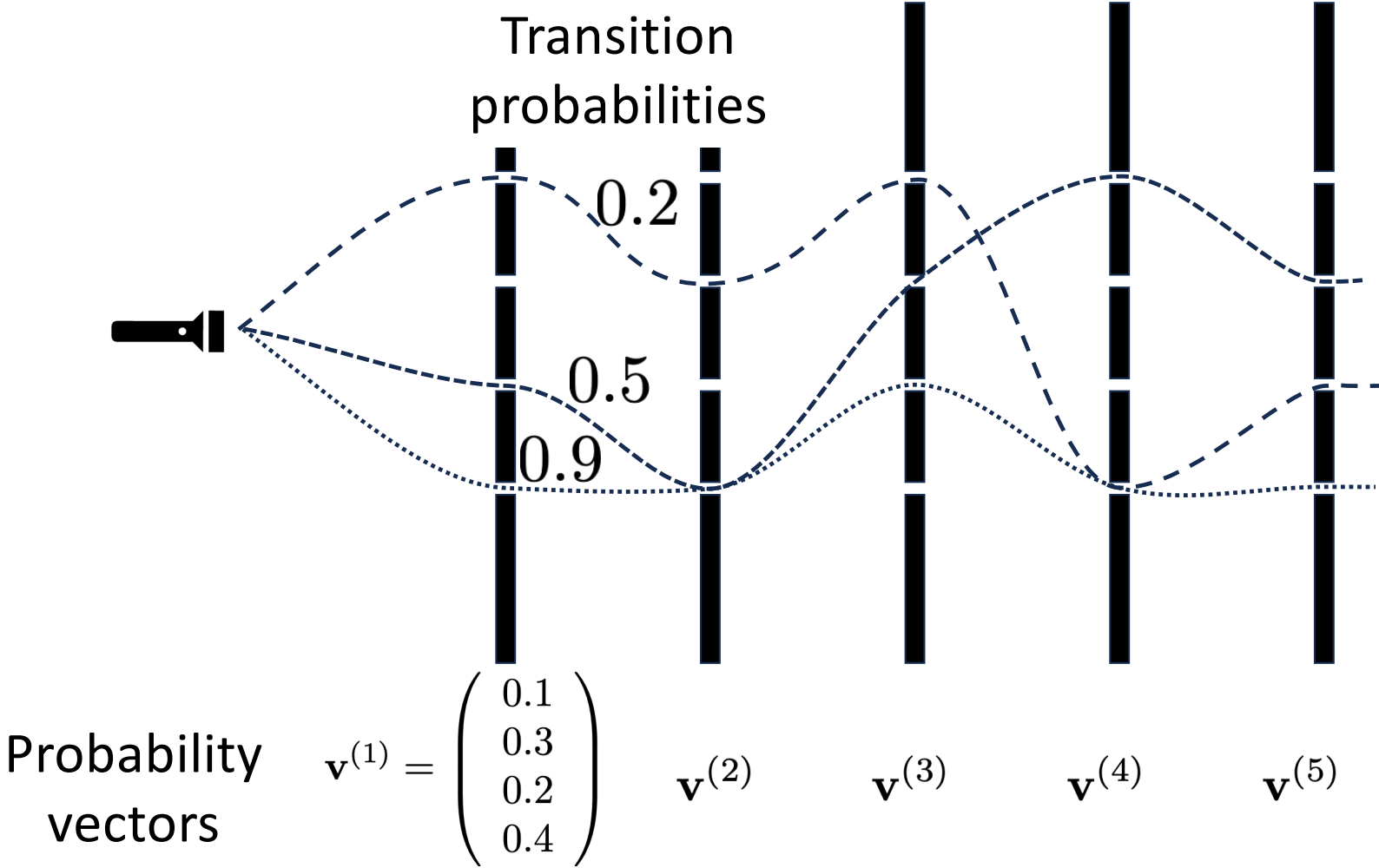
Photon polarization

Today: Comparison to classical mechanics, the observer effect, and QKD



# Comparison to classical statistical mechanics

# Classical statistical mechanics



$\mathbf{v}^{(i)}$  = probability vector at wall  $i$

$U^{(i)}$  = transition probabilities from wall  $i - 1$  to  $i$

$$\mathbf{v}^{(i)} = U_i \mathbf{v}^{(i-1)}$$

$U^{(i)}$  must map probability vectors to probability vectors  $\rightarrow$  columns are probability vectors  
(called a “stochastic matrix”)

## A path view of classical statistical mechanics

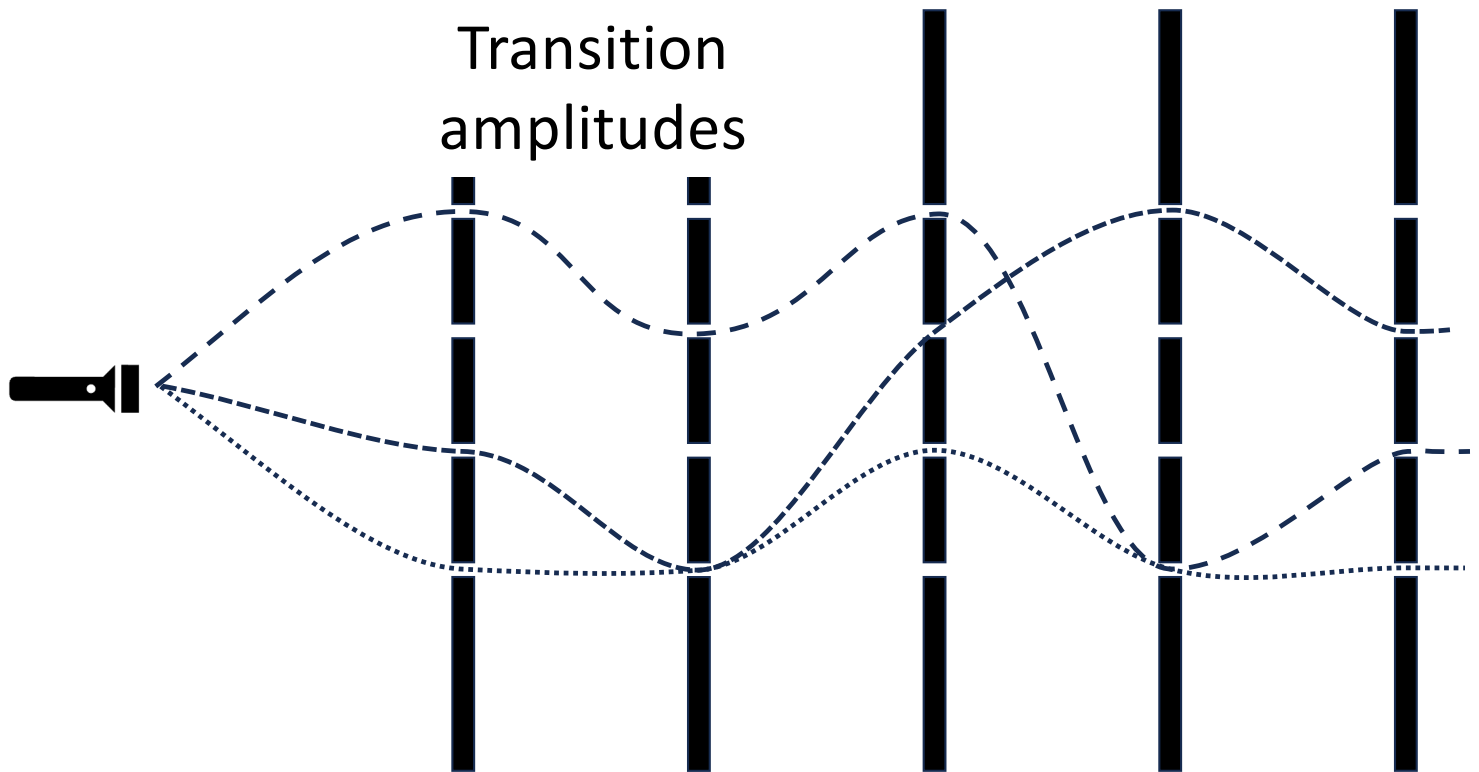
Let  $p$  be a path a particle can take through the walls

$$\Pr[p] = \mathbf{v}_{p_1}^{(1)} \times \prod_{i=2}^n U_{p_i, p_{i-1}}^{(i)}$$

$p_i$  = slit path goes through in wall  $i$

$$v_j^{(n)} = \sum_{p: p_n = j} \Pr[p]$$

# Quantum mechanics



Quantum states =  
amplitude vectors

$$|\psi^{(1)}\rangle$$

$$|\psi^{(2)}\rangle$$

$$|\psi^{(3)}\rangle$$

$$|\psi^{(4)}\rangle$$

$$|\psi^{(5)}\rangle$$

$|\psi^{(i)}\rangle$  = amplitude vector at wall  $i$

$U^{(i)}$  = transition probabilities from wall  $i - 1$  to  $i$

$$|\psi^{(i)}\rangle = U^{(i)} |\psi^{(i-1)}\rangle$$

$U^{(i)}$  must map amplitude vectors to amplitude vectors  $\rightarrow$  unitary

## A path view of quantum mechanics

Let  $p$  be a path a particle can take through the walls

$$\text{Amp}(p) = \alpha_{p_1} \times \prod_{i=2}^n U_{p_i, p_{i-1}}^{(i)} \quad \text{where} \quad |\psi^{(1)}\rangle = \sum_j \alpha_j |j\rangle$$

$$|\psi^{(n)}\rangle = \sum_j |j\rangle \left( \sum_{p: p_n=j} \text{Amp}(p) \right)$$

## A path view of quantum mechanics

Let  $p$  be a path a particle can take through the walls

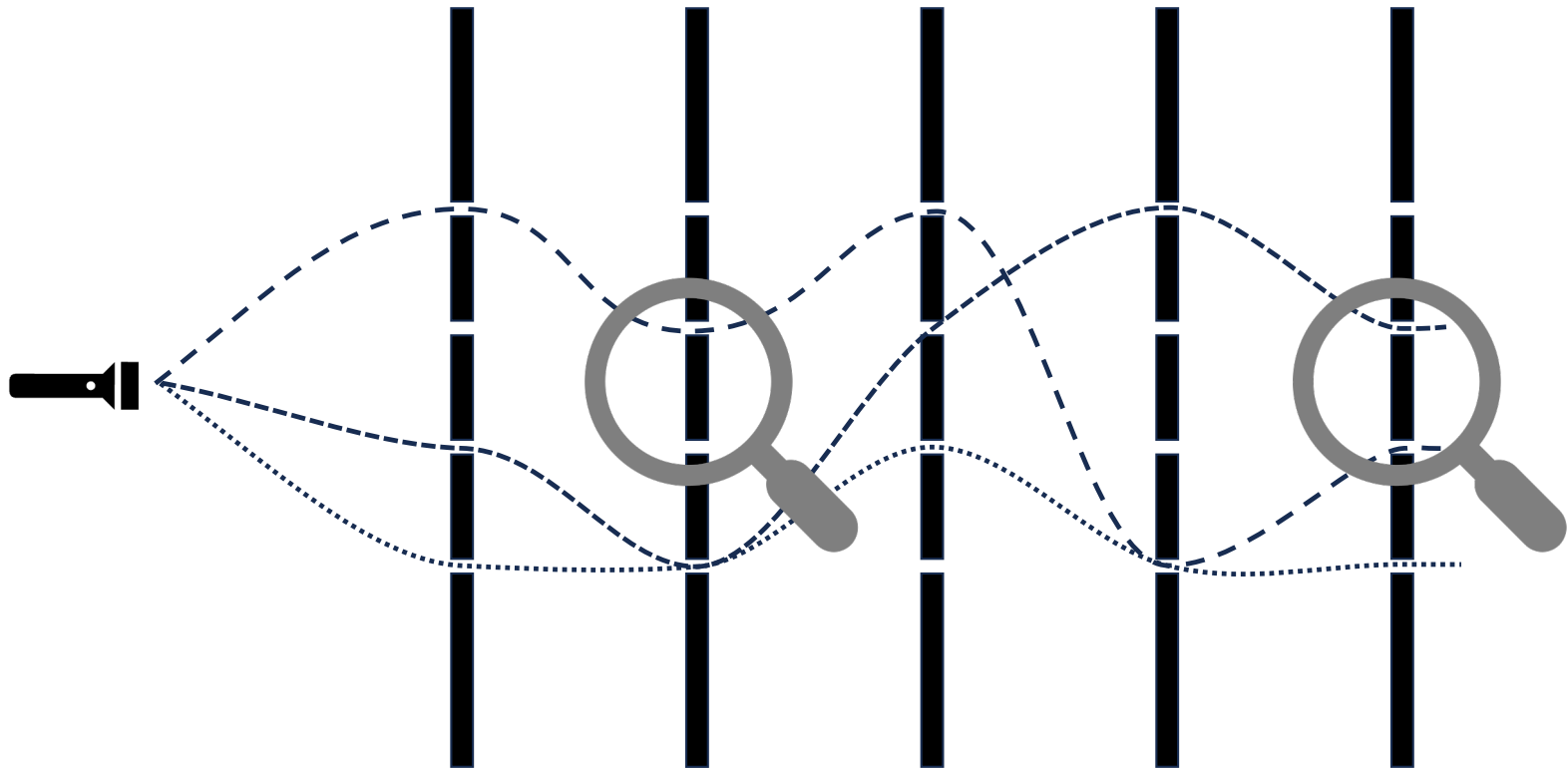
$$\text{Amp}(p) = \alpha_{p_1} \times \prod_{i=2}^n U_{p_i, p_{i-1}}^{(i)} \quad \text{where} \quad |\psi^{(1)}\rangle = \sum_j \alpha_j |j\rangle$$

Probability of observing photon  
at position  $j$  at wall  $n$  :

$$\left| \sum_{p: p_n=j} \text{Amp}(p) \right|^2$$



# Intermediate Measurements



What happens if we look at the particle in two places?

## Classical Statistical Mechanics

$v_{j,k}^{(m,n)}$  = probability of seeing photon at slit  $j$  at wall  $m$  and slit  $k$  at wall  $n$

$$v_{j,k}^{(m,n)} = \sum_{p: p_m=j, p_n=k} \Pr[p]$$

## Classical Statistical Mechanics

Now, what if we look at photon at  $m$ , but forget it's location?

$$\sum_j v_{j,k}^{(m,n)} = \sum_j \left( \sum_{p:p_m=j, p_n=k} \text{Pr}[p] \right) = v_k^{(n)}$$

## Quantum Mechanics

probability of seeing photon at  
slit  $j$  at wall  $m$  and slit  $k$  at wall  $n$

$$\left| \sum_{p:p_m=j, p_n=k} \text{Amp}(p) \right|^2$$

## Quantum Mechanics

Now, what if we look at photon at  $m$ , but forget it's location?

$$\sum_j \left| \sum_{p: p_m=j, p_n=k} \text{Amp}(p) \right|^2$$
$$\neq \left| \sum_j \sum_{p: p_m=j, p_n=k} \text{Amp}(p) \right|^2 = \left| \sum_{p: p_n=k} \text{Amp}(p) \right|^2$$

# The observer effect

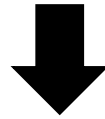
Looking at photon at  $m$  inherently changes its final state

# Applying the observer effect to cryptography: Quantum Key Distribution (QKD)



# Motivation:

Recall that in a classical world, it is impossible to send information in a way that is hidden to a computationally unbounded eavesdropper

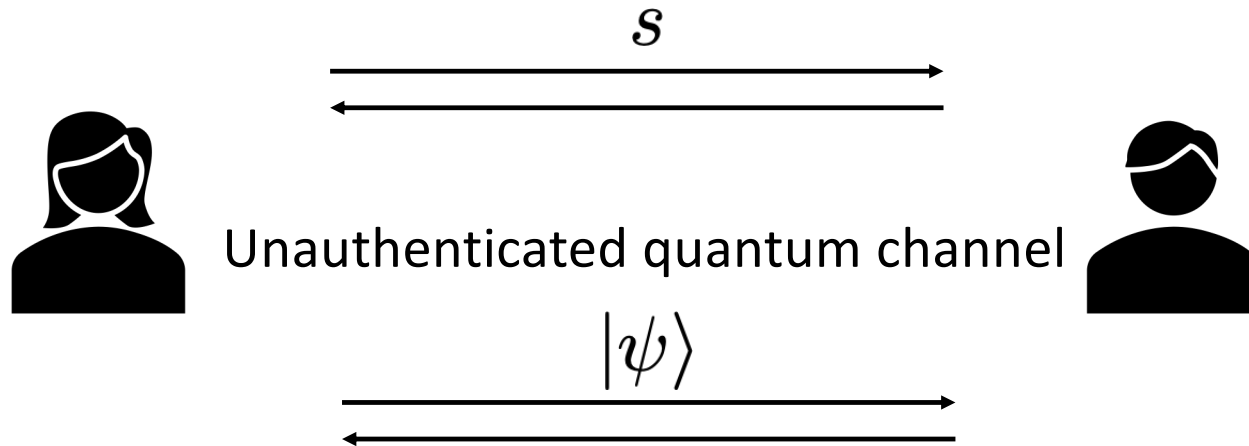


Due to complexity-theoretic challenges (P vs NP), all our cryptosystems are only conditionally secure

Quantum key distribution = unconditionally secure\*  
exchange of secret keys against unbounded eavesdroppers

\* with major caveats

Authenticated classical channel = adversary can't tamper



Goal: Alice and Bob establish secret key  
that is hidden to any eavesdropper

# Idea behind BB84

Bennett, Brassard

Choose random  $b, c \leftarrow \{0, 1\}$



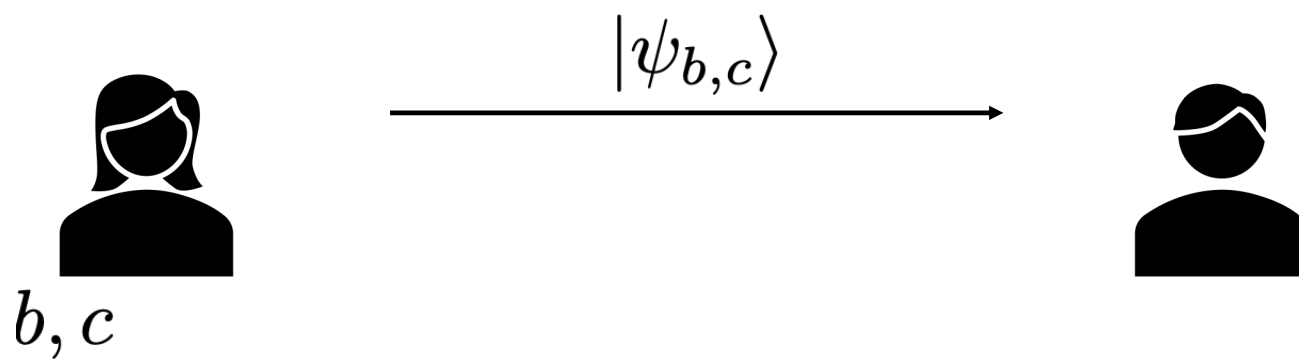
$$|\psi_{b,c}\rangle = \mathbf{H}^b |c\rangle = \begin{cases} |0\rangle & \text{if } b = c = 0 \\ |1\rangle & \text{if } b = 0, c = 1 \\ \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle & \text{if } b = 1, c = 0 \\ \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle & \text{if } b = c = 1 \end{cases}$$

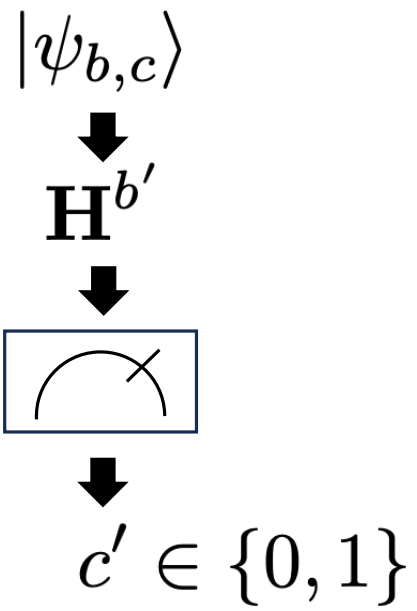
$|+\rangle$

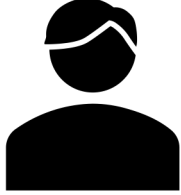
$|-\rangle$

Recall:

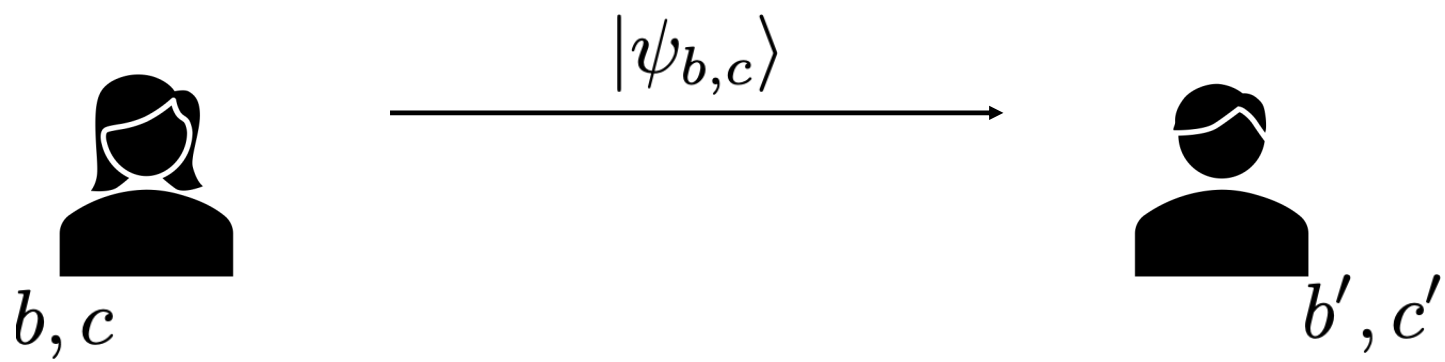
$$\mathbf{H} = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}$$







Choose random  $b' \leftarrow \{0, 1\}$



$b, b', c$  are independent random bits

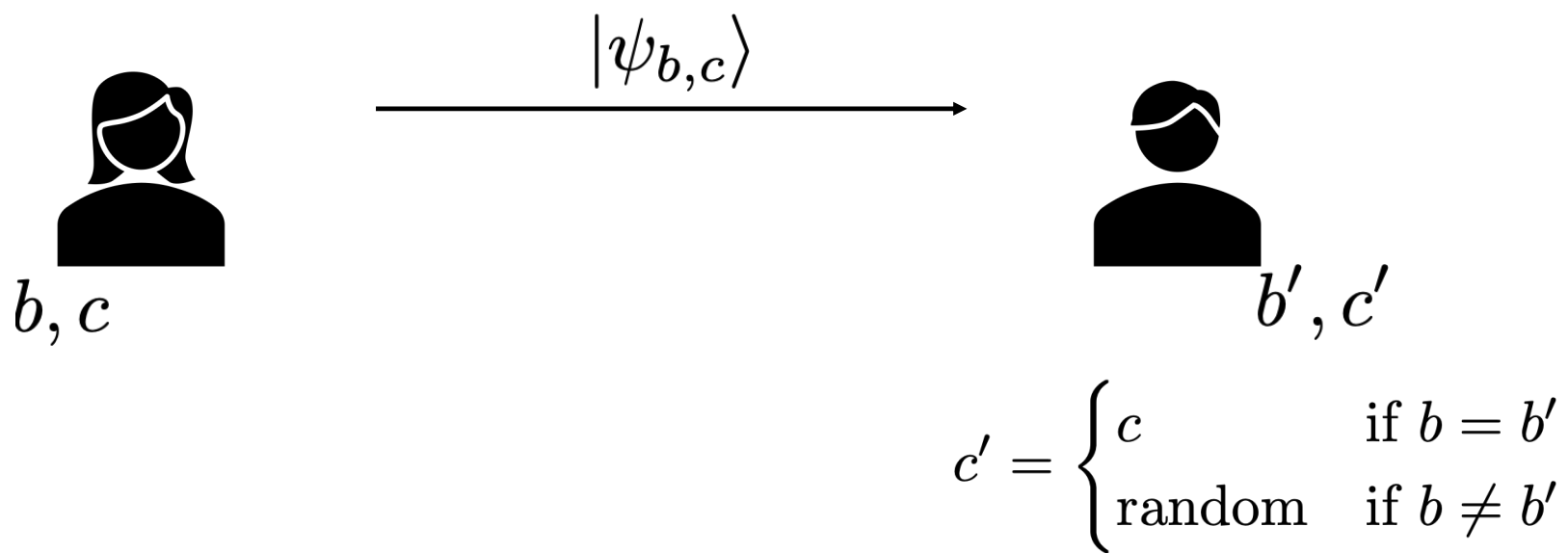
Distribution of  $c'$ :

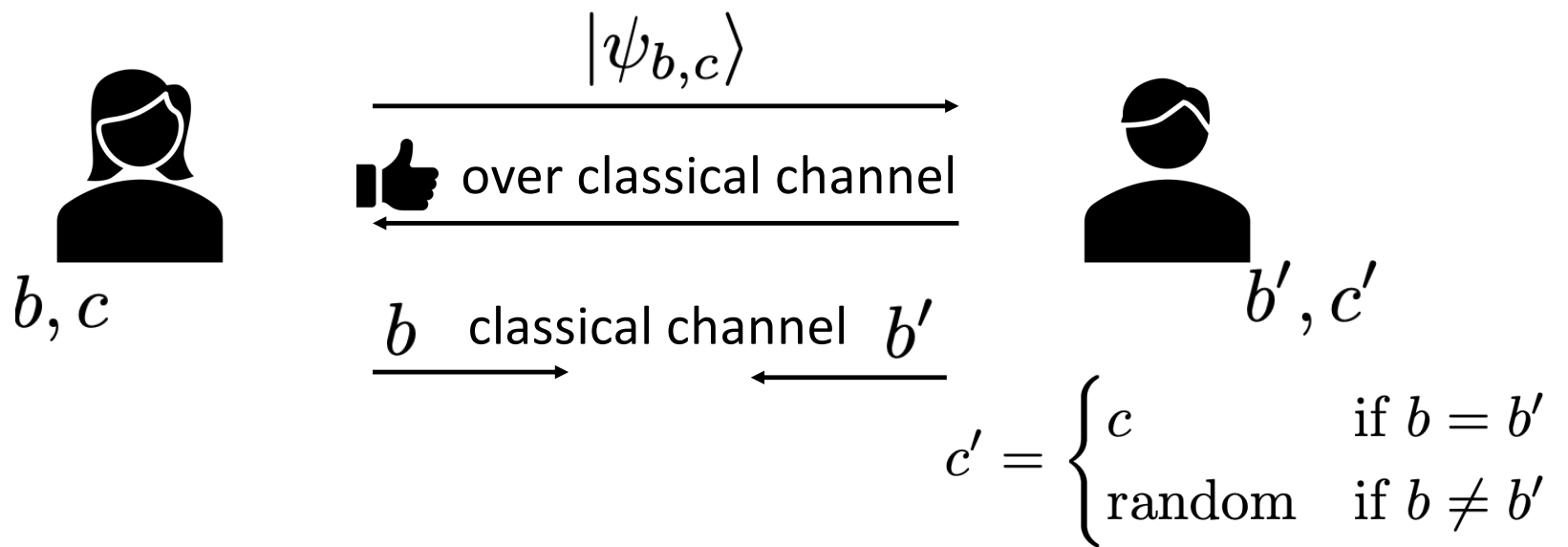
$$\mathbf{H}^{b'} |\psi_{b,c}\rangle = \mathbf{H}^{b'+b} |c\rangle = \mathbf{H}^{b' \oplus b} |c\rangle \Rightarrow \boxed{\text{circuit diagram}} \Rightarrow c'$$

$$\text{If } b = b' : |c\rangle \Rightarrow \boxed{\text{circuit diagram}} \Rightarrow c' = c$$

$$\text{If } b \neq b' : \mathbf{H}|c\rangle \in \{|+\rangle, |-\rangle\} \Rightarrow \boxed{\text{circuit diagram}} \Rightarrow c' \text{ random}$$

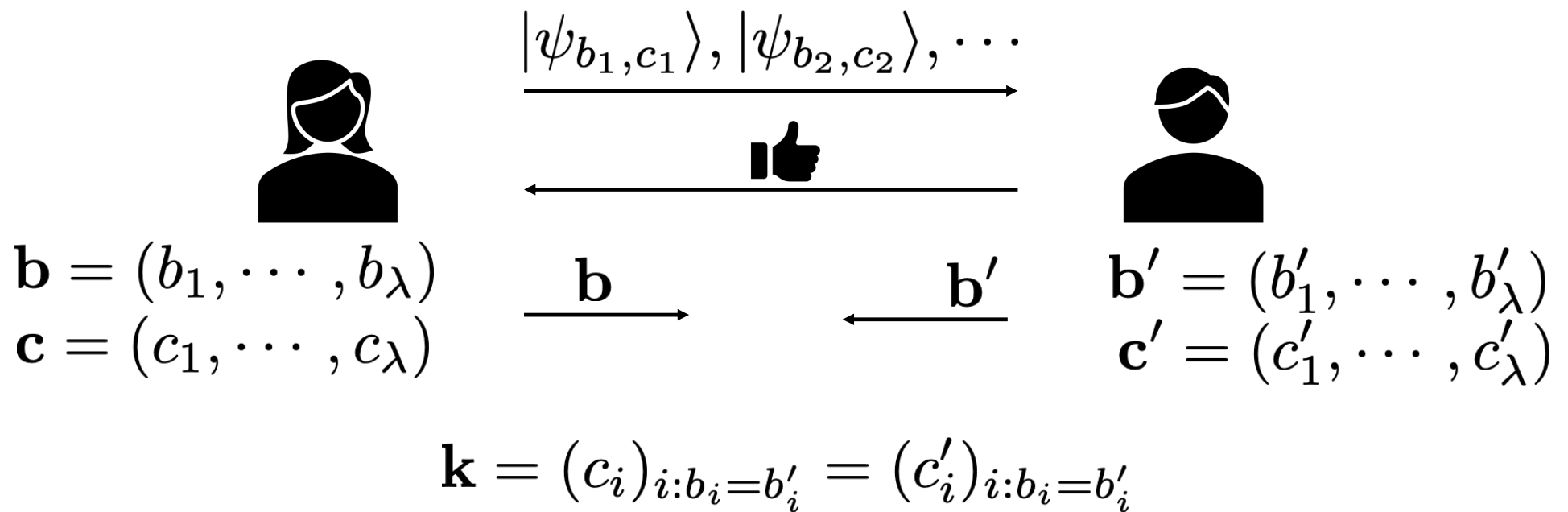






If  $b = b'$ ,  $k = c = c'$

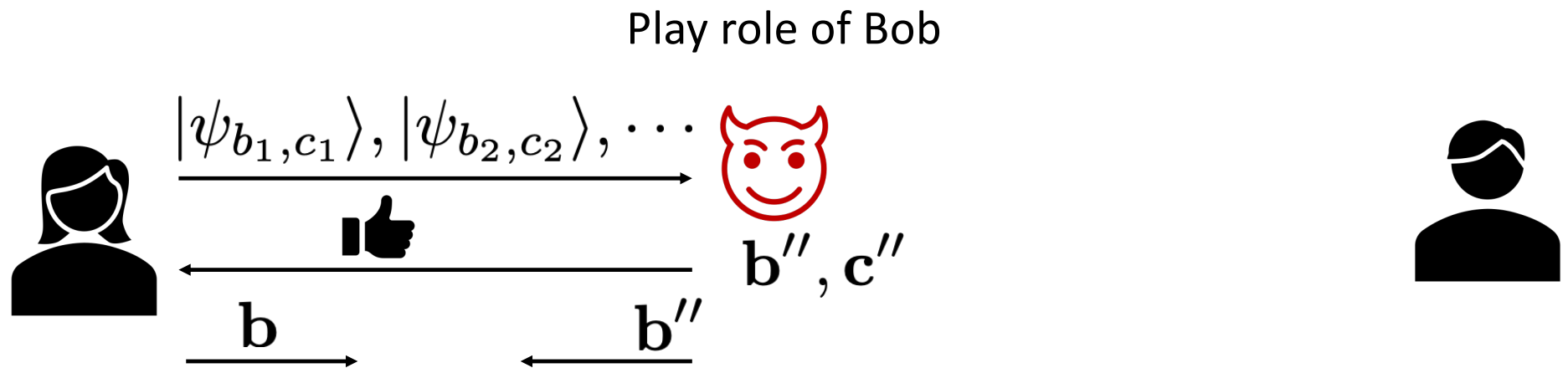
If  $b \neq b'$ , abort



Expected key length =  $\lambda/2$

Why do we need the classical channel to be authenticated?

# “Man-in-the-middle”

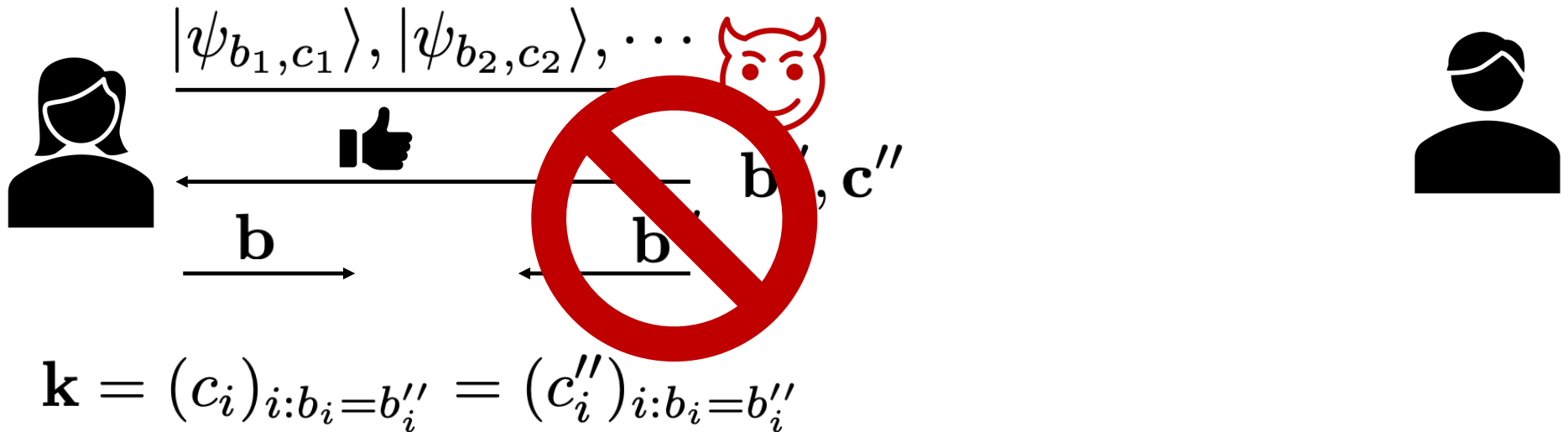


$$\mathbf{k} = (c_i)_{i:b_i=b''_i} = (c''_i)_{i:b_i=b''_i}$$

Adversary learns Alice's key entirely

# “Man-in-the-middle”

Play role of Bob



Fortunately, because the classical channel is authenticated, Alice cannot send these messages pretending to be Bob

Why not just assume the quantum channel is authenticated?

# Authentication → Encryption

Recall the observer effect: looking at the quantum channel changes it



An authenticated quantum channel cannot even be looked at! That is, authenticated quantum channels are necessarily already encrypted

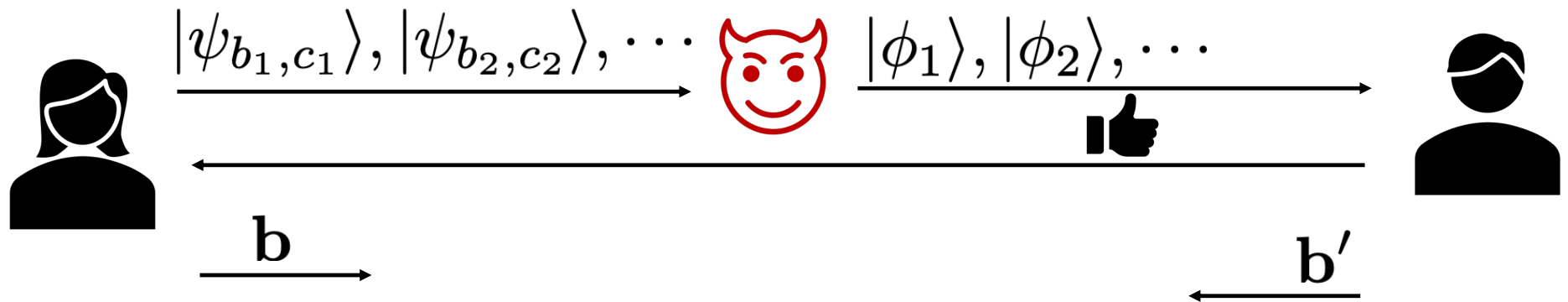


Encryption/key agreement is trivial/uninteresting if quantum channel is authenticated



Other possible attacks

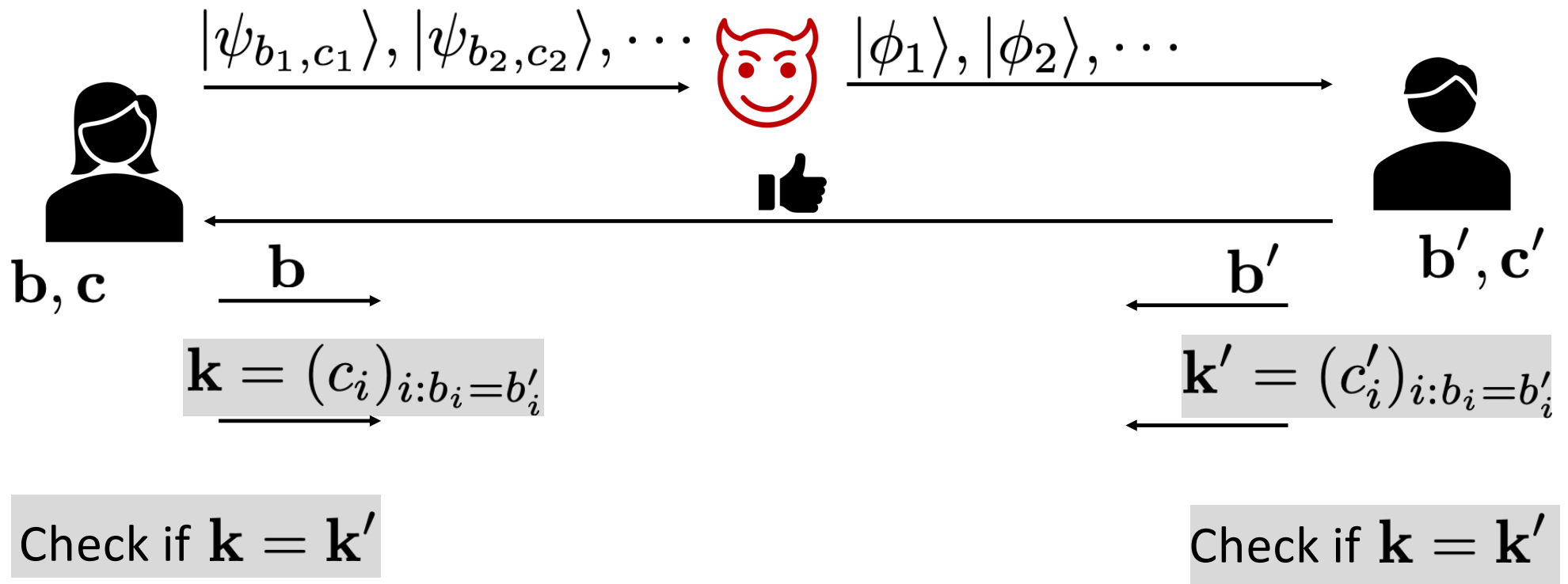
# The wait-and-see attack



$$\mathbf{H}^{b_i} |\psi_{b_i, c_i}\rangle = |c_i\rangle \Rightarrow \boxed{\text{Measurement}} \Rightarrow c_i$$

Adversary actually can learn  $\mathbf{c}$

# Catching Eavesdroppers



Since  $|\phi_i\rangle$  just an arbitrary state, unlikely  $\mathbf{k} = \mathbf{k}'$

**Problem:** to catch eavesdroppers, send  $\mathbf{k}, \mathbf{k}'$



Now Alice and Bob have no more secrets!

# Information-reconciliation

Ensure Alice and Bob have same key, while keeping that key secret

## Tool: 2-Universal Hash Function

**Def:** A family  $\mathcal{H}$  of functions  $h : \{0, 1\}^n \rightarrow \{0, 1\}^m$  is called **2-universal** if for all  $x, x' \in \{0, 1\}^n, x \neq x'$

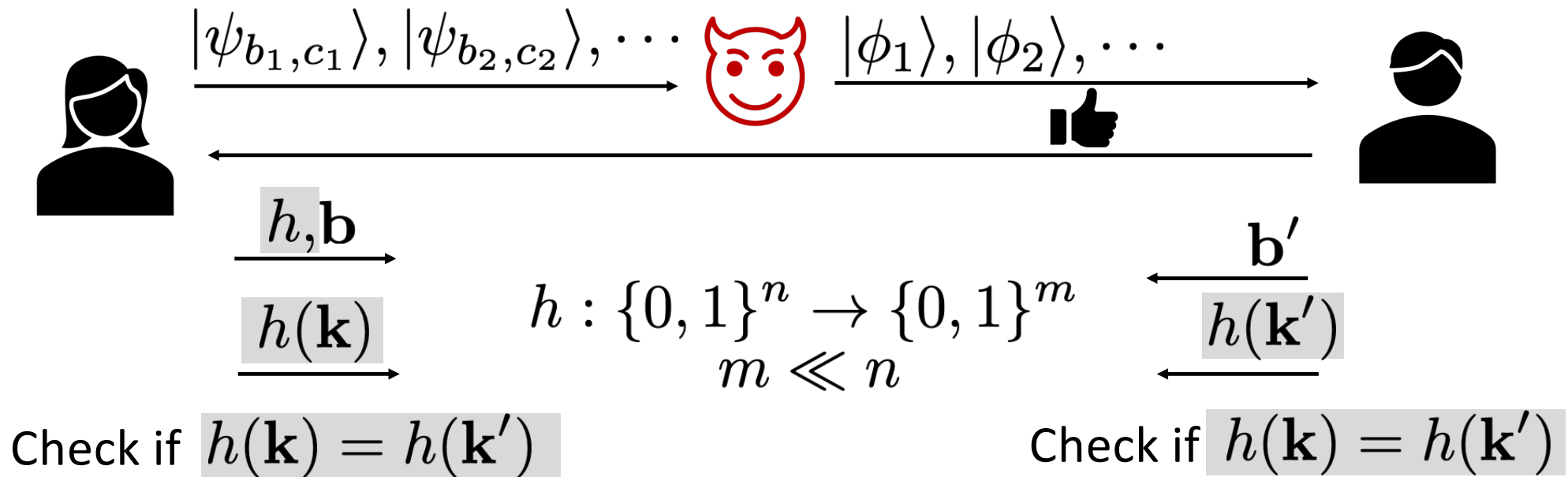
$$\Pr_{h \leftarrow \mathcal{H}} [h(x) = h(x')] = 2^{-m}$$

Example: random linear functions

$$\mathcal{H} = \{h_{\mathbf{a},b}\}_{\mathbf{a},b} \quad \text{where } h_{\mathbf{a},b}(\mathbf{x}) = \mathbf{a} \cdot \mathbf{x} + b$$

arithmetic over some finite field of size  $2^m$

# Information-reconciliation



Still unlikely that  $h(\mathbf{k}) = h(\mathbf{k}')$ , but now  $\mathbf{k}$  is still mostly hidden

# Information-reconciliation

In actual protocols, we are also worried about errors just do to random noise. As such, information-reconciliation doesn't just detect errors, but also tries to fix them



## Another Problem: $\mathbf{k}$ not completely hidden

- Information-reconciliation reveals information
- What if adversary only waits-and-sees on a single state, and otherwise just forwards the states?

➡ Constant probability  $\mathbf{k}, \mathbf{k}'$  stay same, while adversary still learns 1 bit

# Randomness Extraction / Privacy Amplification

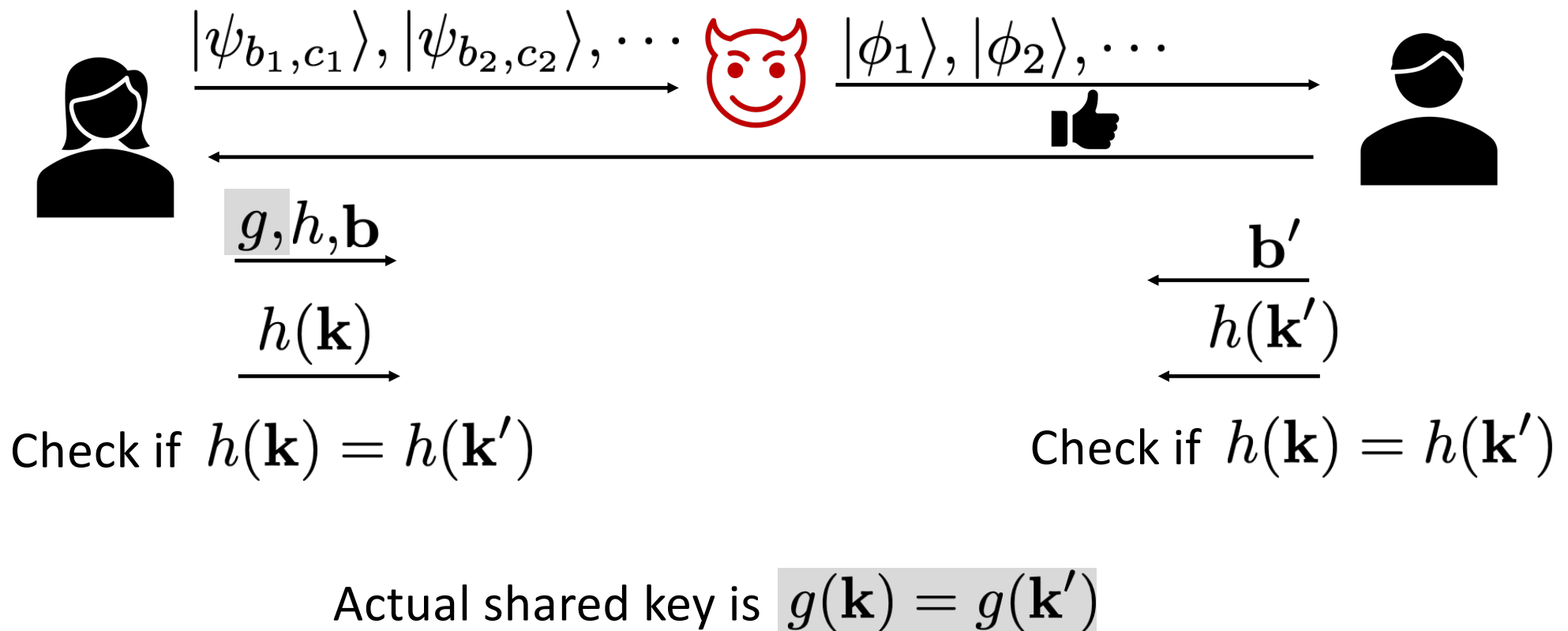
Conditioned on view of adversary,  $\mathbf{k}$  has entropy, but is non-uniform

Want to extract a uniform secret key

**Def (informal):** A function  $\text{Ext}(s, x)$  is a randomness extractor if, for all distributions  $X$  of sufficient “entropy”, for  $s$  drawn uniformly and for  $x \leftarrow X$ ,  $\text{Ext}(s, x)$  is close to uniform, even given  $s$

**Leftover Hash Lemma:** 2-universal hash functions are good randomness extractors

# Privacy Amplification



Other attacks are possible as well

- Guess  $b''$ , measure  $\mathbf{H}^{b''} |\psi_{b,c}\rangle \rightarrow c''$ , send  $|\psi_{b'',c''}\rangle$

May allow adversary some information  
about  $c$  while also having some chance of  
evading detection

- Measure  $U|\psi_{b,c}\rangle$  for different unitary  $U$
- Perform operations/measurements over multiple  $|\psi_{b,c}\rangle$

**Theorem (informal):** By instantiating protocol correctly, can achieve security against arbitrary eavesdroppers:

- Abort if eavesdropper looks at “too much” of quantum message
- If no abort, shared key is hidden to eavesdropper

QKD vs classical alternatives

# Authenticated-to-private Channels

QKD assumes as a resource an authenticated classical channel, and unconditionally converts it into a private channel against computationally unbounded adversaries

Public key encryption solves this classically, but only against computationally-bounded adversaries, and only under computational assumptions

Known to be impossible classically without computational bounds

But where does the authenticated classical channel come from?

Typically, from cryptography!

But then we're back to needing  
computationally-bounded adversaries and  
computational assumptions

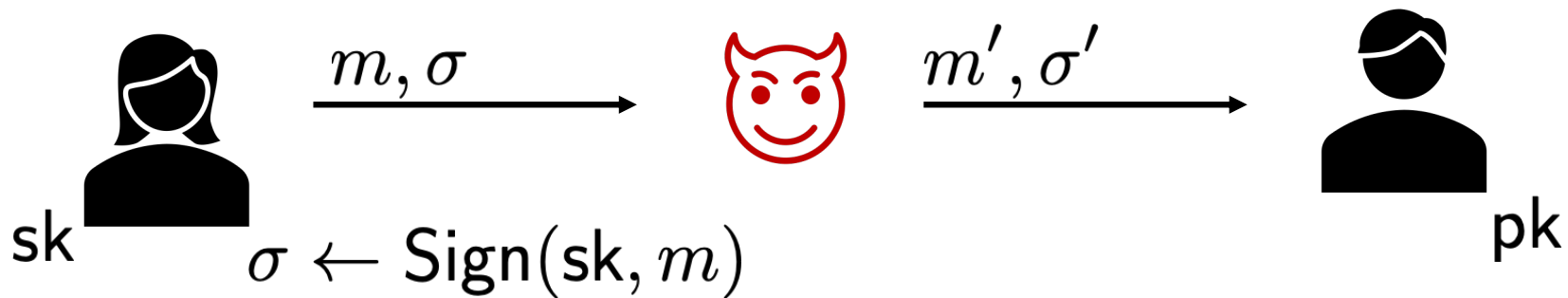


# Digital Signatures



# Digital Signatures

$$(\text{sk}, \text{pk}) \leftarrow \text{Gen}(1^\lambda)$$



$$0/1 \leftarrow \text{Ver}(\text{pk}, m, \sigma)$$

1 = “accept”, 0 “reject”

Security: impossible for adversary to generate valid signature on any message that wasn't signed by Alice

## Possible advantages of QKD

**Everlasting security:** as long as the adversary cannot break the authenticated channel during the protocol execution, the key will be secure even if the adversary later gains the power to break the authentication.

**Milder assumptions:** In theory, it is believed that classical authenticated channels can be obtained using milder computational assumptions than public key encryption. QKD only needs these milder assumptions

However, in practice, authentication uses the same assumptions as public key encryption

## Possible advantages of QKD

**Conceptual:** similar ideas come up in many other applications of quantum information, and QKD is an interesting test-bed for these ideas

Next time: more quantum:  
no-cloning and quantum money