CS 258: Quantum Cryptography

Mark Zhandry

Previously…

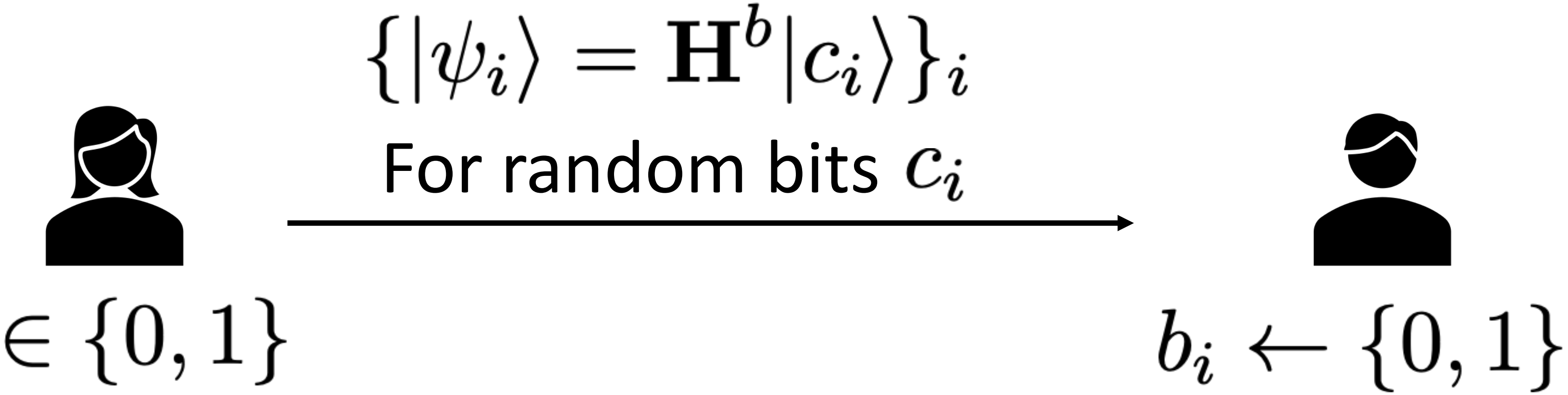
Dream inspired by QKD: maybe everything can be made information-theoretic!

Unfortunately, as with classical crypto, basically everything requires computational security

Example: quantum commitments

A protocol inspired by QKD

Commit phase:



$$\{|\psi_i\rangle = \mathbf{H}^b|c_i\rangle\}_i$$

For random bits c_i

$b \in \{0,1\}$

$b_i \leftarrow \{0,1\}$

measure $\mathbf{H}^{b_i}|\psi\rangle = \mathbf{H}^{b_i \oplus b}|c_i\rangle$

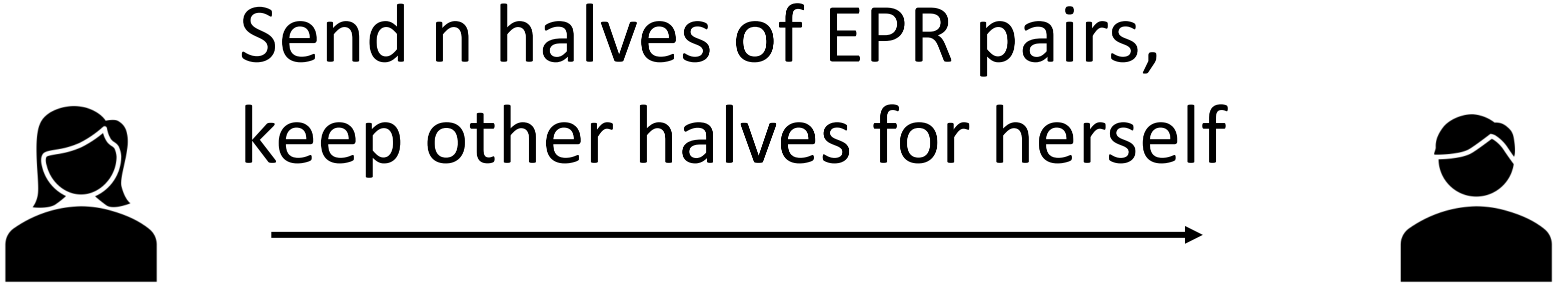
➡ c_i'

Roughly half the b_i will be correct ➡ $c_i' = c_i$

Roughly half the b_i will be incorrect ➡ c_i' uniform

EPR Attack

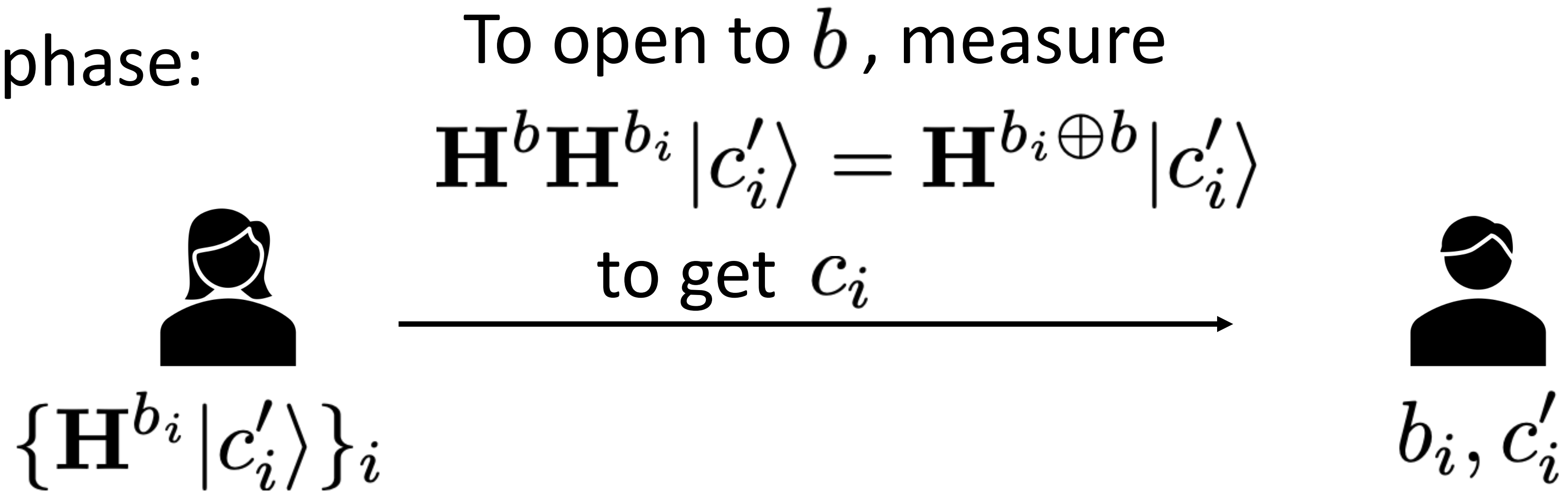
Commit phase:



Send n halves of EPR pairs, keep other halves for herself

Recall: $|\mathsf{EPR}\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$

Reveal phase:



To open to b, measure

$$\mathbf{H}^{b}\mathbf{H}^{b_i}|c_i'\rangle = \mathbf{H}^{b_i \oplus b}|c_i'\rangle$$

to get c_i

$\{\mathbf{H}^{b_i}|c_i'\rangle\}_i$

b_i, c_i'

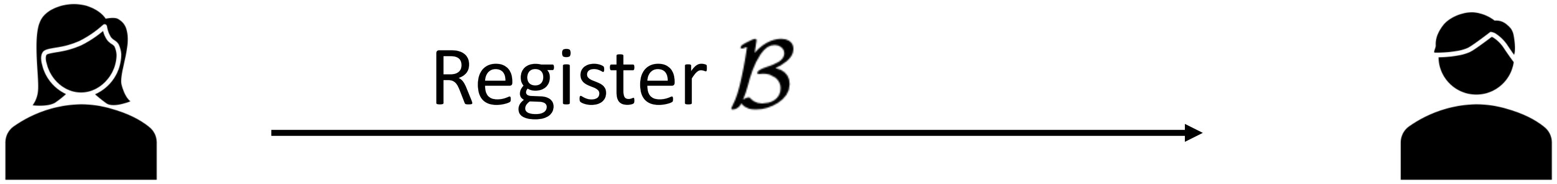
Roughly half the b_i will be correct ➡ $c_i' = c_i$

Roughly half the b_i will be incorrect ➡ c_i' uniform

Theorem: No commitment can be both statistically binding and hiding

Canonical commitment

Commit phase:



Register $\mathcal{B}$

Alice prepares $|\psi_b\rangle_{\mathcal{A},\mathcal{B}}$

Reveal phase:

b , Register $\mathcal{A}$

Checks if joint system is $|\psi_b\rangle$

Statistical hiding implies:

$$|\psi_0\rangle = \sum_i \sqrt{d_i}|\tau_i^0\rangle|\gamma_i\rangle \qquad |\psi_1\rangle = \sum_i \sqrt{d_i}|\tau_i^1\rangle|\gamma_i\rangle$$

Since $\{|\tau_i^0\rangle\}_i$ and $\{|\tau_i^1\rangle\}_i$ are each orthonormal sets, there exists a unitary W mapping between them

Alice’s Binding Attack

- Commit to 0
- Later open to 1 by applying W

Today: quantum commitments even if P=NP

Thm: If P=NP, classical commitments impossible

Intuition: Alice sends $c = \mathsf{Com}(m;r)$ to Bob

Two cases:

- c statistically binds to m

Bob can use NP solver to find satisfying assignment to

$$C(m,r) = (c == \mathsf{Com}(m;r))$$

➡ Must reveal m

Thm: If P=NP, classical commitments impossible

Intuition: Alice sends $c = \mathsf{Com}(m; r)$ to Bob

Two cases:

- c statistically hides m

Alice can use NP solver to find satisfying assignment to

$$C(m', r') = (c == \mathsf{Com}(m', r') \wedge m' \neq m)$$

➡ Must reveal valid opening (m', r') with $m' \neq m$

Last time, we saw that commitments require some computational bound

But unclear how to adapt P=NP impossibility to quantum setting

$$|\psi_0\rangle = \sum_i \sqrt{d_i}|\tau_i^0\rangle|\gamma_i\rangle \qquad |\psi_1\rangle = \sum_i \sqrt{d_i}|\tau_i^1\rangle|\gamma_i\rangle$$

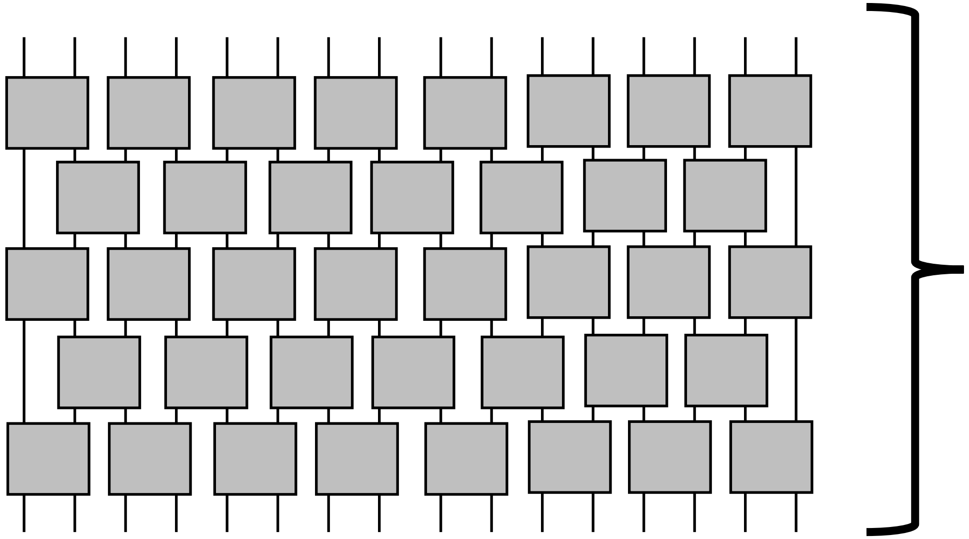
Alice needs to map $|\tau_i^0\rangle$ to $|\tau_i^1\rangle$

This is in general a unitary transformation. Unclear how Alice would solve this with a (classical or quantum) procedure for NP, which computes a function

Candidate commitments in a world where P=NP

Let U_0, U_1 be two "random" circuits on 3λ qubits

Ex: random brickwork:



Depth somewhat larger than 3λ

Random 2-qubit unitaries

Candidate commitments in a world where P=NP

$$|\psi_b\rangle = U_b|0^{3\lambda}\rangle$$

Alice’s system $\mathcal{A}$ = first 2λ qubits

Bob’s system $\mathcal{B}$= last λ qubits

Lemma: The protocol is statistically hiding. More precisely, Bob’s state is very close to the maximally mixed state, regardless of bit being committed

Reason: a random circuit generates the quantum analog of “2-universal” random quantum states

For such states, if you look at any subsystem with much less than half the qubits, the state looks maximally mixed

Because the protocol is statistically hiding,
we know it cannot be statistically binding

In fact:

$$|\psi_0\rangle \approx \frac{1}{\sqrt{2^\lambda}} \sum_i |\tau_i^0\rangle |i\rangle \qquad\qquad |\psi_1\rangle \approx \frac{1}{\sqrt{2^\lambda}} \sum_i |\tau_i^1\rangle |i\rangle$$

While there must exist a unitary mapping $|\tau_i^0\rangle$ to $|\tau_i^1\rangle$,
it is not clear how to derive such a unitary from U_0, U_1

Theorem: If U_0, U_1 modeled as random black box unitaries, then the protocol is computationally binding

Provides some evidence that the protocol is binding, even if we cannot prove it

Now what if P = NP?

We want to give some justification that the commitment scheme remains secure, even in this case

Black-box Separations

Used to argue that A does not imply B, where A,B are complexity-theoretic or cryptographic statements

A = “Commitments exist” B = “P != NP”

Equiv. A = “P=NP” B = “Commitments don’t exist”

Challenge

Typical crypto statement:

$A \Longrightarrow B$ equiv: $\neg B \Longrightarrow \neg A$, or even $\neg A \vee B$

e.g. LWE $\Longrightarrow$ PKE

P = NP $\Longrightarrow$ classical commitments don’t exist

Sometimes additionally have converse

e.g. LWE $\Longleftrightarrow$ particular PKE is secure

Challenge

With A $\Longrightarrow$ B or A $\Longleftrightarrow$ B, we are formally making no statements about whether A is true or false, just drawing an implication

Of course, we usually believe A (and hence B) to be true, but the proof doesn’t show this

Challenge

For a separation, we are interested in:

$\neg (A \implies B)$ equiv: $A \land \neg B$

e.g. $\neg$ (P = NP $\implies$ quantum commitments don’t exist)

The only way this can be true is if **both** A is true and B is false

P = NP **and** quantum commitments exist

Both incredibly hard problems, and we believe P != NP!

Black-box Separations

Solution: provide oracle relative to which A is true but B is false

Takeaway: any techniques which work relative to oracles (“relativize”) are incapable of proving B from A

For example, all the security proofs we’ve seen in this course relativize, since they just treat adversary as a black box. It’s fine if that black box makes queries

Black-box Separations

Black-box separations must be interpreted with care, as there are non-relativizing techniques which famously circumvent certain impossibilities

So black-box separations usually interpreted as heuristic evidence, but far from a full proof

How to design a black box separation

Step 1: provide oracles relative to which A is true

Want commitments to exist. Natural choice of oracle is two random unitaries U_0, U_1

How to design a black box separation

Step 2: provide oracles relative to which B is false

Want P=NP. So give oracle

$$\mathsf{SAT}(C) = \begin{cases} 1 & \text{if } C(x) = 1 \text{ for some } x \\ 0 & \text{if there does not exist an } x \end{cases}$$

Clearly breaks all of NP

Must be careful!

We can do the same thing in the classical world:

To make commitments exist, give out a random oracle O

To make P = NP, give out an oracle SAT

But we know that “commitments exist” implies “P != NP”. Why not a contradiction?

Reason: “commitments exist” implies “P != NP” applies supposed NP solver to the commitment

But in this world, the commitment uses the random oracle. SAT doesn’t work on circuits that make oracle queries

Results in a rather meaningless separation, since it doesn’t even capture simple attacks

Instead, SAT should work on circuits that themselves can make oracle queries

Now such an oracle will break even commitments constructed using O

Thus in this world, P=NP and commitments don’t exist, so no separation

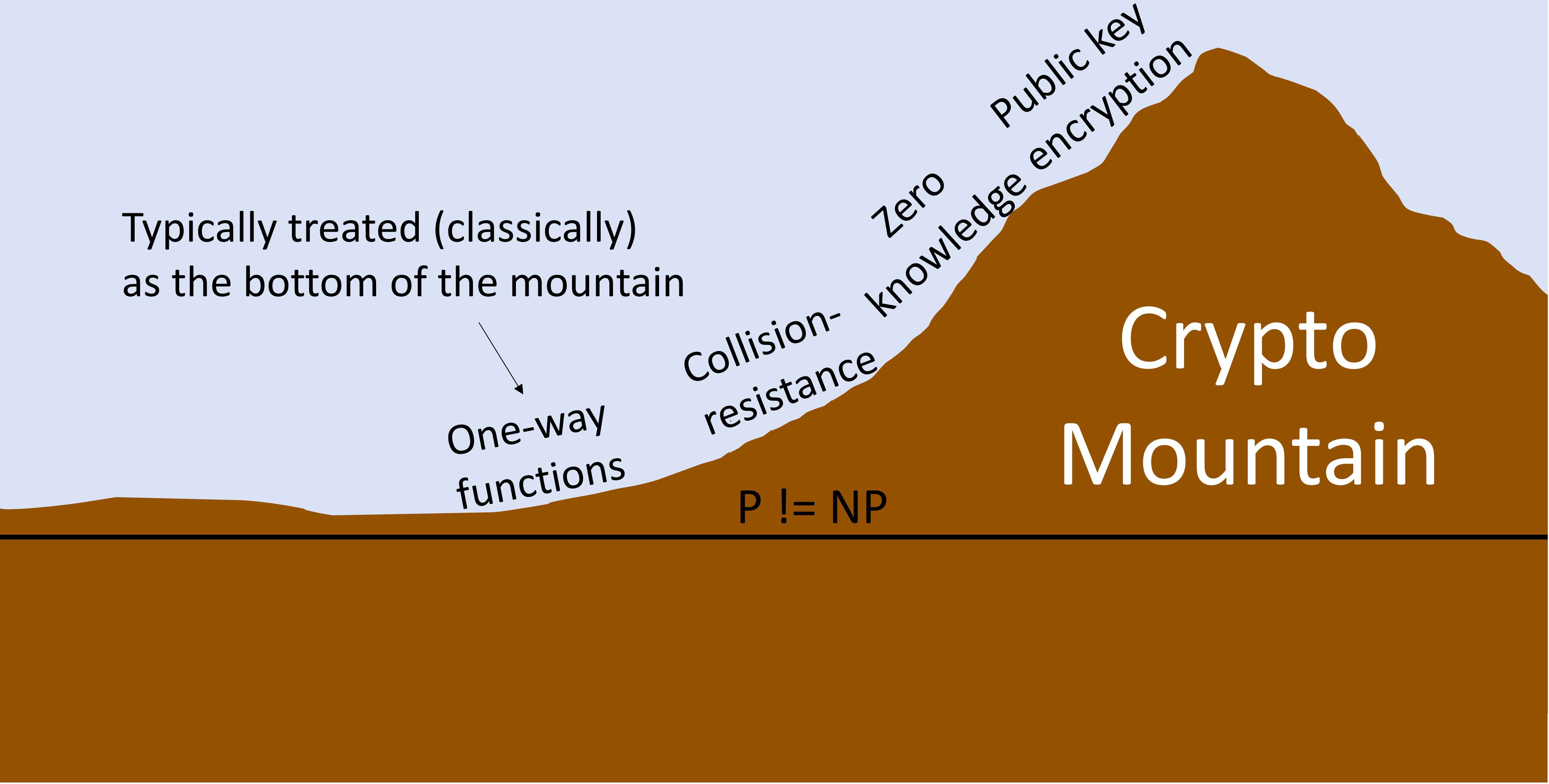
Back to quantum separation

If our commitment is built instead using U_0, U_1, it is natural to restrict circuits that are input to SAT from querying U_0, U_1. After all, SAT is supposed to work on classical circuits

Gives a meaningful separation, but perhaps unsatisfying since we restricted inputs to SAT from querying commitment oracles for trivial reasons

Turns out, it is actually possible to give a **classical** oracle relative to which commitments exist, even in the presence of an NP solver that works on circuits make queries to the classical oracle

Bigger picture



Typically treated (classically) as the bottom of the mountain

One-way functions

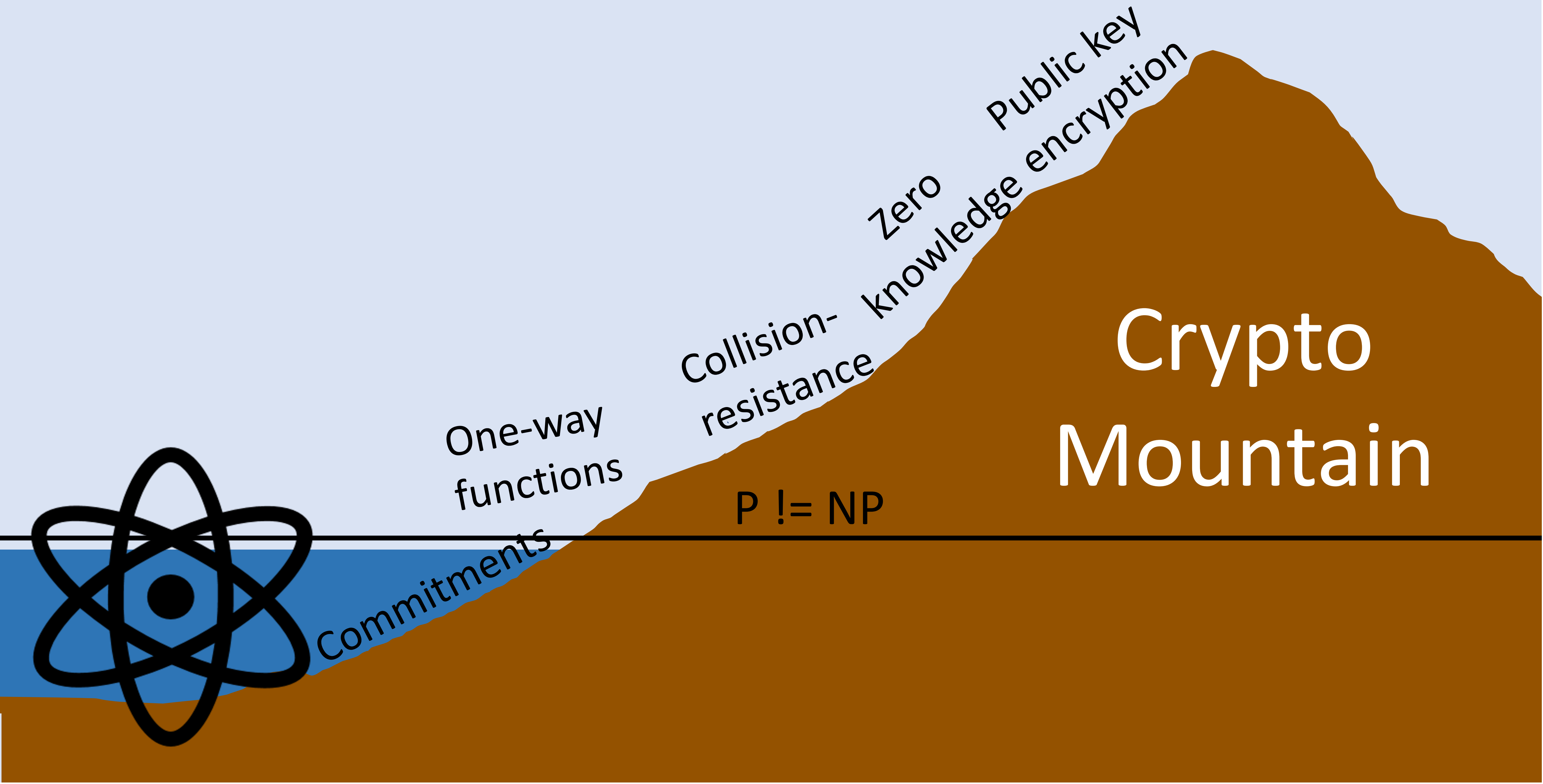
Collision-resistance

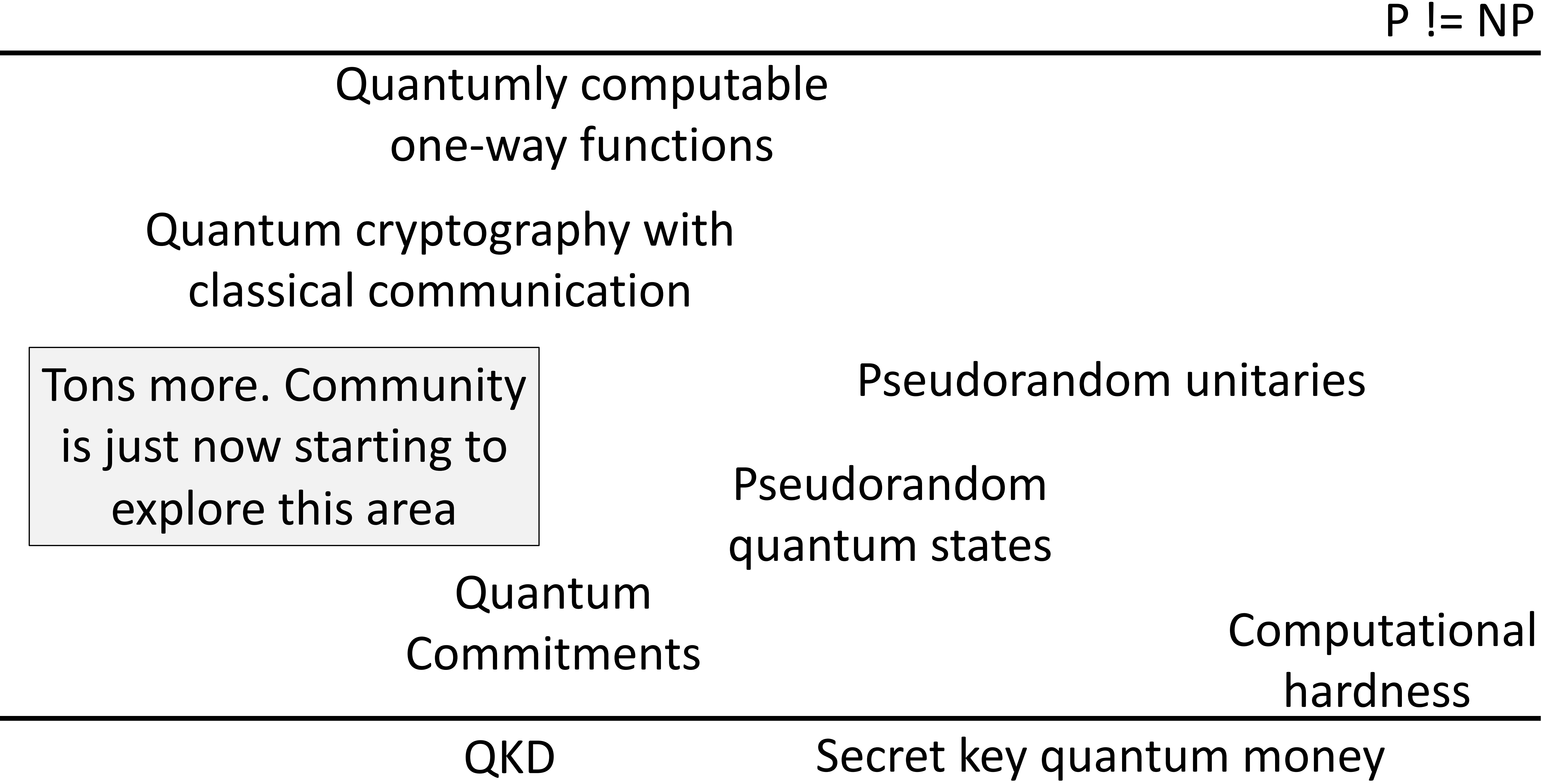
Zero knowledge

Public key encryption

Crypto Mountain

P != NP


Public key
encryption
Zero
knowledge
Collision-
resistance
One-way
functions
Commitments
P != NP
Crypto
Mountain



P != NP

Quantumly computable one-way functions

Quantum cryptography with classical communication

Tons more. Community is just now starting to explore this area

Pseudorandom unitaries

Pseudorandom quantum states

Quantum Commitments

Computational hardness

QKD

Secret key quantum money

Next week: Thanksgiving

Final week: quantum protocols achieving the impossible