On Central Primitives for Quantum Cryptography with Classical Communication

Kai-Min Chung, **Eli Goldin**, Matthew Gray

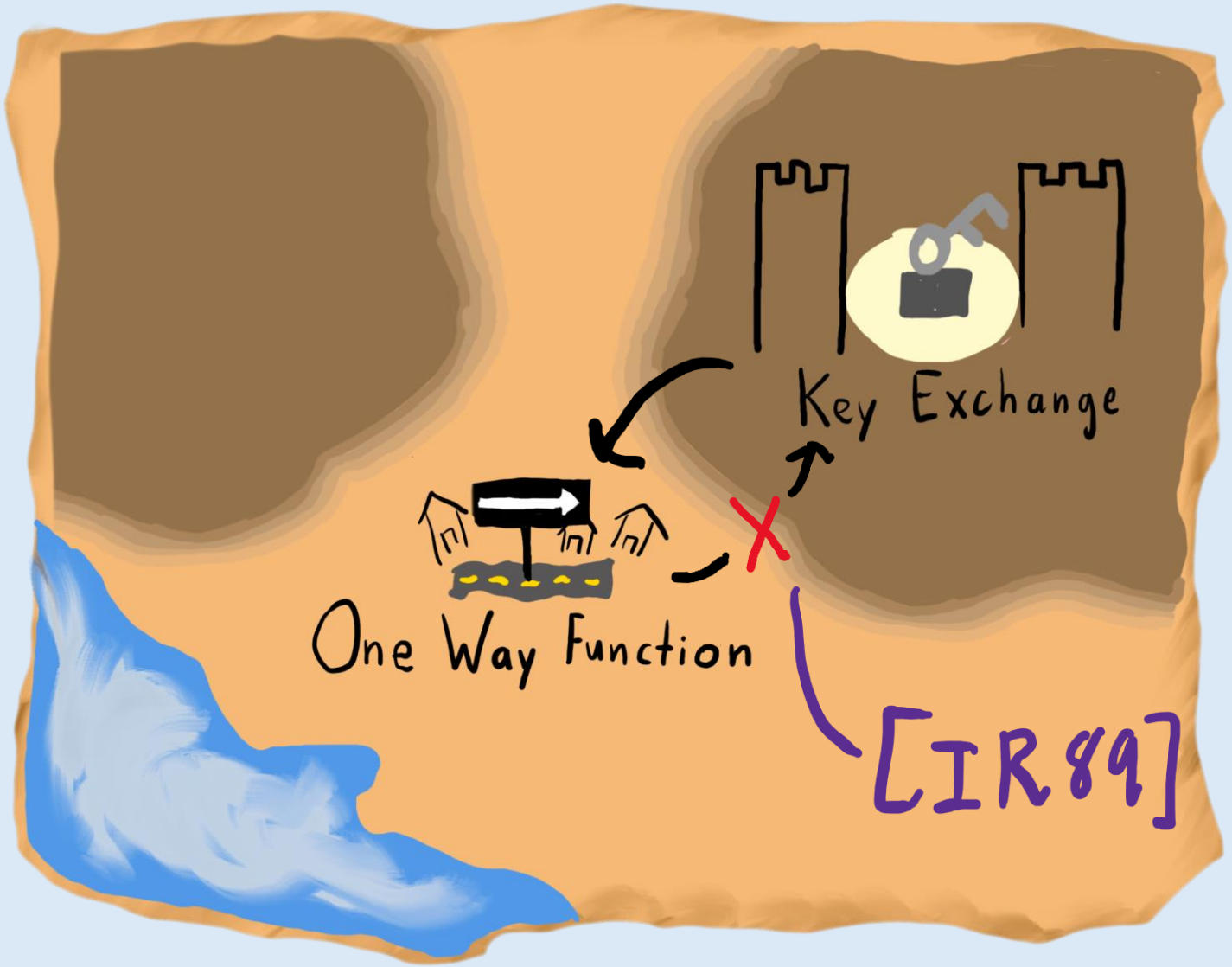
(Classical) Cryptography Topography

(Classical) Cryptography Topography

(Classical) Cryptography Topography

Key Exchange can be used to build one way functions

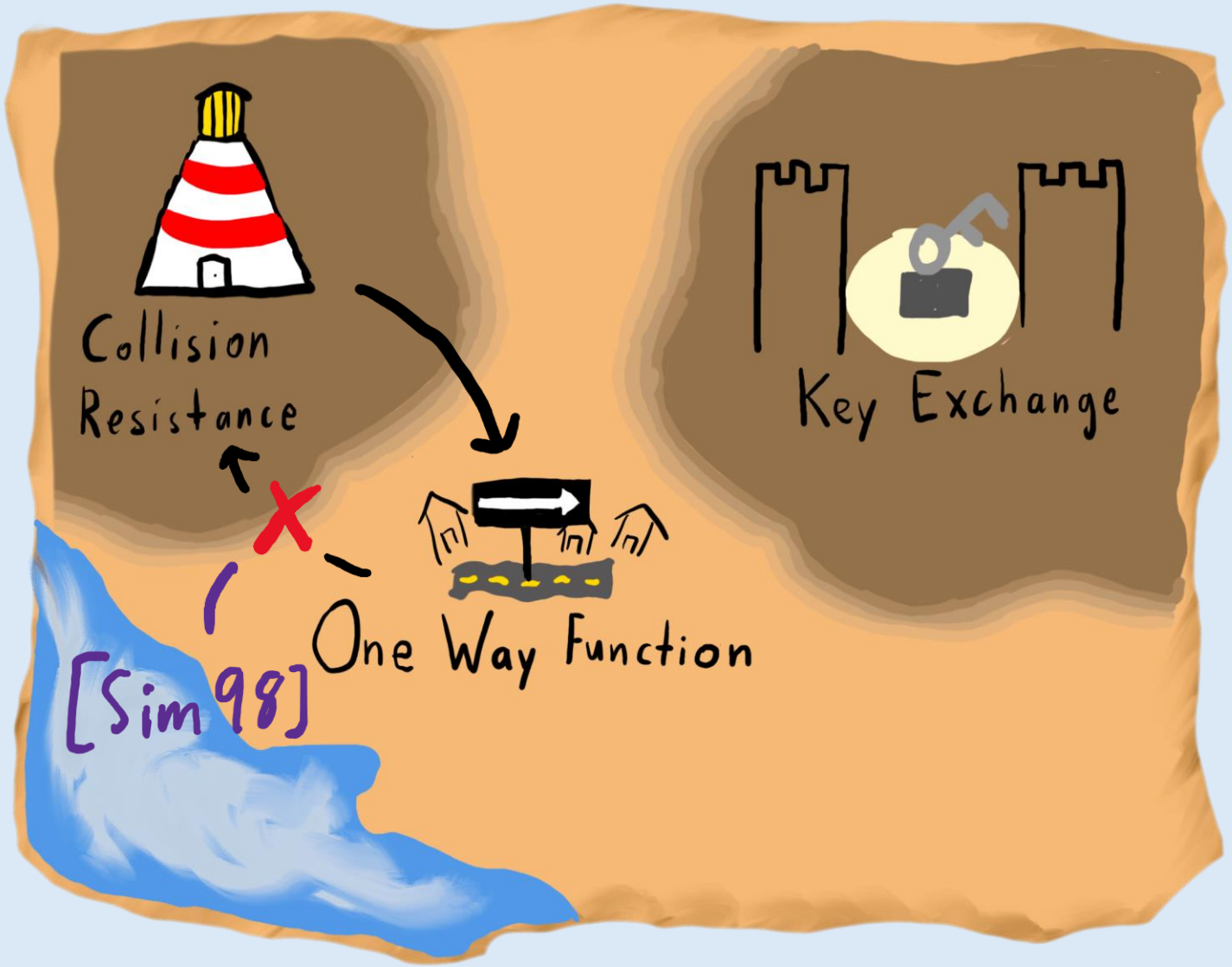
(Classical) Cryptography Topography



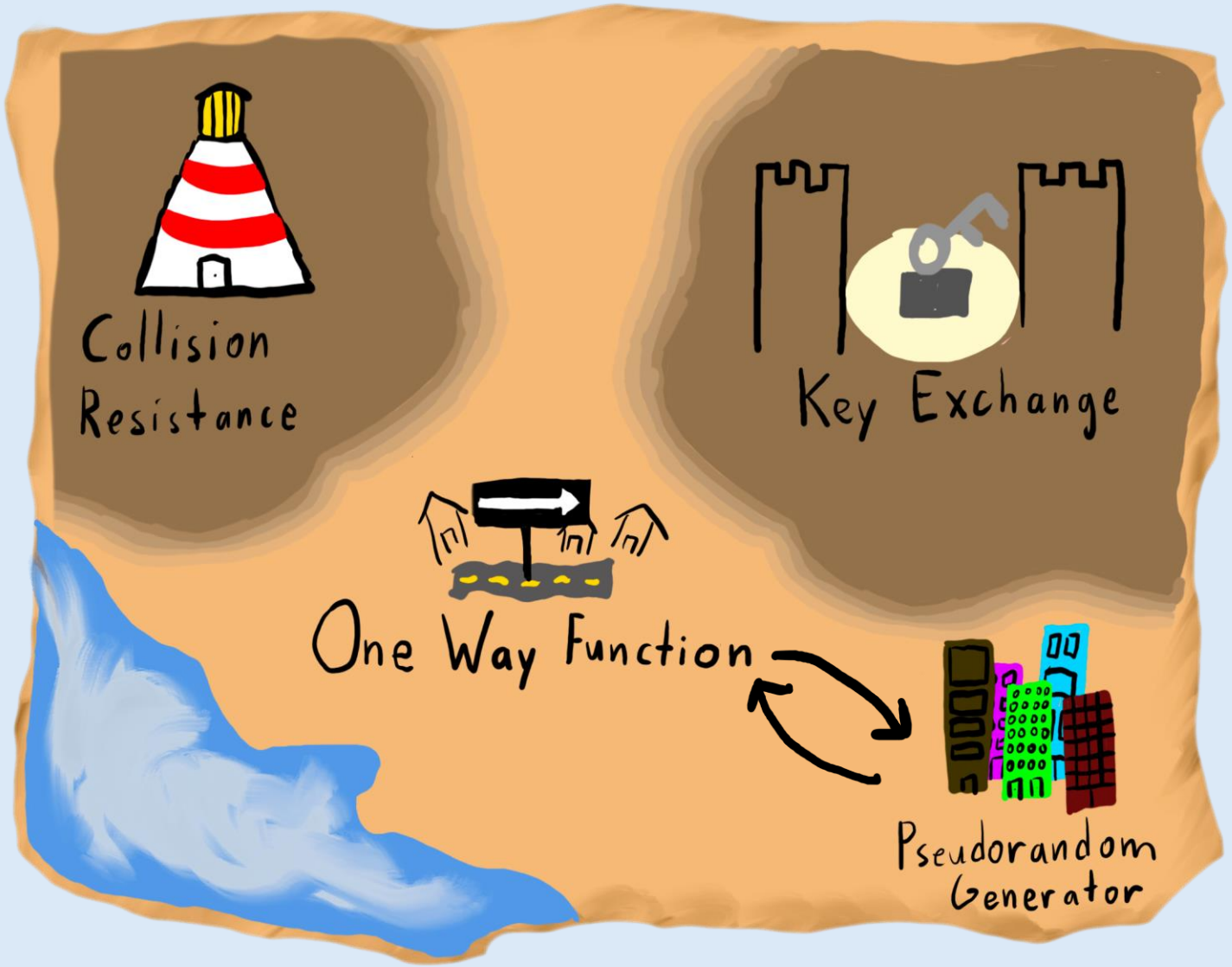
Key Exchange can be used to build one way functions

Hard to build KE from OWF

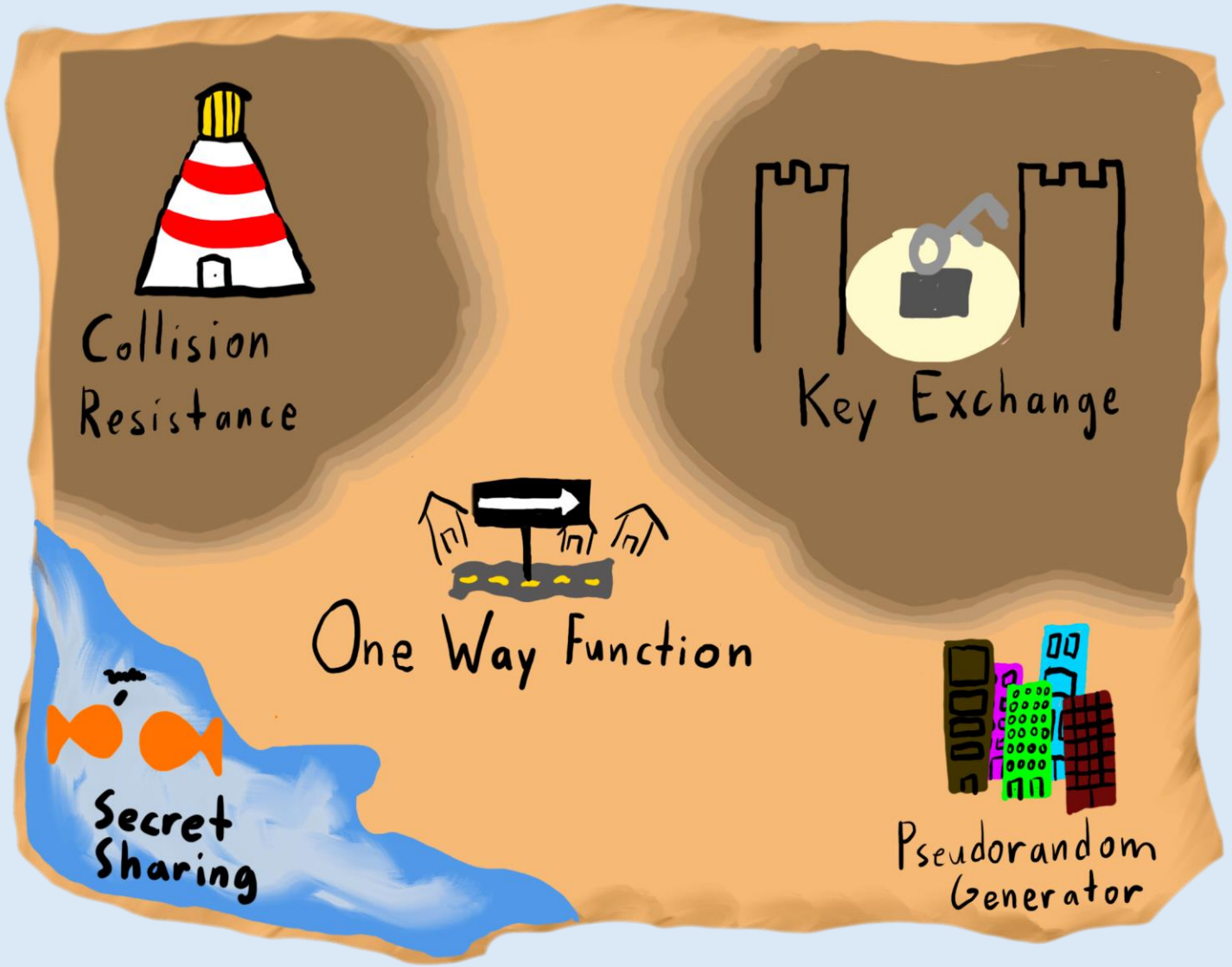
(Classical) Cryptography Topography



(Classical) Cryptography Topography

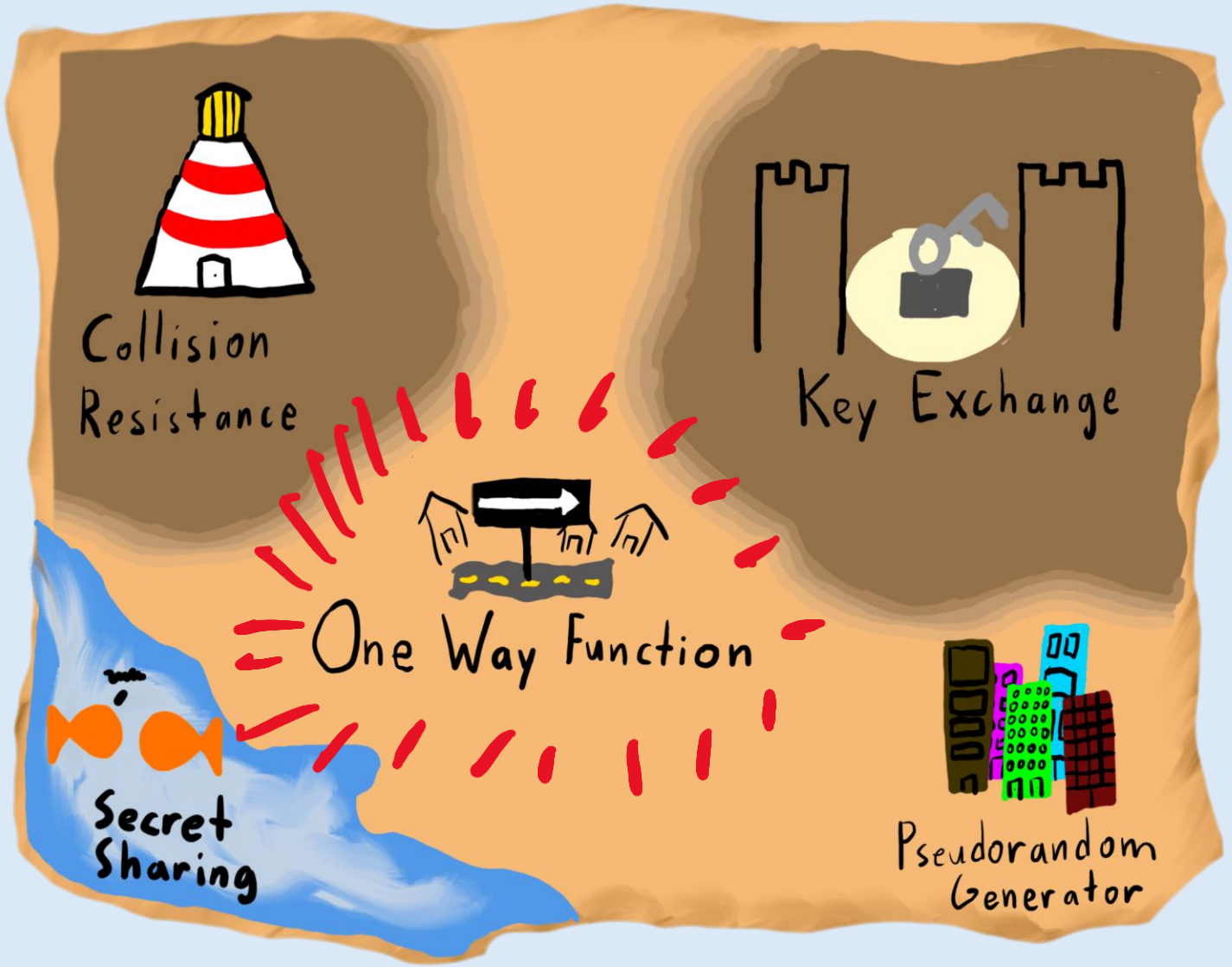


(Classical) Cryptography Topography



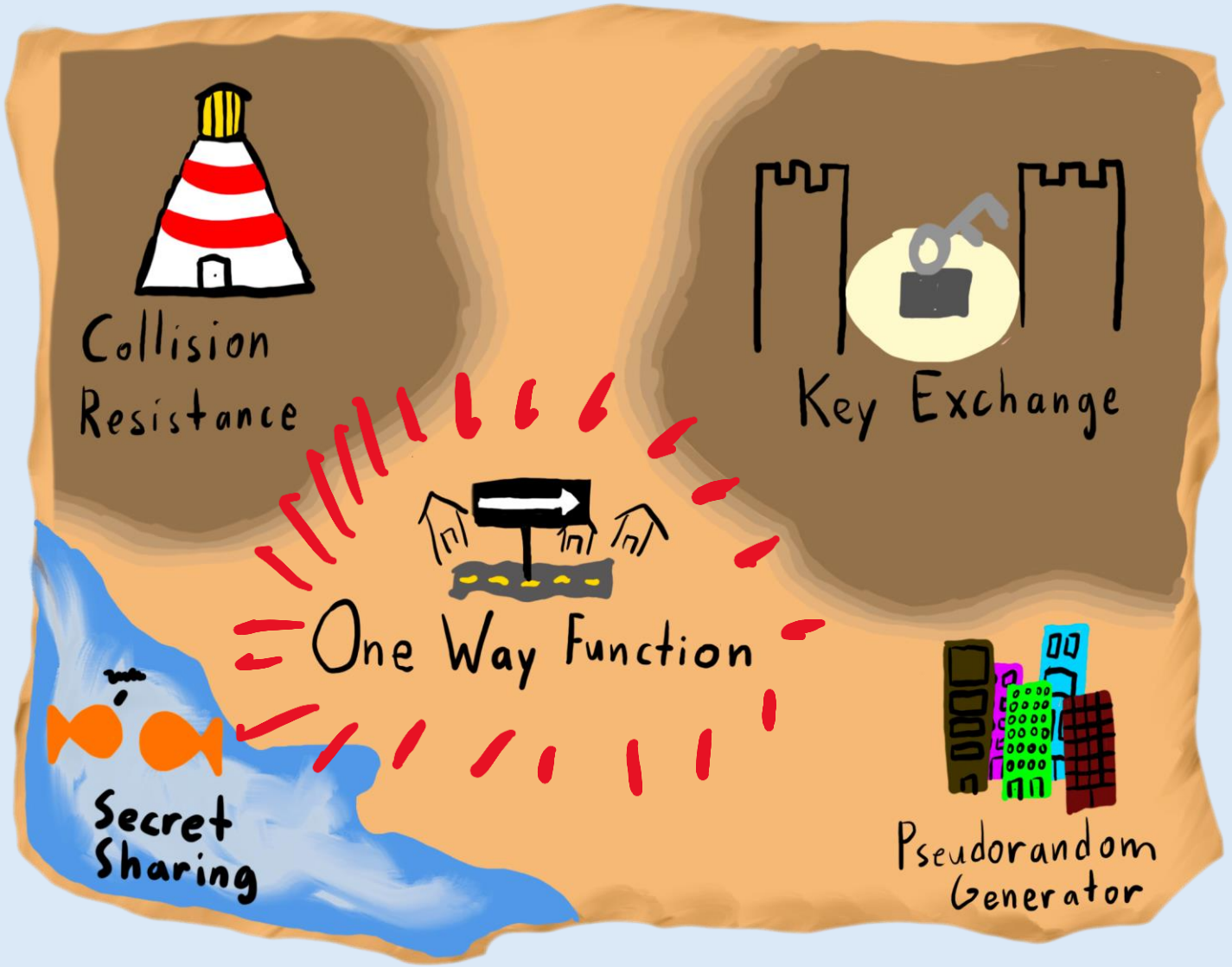
Secret sharing exists unconditionally (and has information theoretic security)

The Center of the World: OWFs



OWFs are special. Very useful starting place for understanding the map of Cryptography.

The Center of the World: OWFs



OWFs are special. Very useful starting place for understanding the map of Cryptography.

Why?

The Center of the World: OWFs

Why are one way functions so important?

1. Simple
2. Minimal
3. Useful
4. Flexible

The Center of the World: OWFs

Why are one way functions so important?

1. **Simple**: "Easy to compute, hard to invert"
2. Minimal
3. Useful
4. Flexible

The Center of the World: OWFs

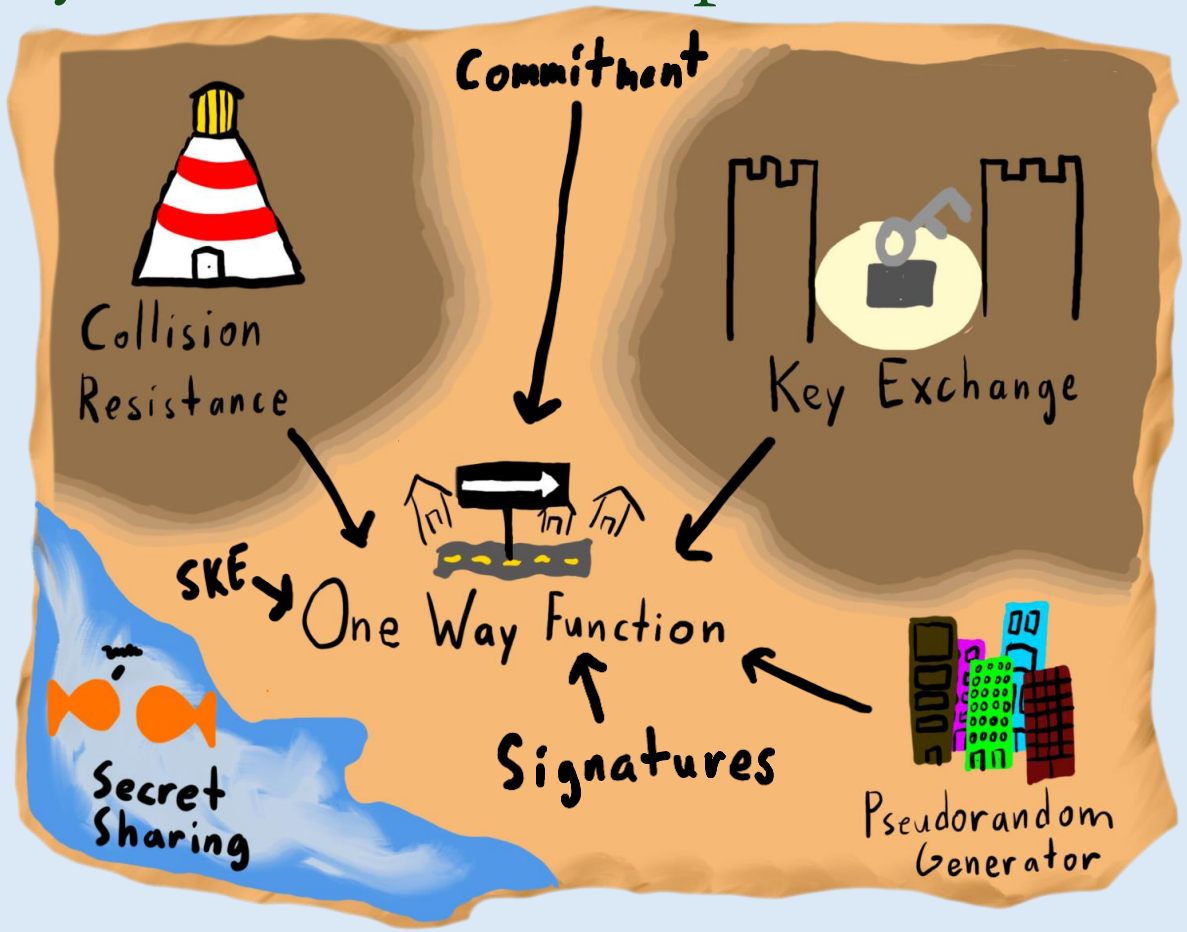
Why are one way functions so important?

1. Simple
2. **Minimal**
3. Useful
4. Flexible

The Center of the World: OWFs

Why are one way functions so important?

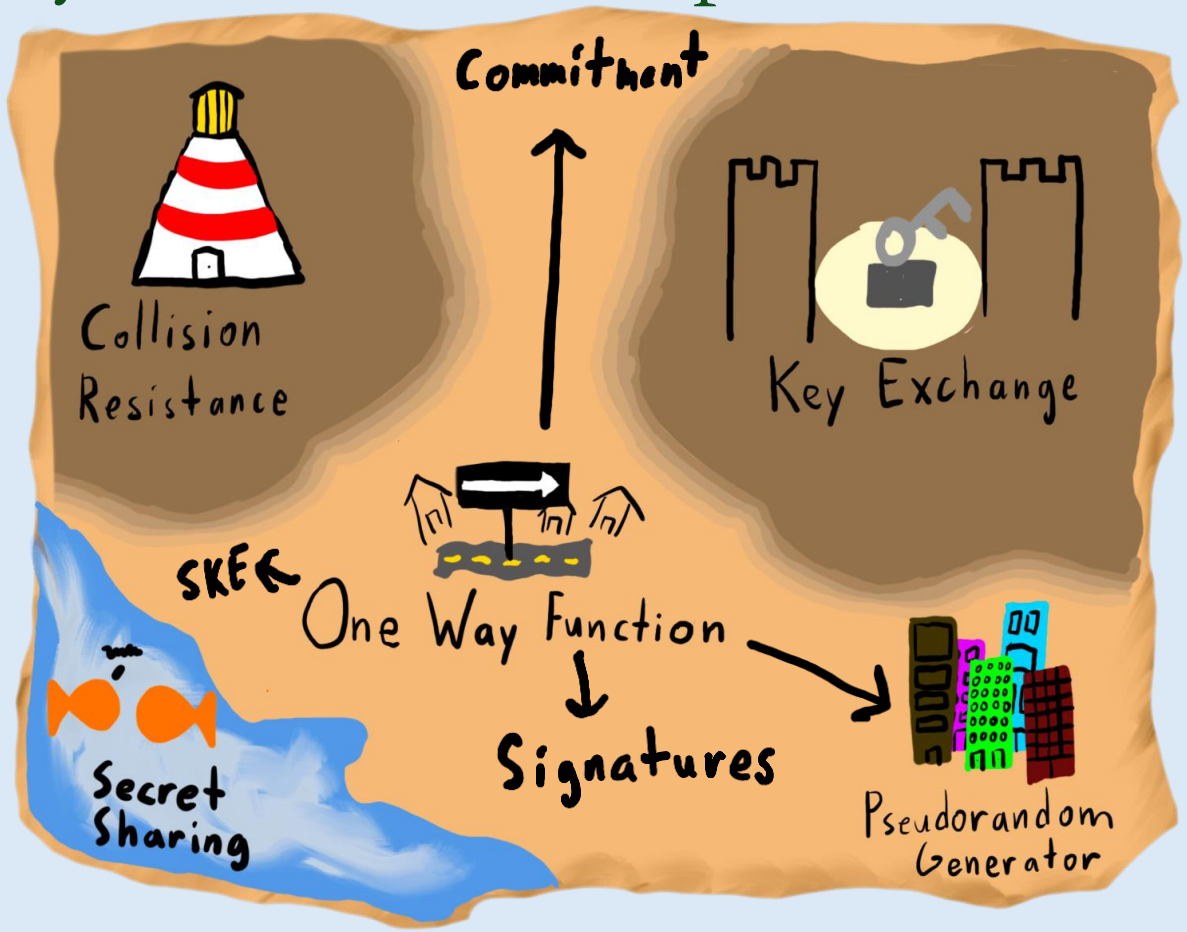
1. Simple
2. **Minimal**
3. Useful
4. Flexible



The Center of the World: OWFs

Why are one way functions so important?

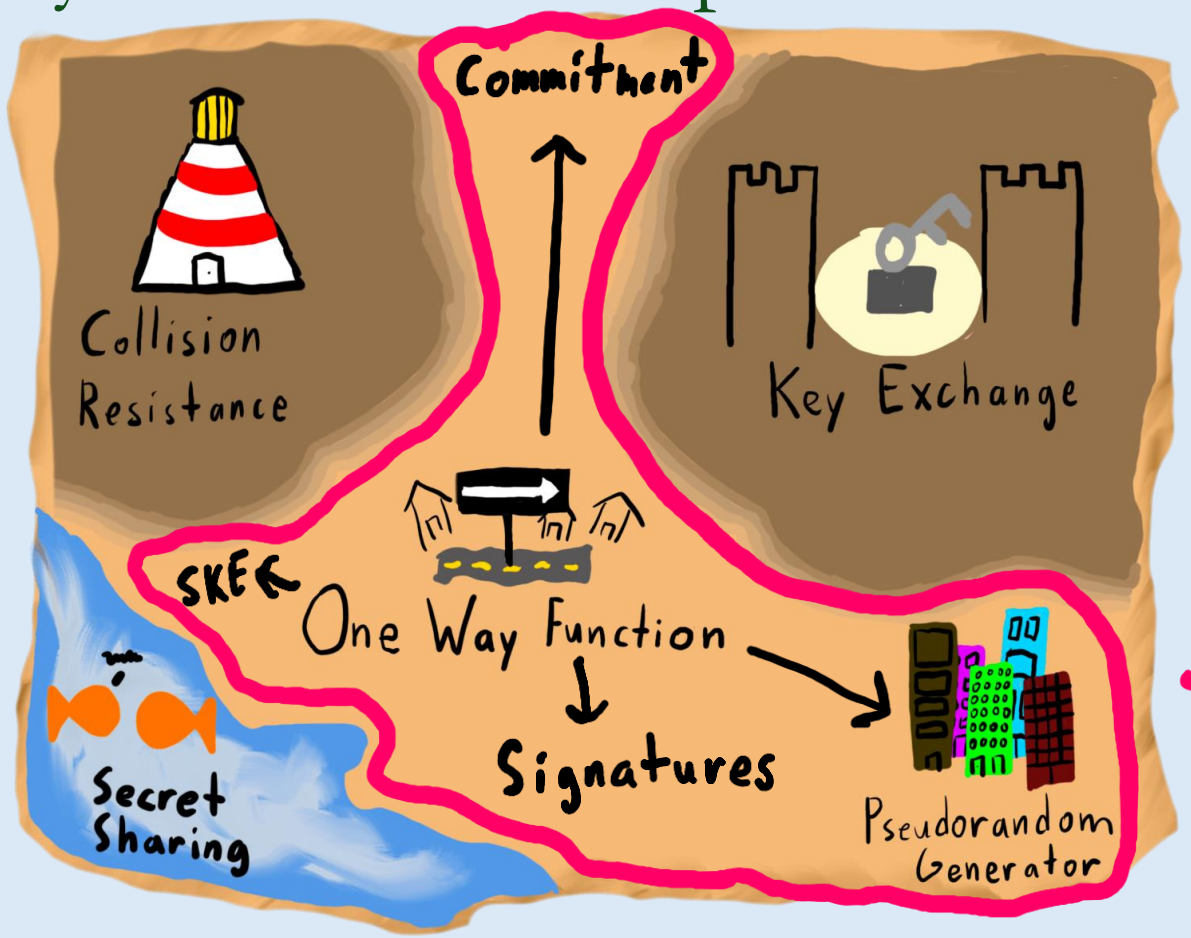
1. Simple
2. Minimal
3. **Useful**
4. Flexible



The Center of the World: OWFs

Why are one way functions so important?

1. Simple
2. Minimal
3. **Useful**
4. Flexible



MiniCrypt

The Center of the World: OWFs

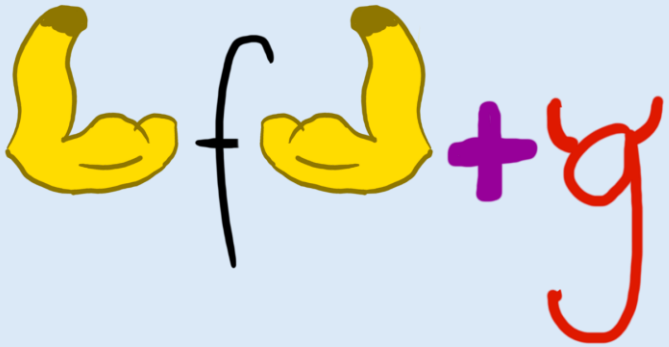
Why are one way functions so important?

1. Simple
2. Minimal
3. Useful
4. **Flexible**

The Center of the World: OWFs

Why are one way functions so important?

1. Simple
2. Minimal
3. Useful
4. **Flexible**

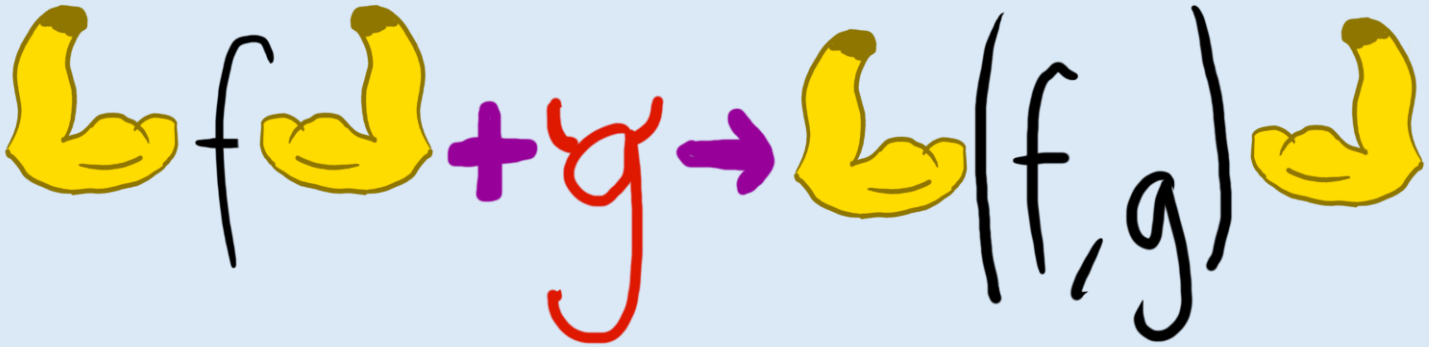


Combiners

The Center of the World: OWFs

Why are one way functions so important?

1. Simple
2. Minimal
3. Useful
4. **Flexible**

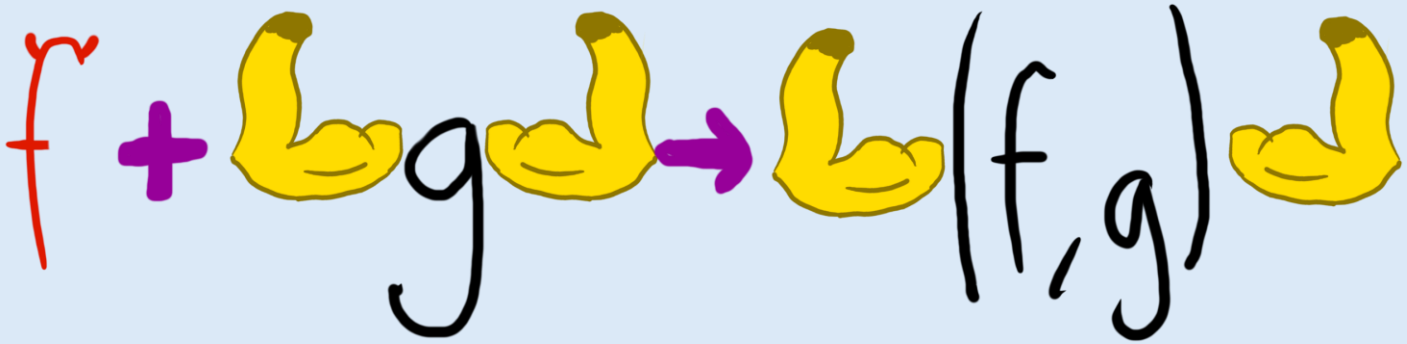


Combiners

The Center of the World: OWFs

Why are one way functions so important?

1. Simple
2. Minimal
3. Useful
4. **Flexible**

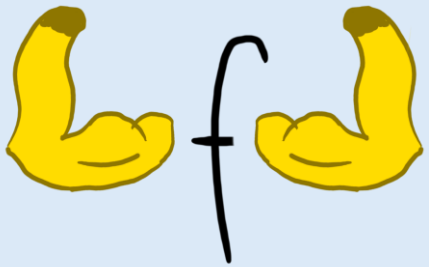


Combiners

The Center of the World: OWFs

Why are one way functions so important?

1. Simple
2. Minimal
3. Useful
4. **Flexible**

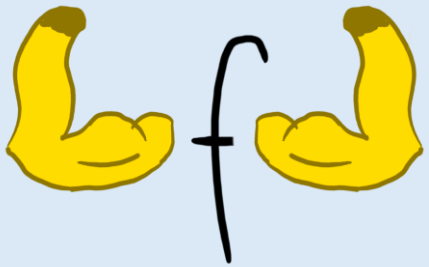


The Center of the World: OWFs

"strong" OWF

Why are one way functions so important?

1. Simple
2. Minimal
3. Useful
4. **Flexible**



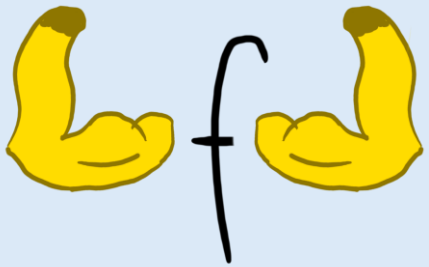
The Center of the World: OWFs

Why are one way functions so important?

1. Simple
2. Minimal
3. Useful
4. **Flexible**

"weak" OWF

"strong" OWF



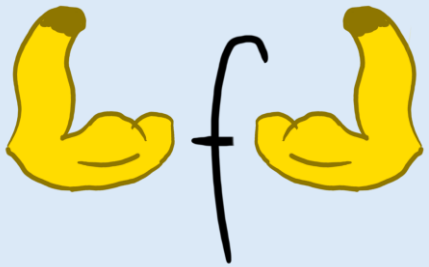
The Center of the World: OWFs

Why are one way functions so important?

1. Simple
2. Minimal
3. Useful
4. **Flexible**

"weak" OWF

"strong" OWF

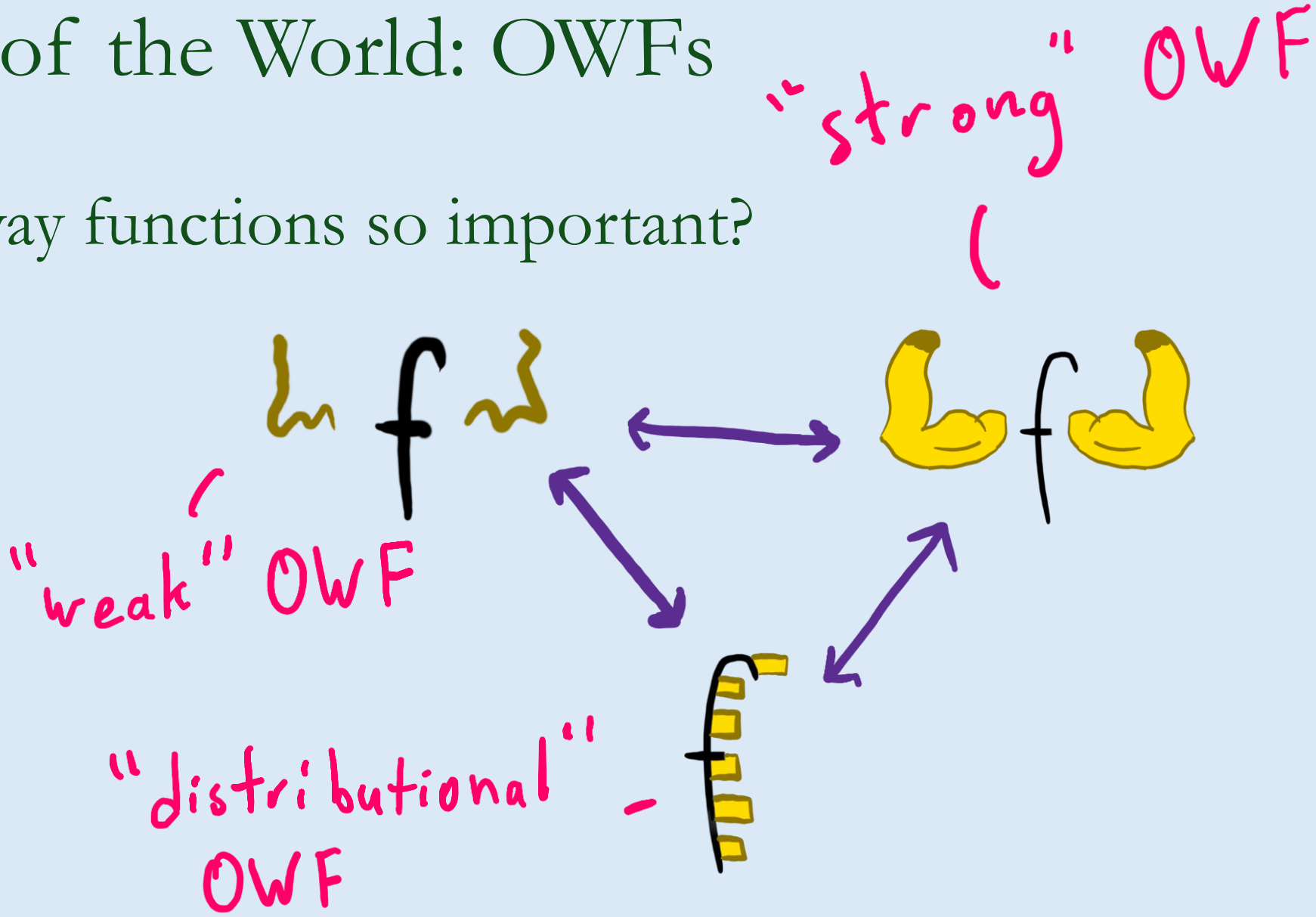


"distributional" OWF

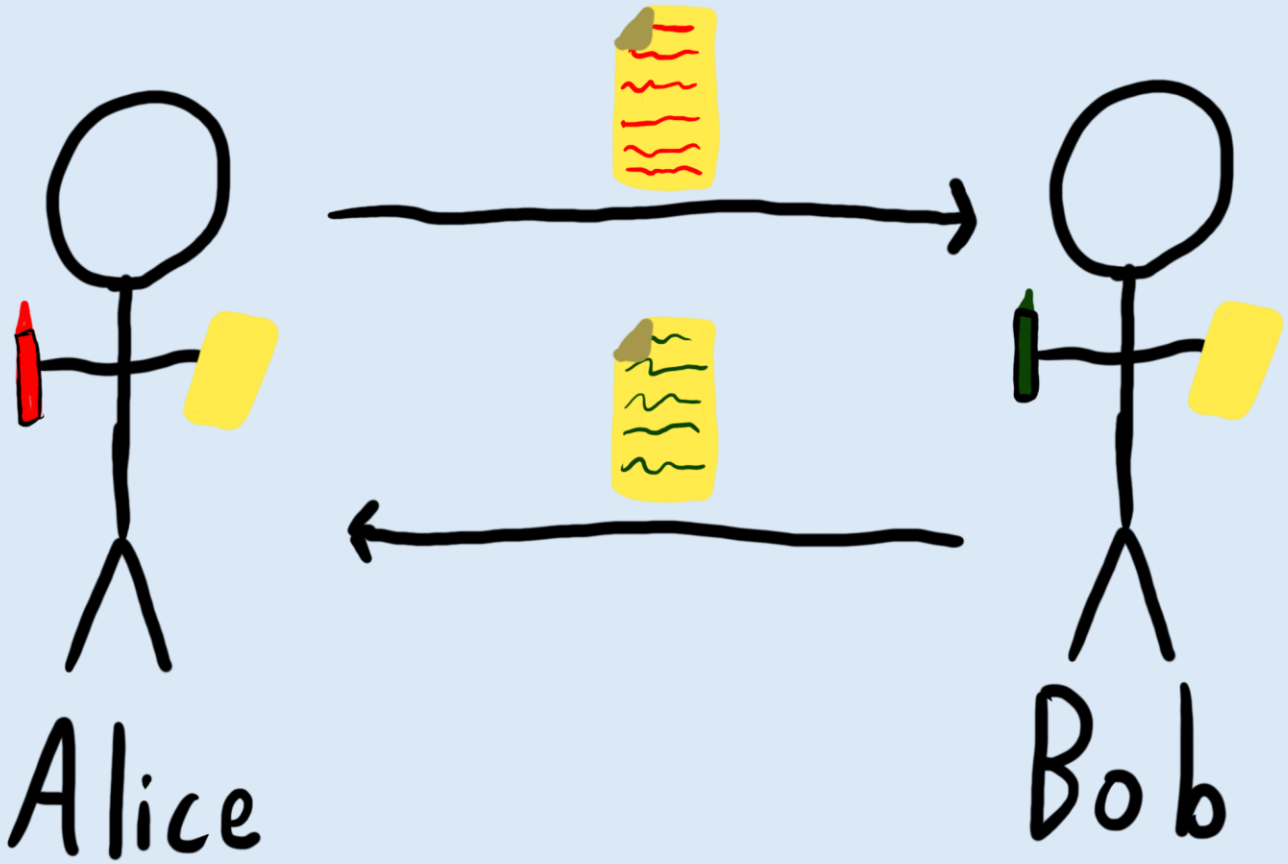
The Center of the World: OWFs

Why are one way functions so important?

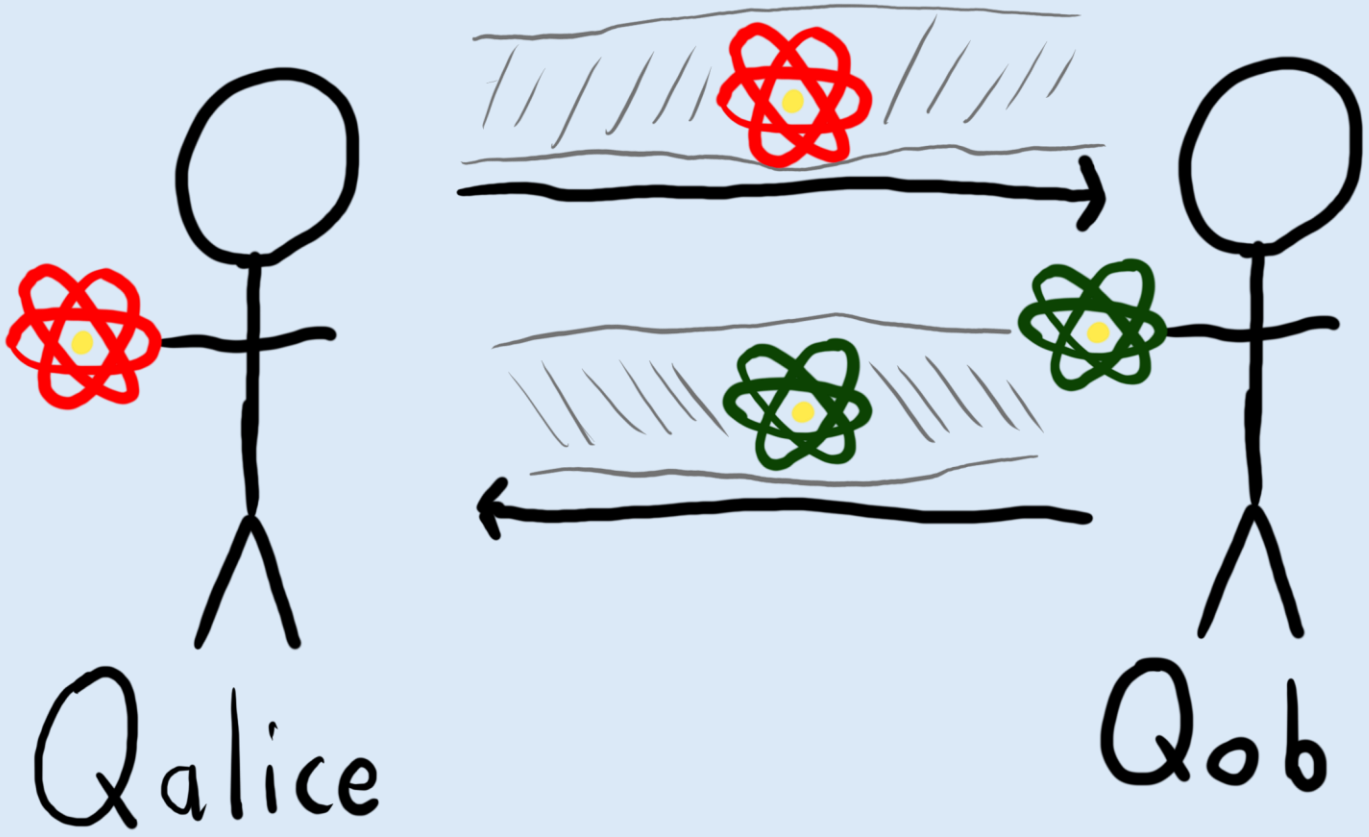
1. Simple
2. Minimal
3. Useful
4. **Flexible**



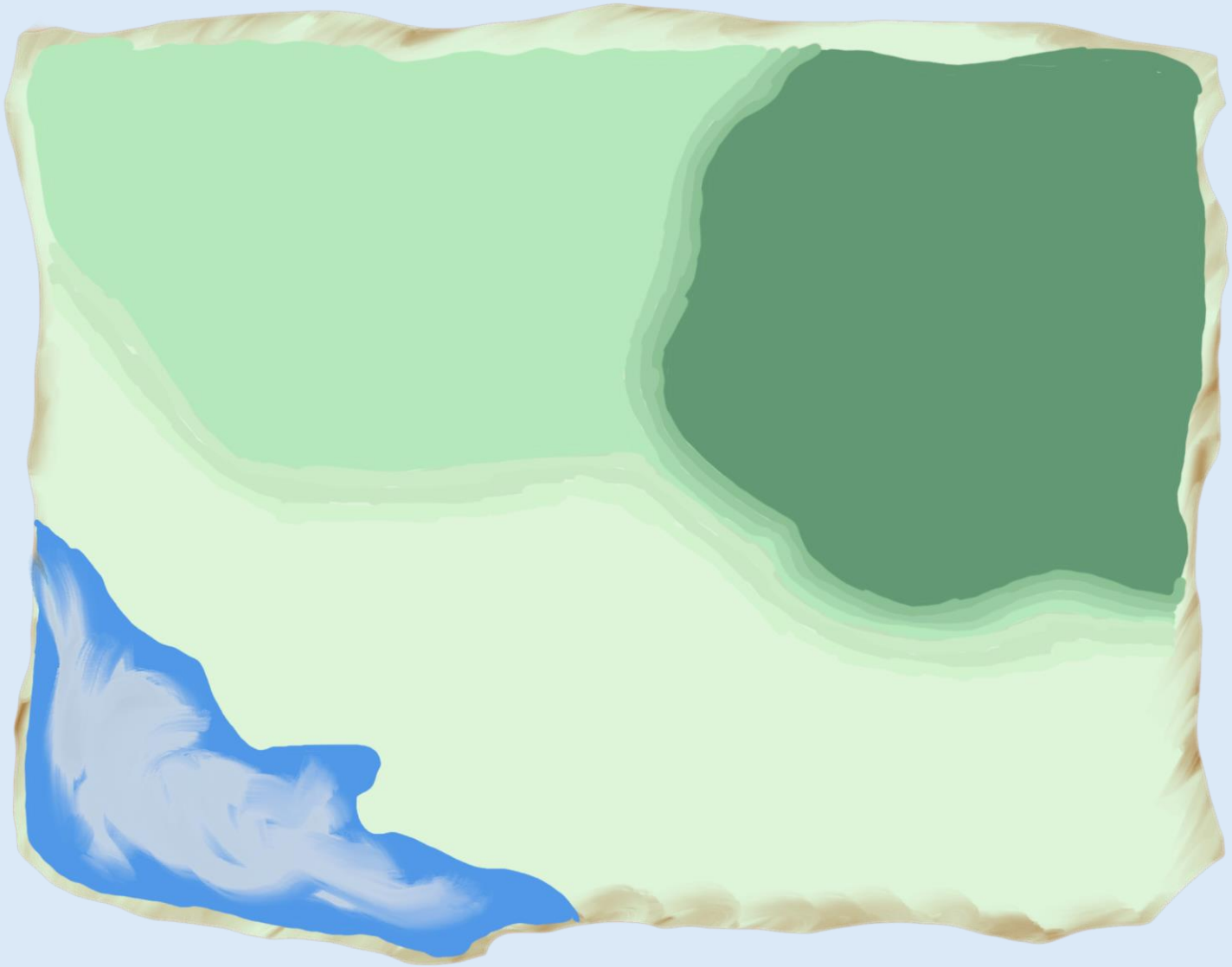
What about quantum communication?



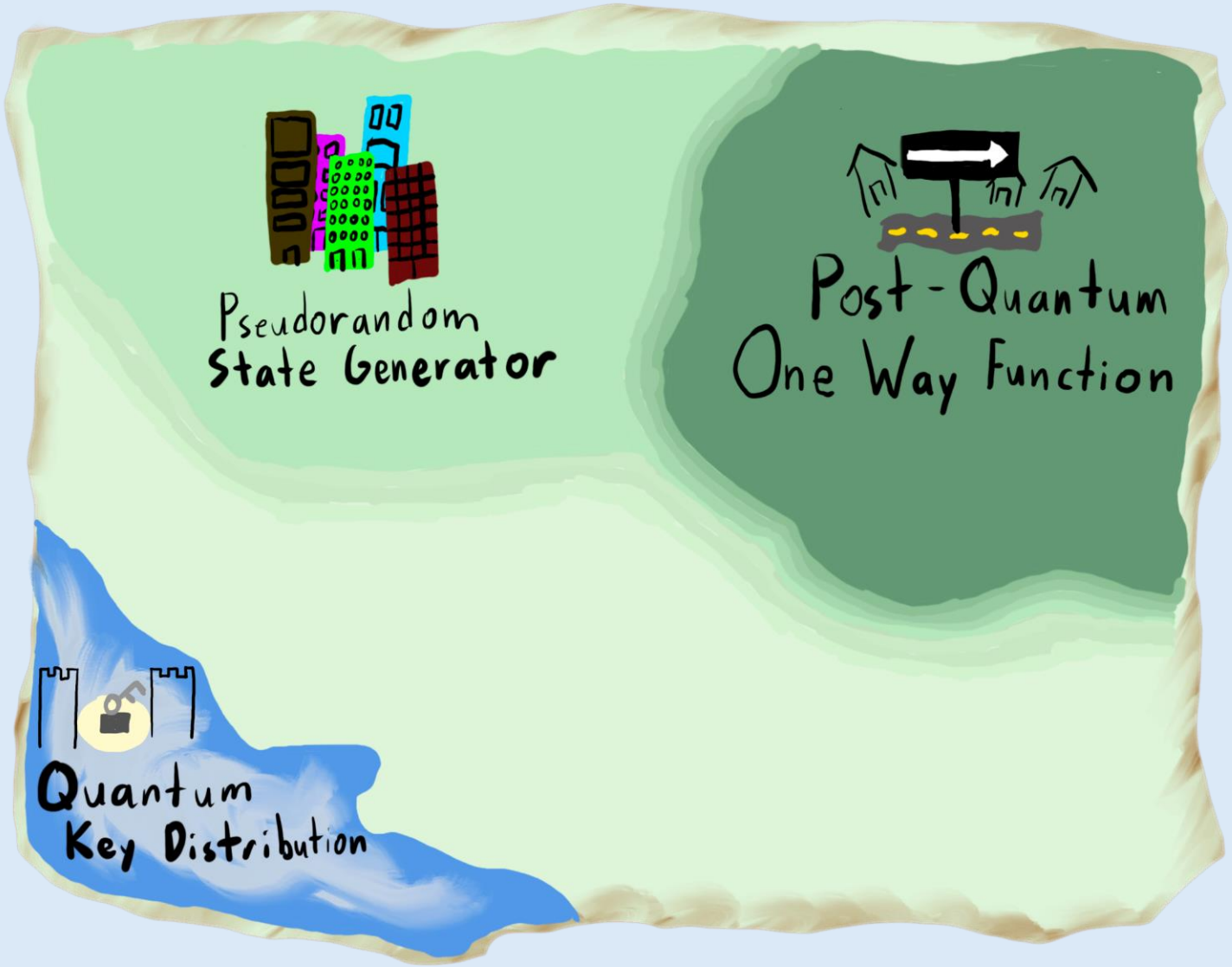
What about quantum communication?



Quantum Cryptography Topography

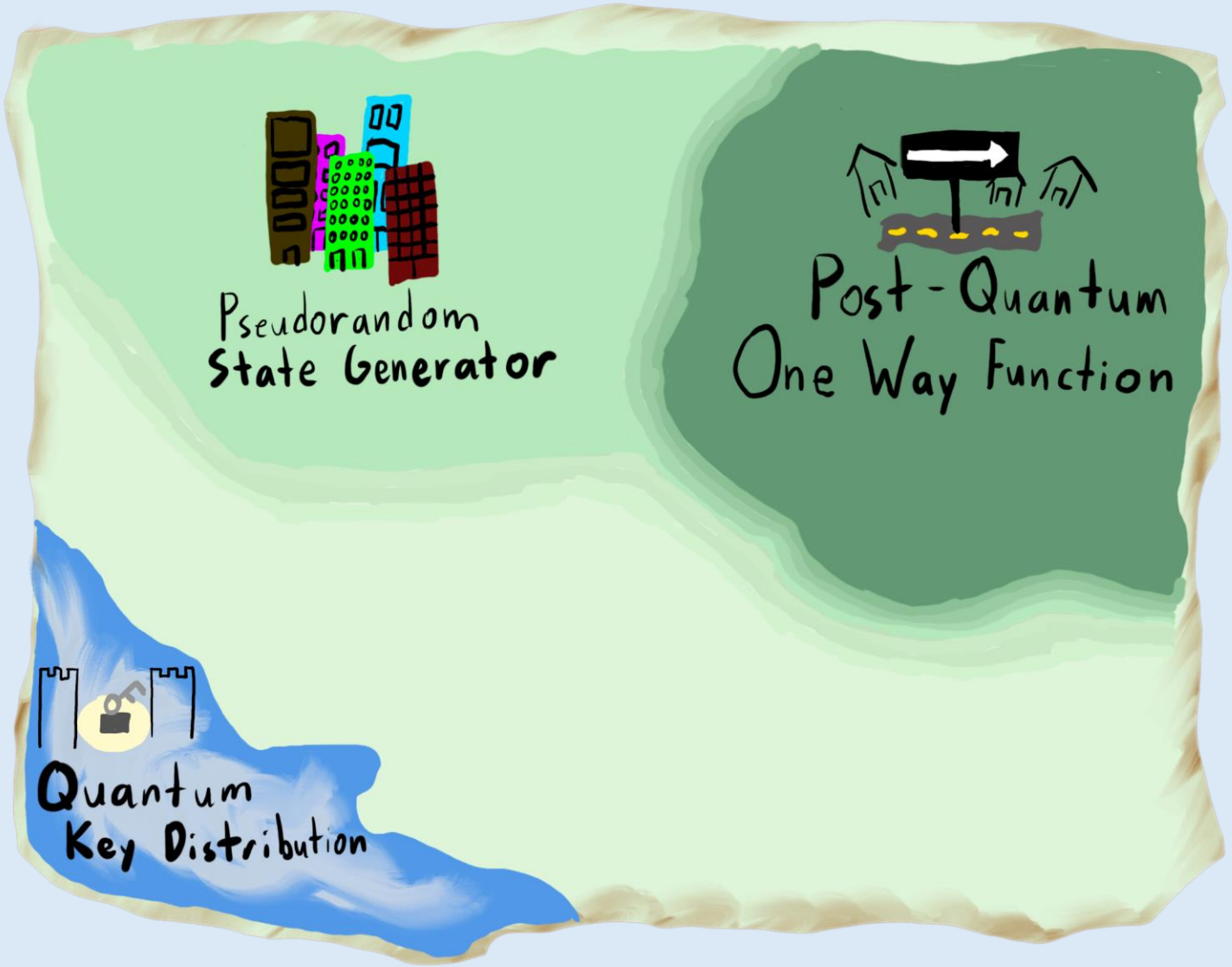


Quantum Cryptography Topography



Map different!

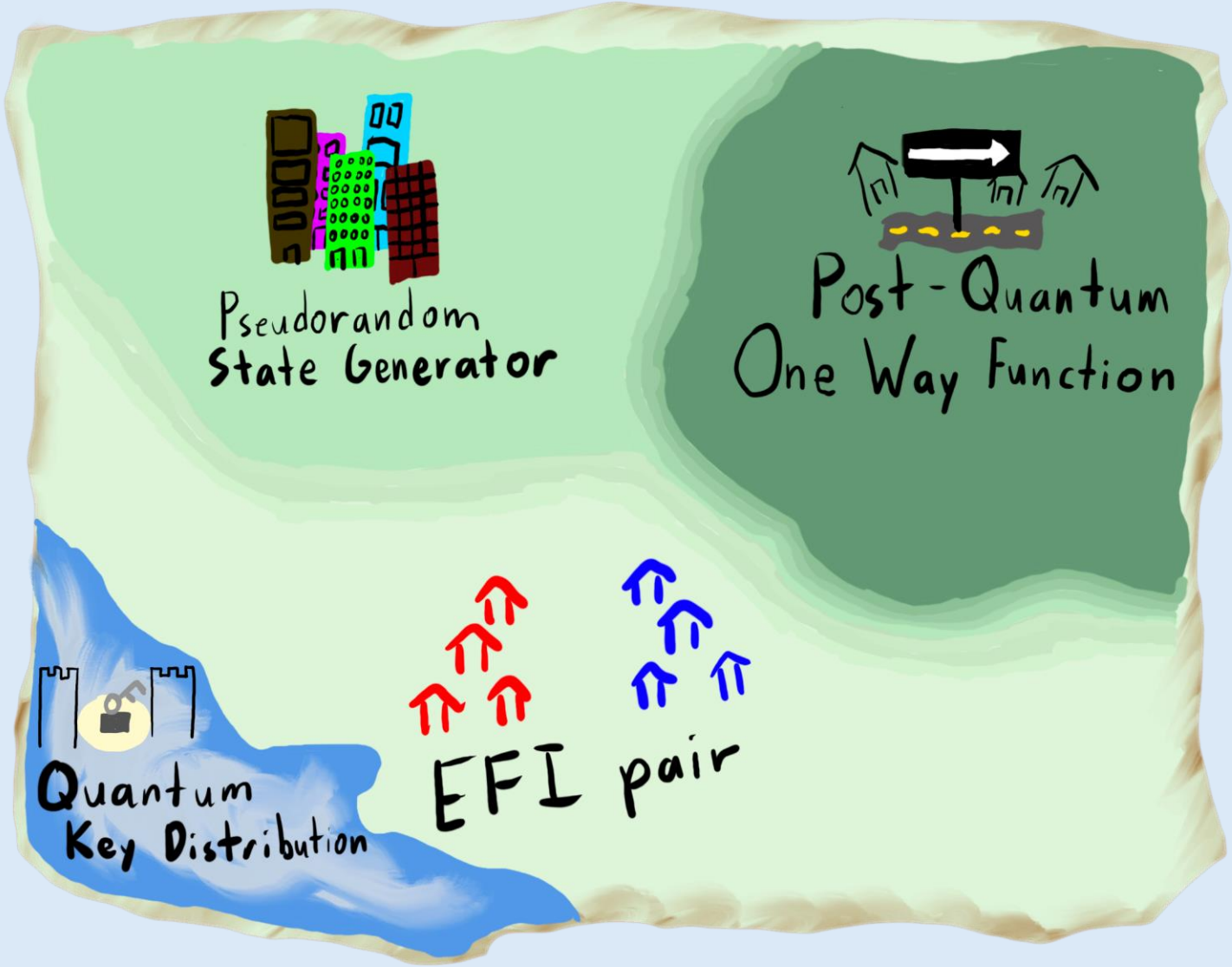
Quantum Cryptography Topography



Map different!

Is there a central primitive?

Quantum Cryptography Topography

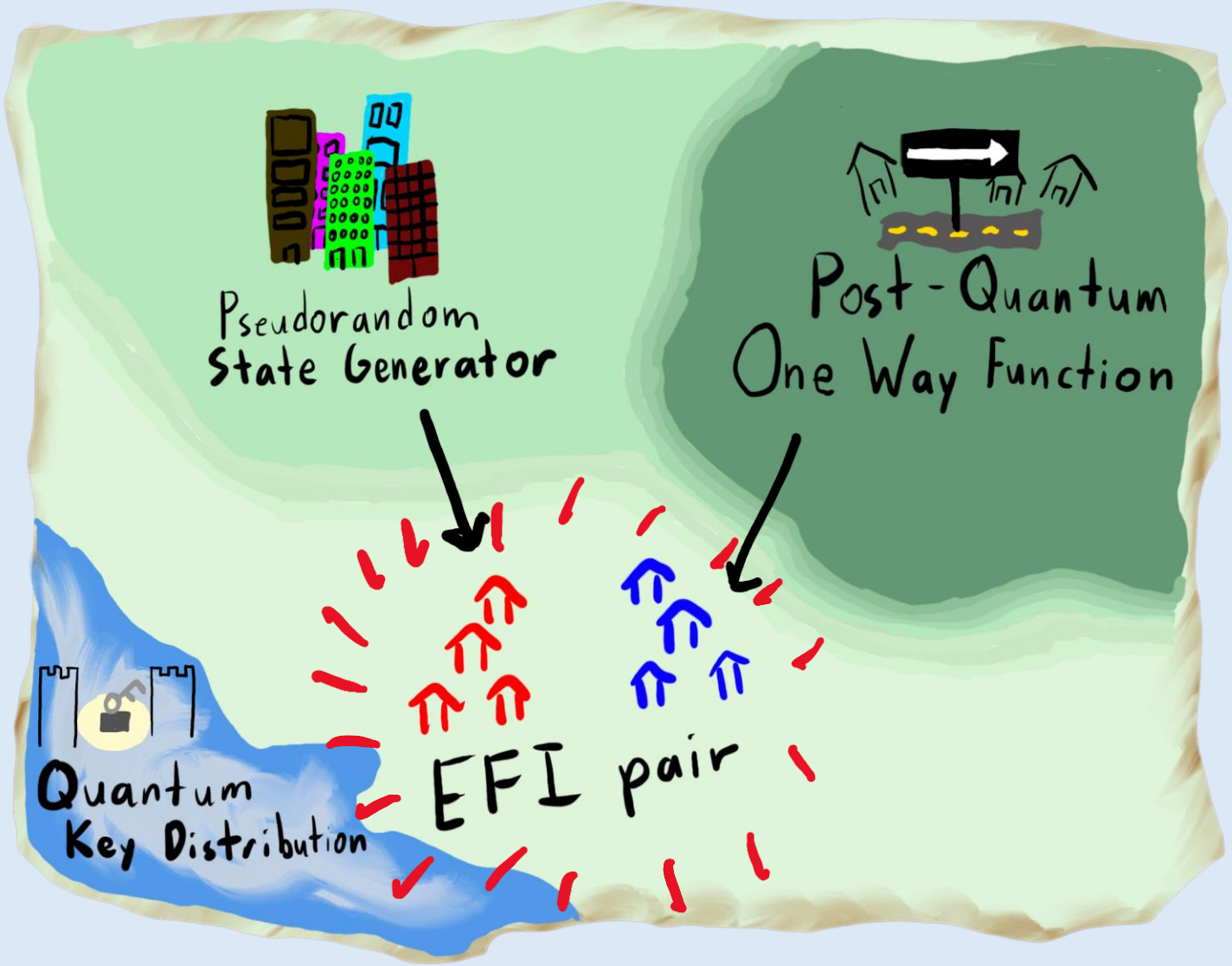


Map different!

Is there a central primitive?

Pretty good candidate: EFI pairs

Quantum Cryptography Topography

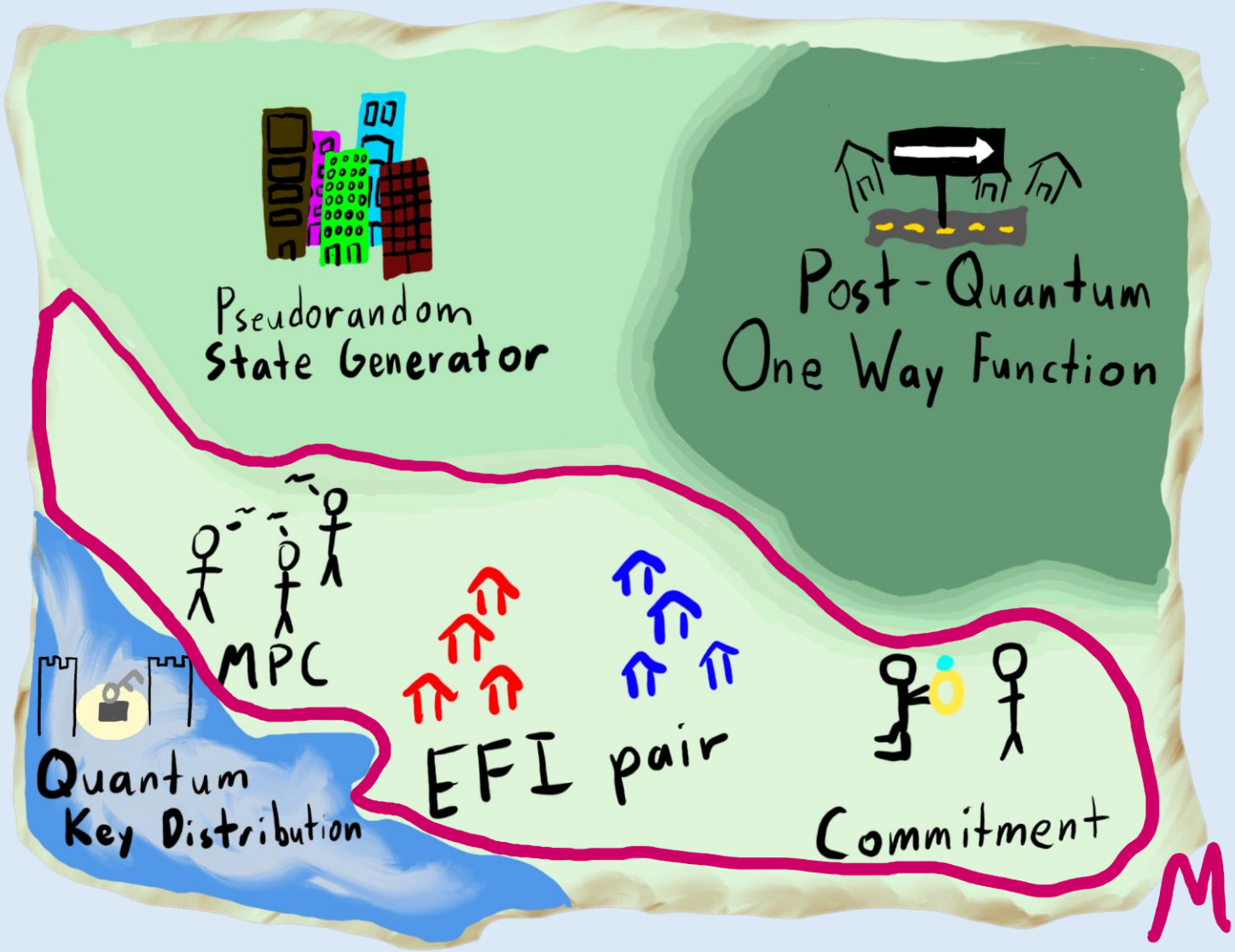


Map different!

Is there a central primitive?

Pretty good candidate: EFI pairs

Quantum Cryptography Topography



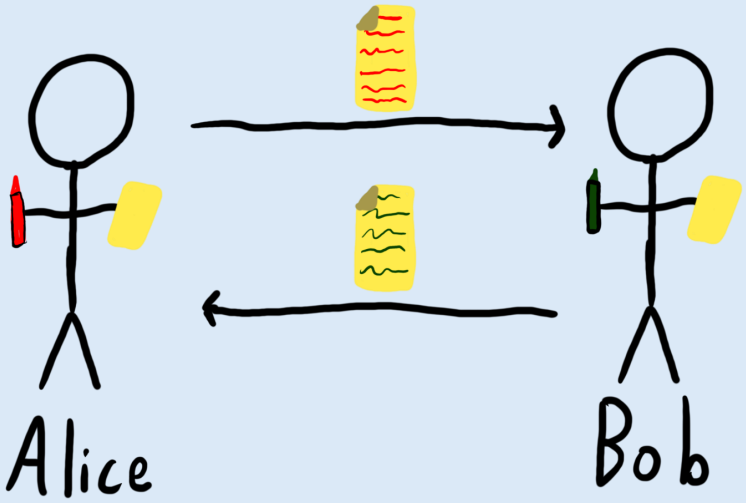
Map different!

Is there a central primitive?

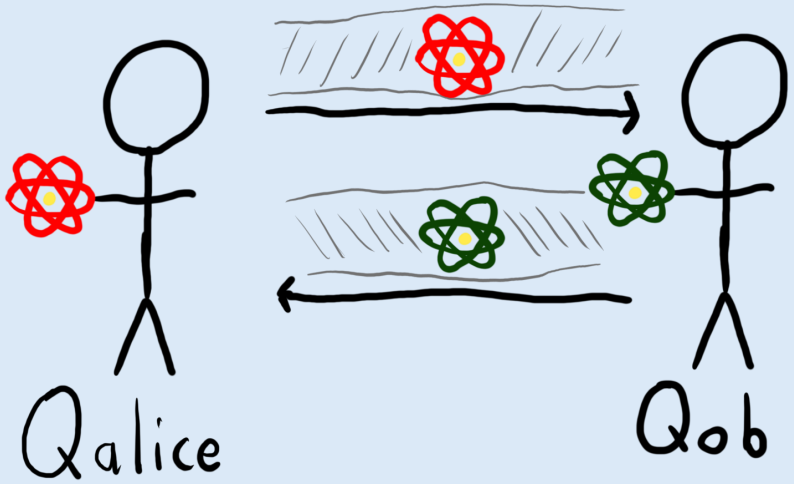
Pretty good candidate: EFI pairs

MicroQrypt

Our focus: The QCCC (QC) setting



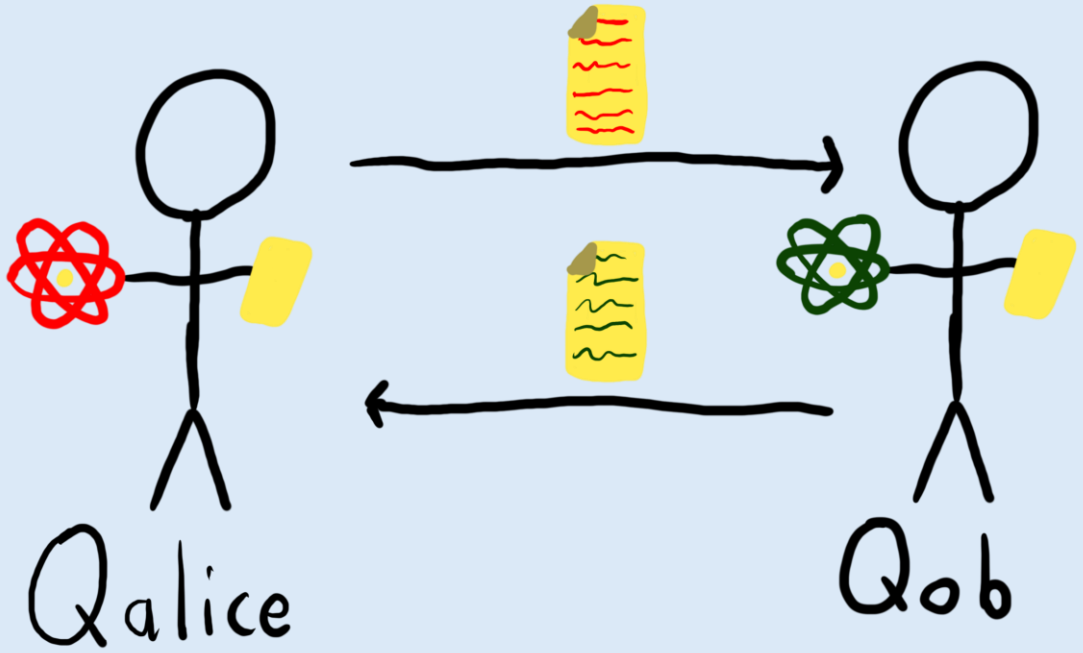
OWF



EFI

Our focus: The QCCC (QC) setting

"Quantum Computation with Classical Communication"



Our Goals

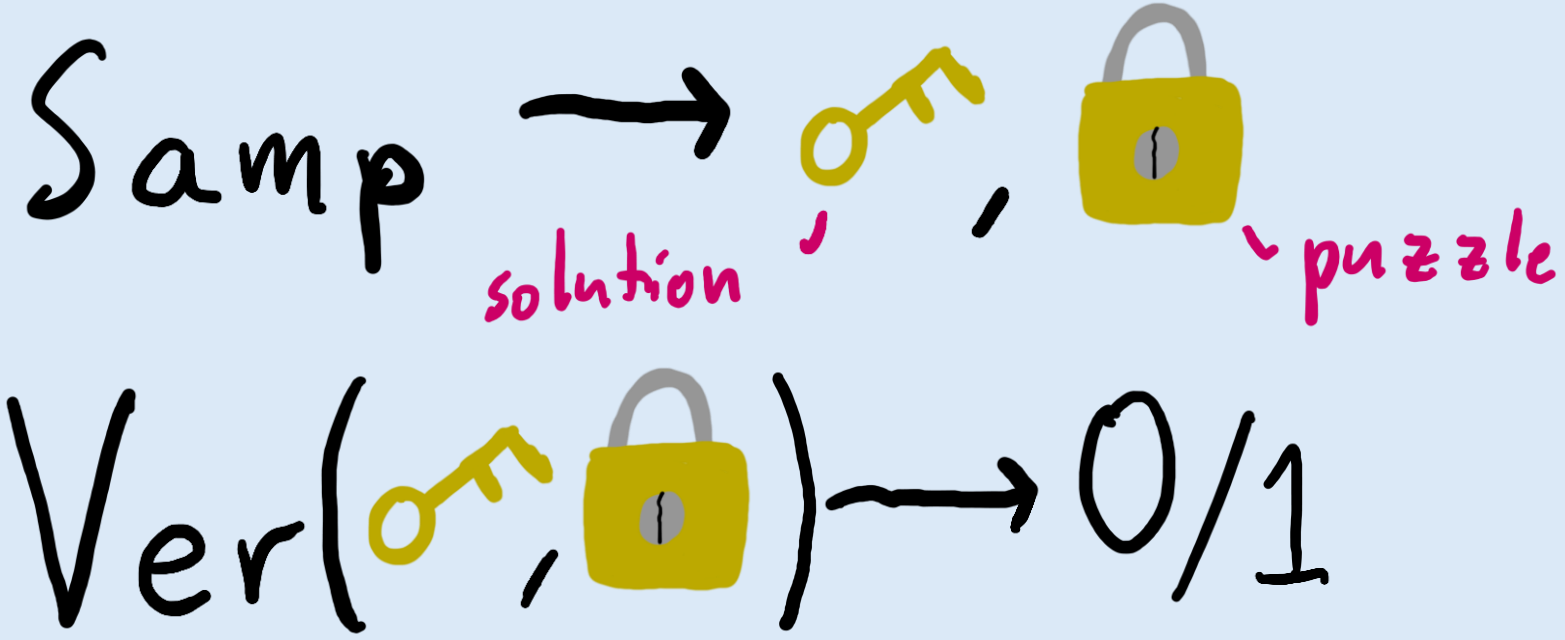
What does the “map” of QC cryptography look like?

Is there a central primitive in the QC setting?

Prior Work

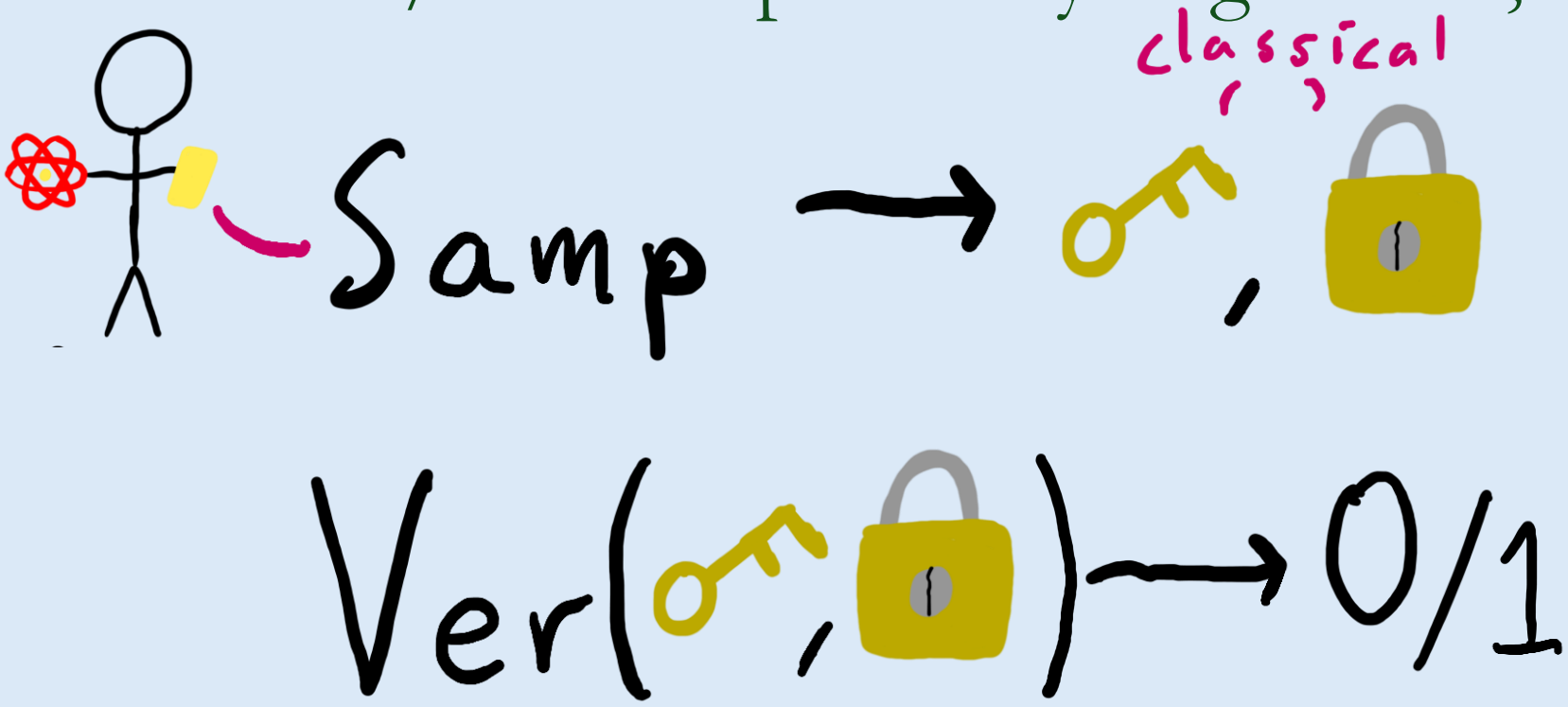
Candidate: One Way Puzzles [KT24]

Puzzle/solution pairs easy to generate, hard to solve.



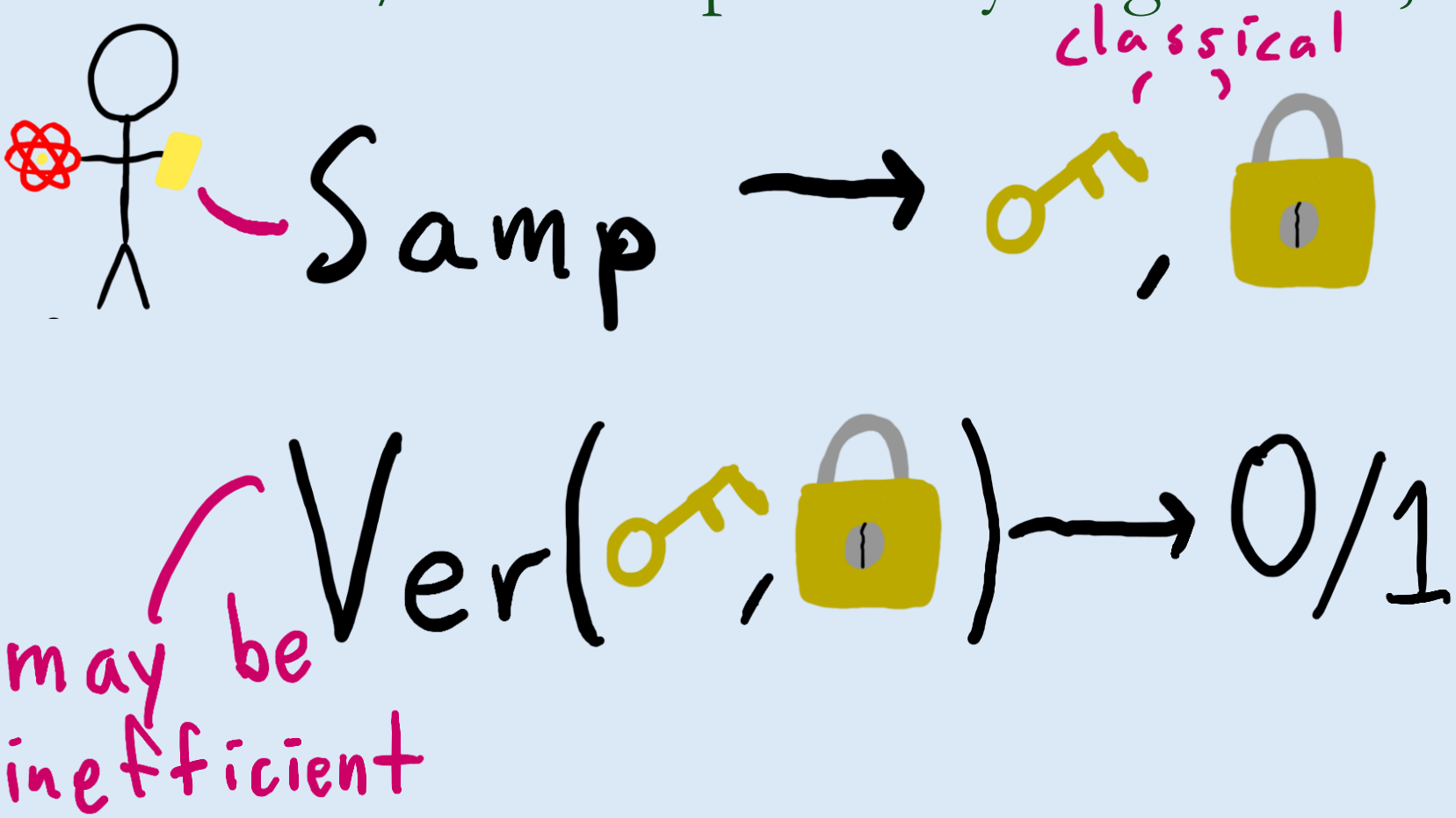
Candidate: One Way Puzzles [KT24]

Puzzle/solution pairs easy to generate, hard to solve.



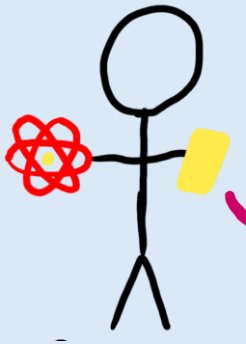
Candidate: One Way Puzzles [KT24]

Puzzle/solution pairs easy to generate, hard to solve.



Candidate: One Way Puzzles [KT24]

Puzzle/solution pairs easy to generate, hard to solve.



Samp $\longrightarrow$ 

classical

Ver() $\longrightarrow$ 0/1

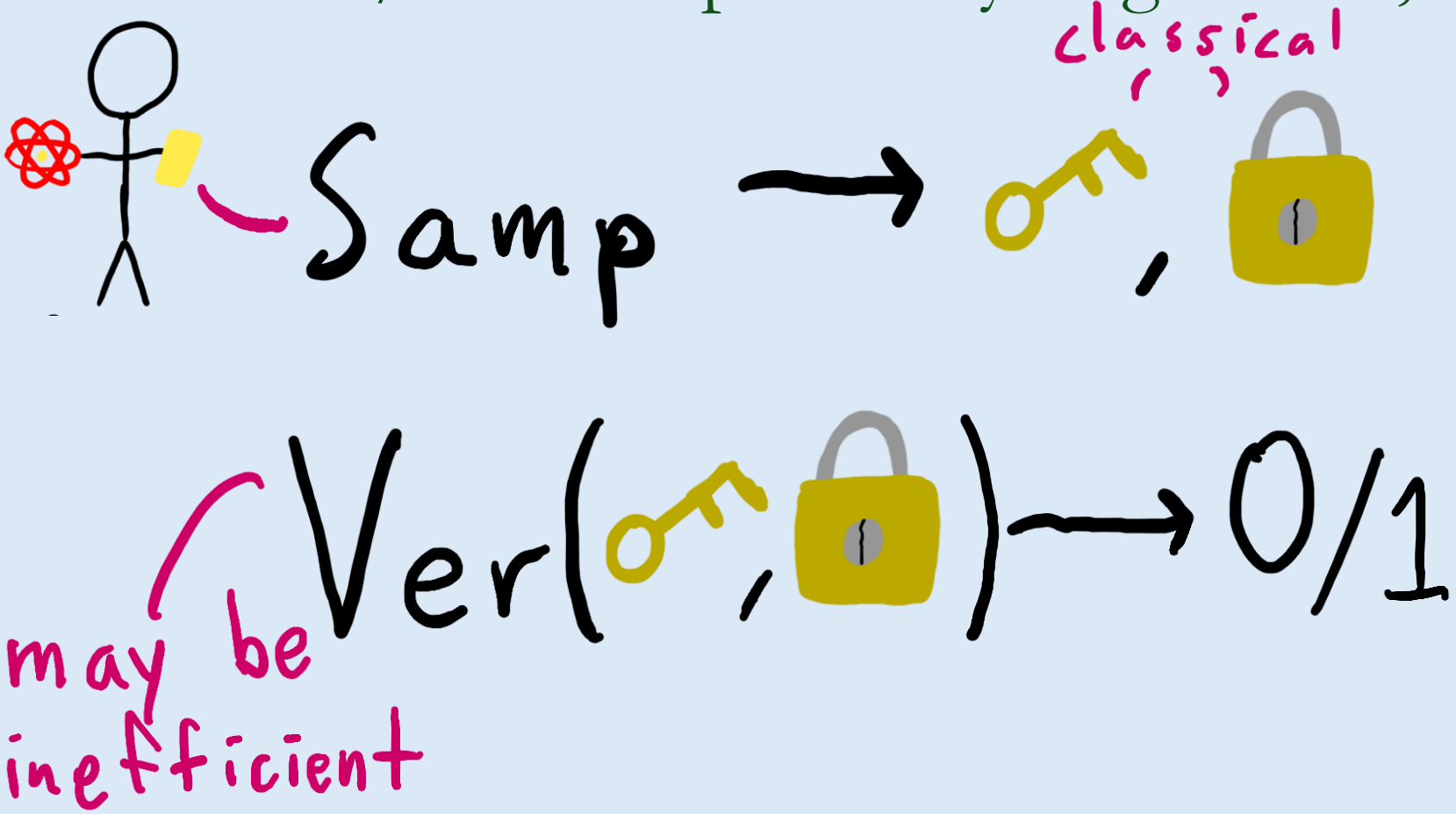
may be inefficient

Correctness

$\Pr[\mathrm{Ver}(\text{🔑}, \text{🔒}) \to 1] \geq 1 - \mathrm{negl}$

Candidate: One Way Puzzles [KT24]

Puzzle/solution pairs easy to generate, hard to solve.



Correctness

$\Pr[\mathrm{Ver}(\text{🔑}, \text{🔒}) \to 1] \geq 1 - \mathrm{negl}$

Security

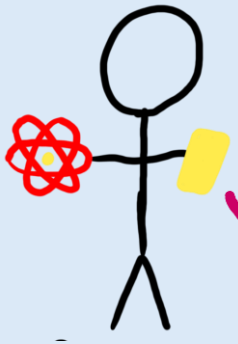
$\mathcal{A}(\text{🔒}) \to \text{🔑}$

$\Pr[\mathrm{Ver}(\text{🔑}, \text{🔒}) \to 1] \leq \mathrm{negl}$

Candidate: One Way Puzzles [KT24]

classically $\approx$ OWF!

Puzzle/solution pairs easy to generate, hard to solve.



Samp $\longrightarrow$ 

classical

Ver() $\longrightarrow$ 0/1

may be inefficient

Correctness

$\Pr[\mathrm{Ver}(\text{🔑}, \text{🔒}) \to 1] \geq 1 - \mathrm{negl}$

Security

$A(\text{🔒}) \to \text{🔑}$

$\Pr[\mathrm{Ver}(\text{🔑}, \text{🔒}) \to 1] \leq \mathrm{negl}$

Are one way puzzles a good central primitive?

Important properties of central primitives

1. **Simple**✓
2. Minimal
3. Useful
4. Flexible

Are one way puzzles a good central primitive?

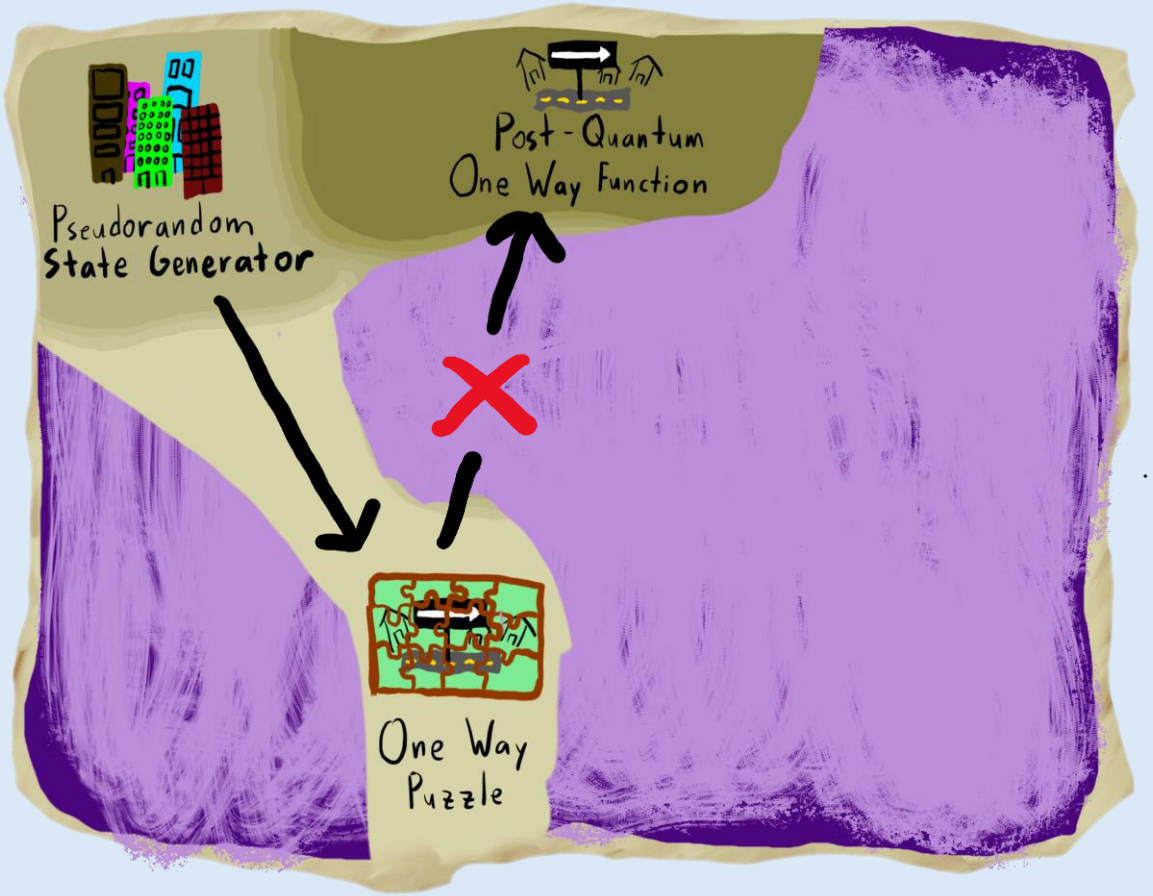
Important properties of central primitives

1. Simple ✓
2. **Minimal**
3. Useful
4. Flexible

Are one way puzzles a good central primitive?

Important properties of central primitives

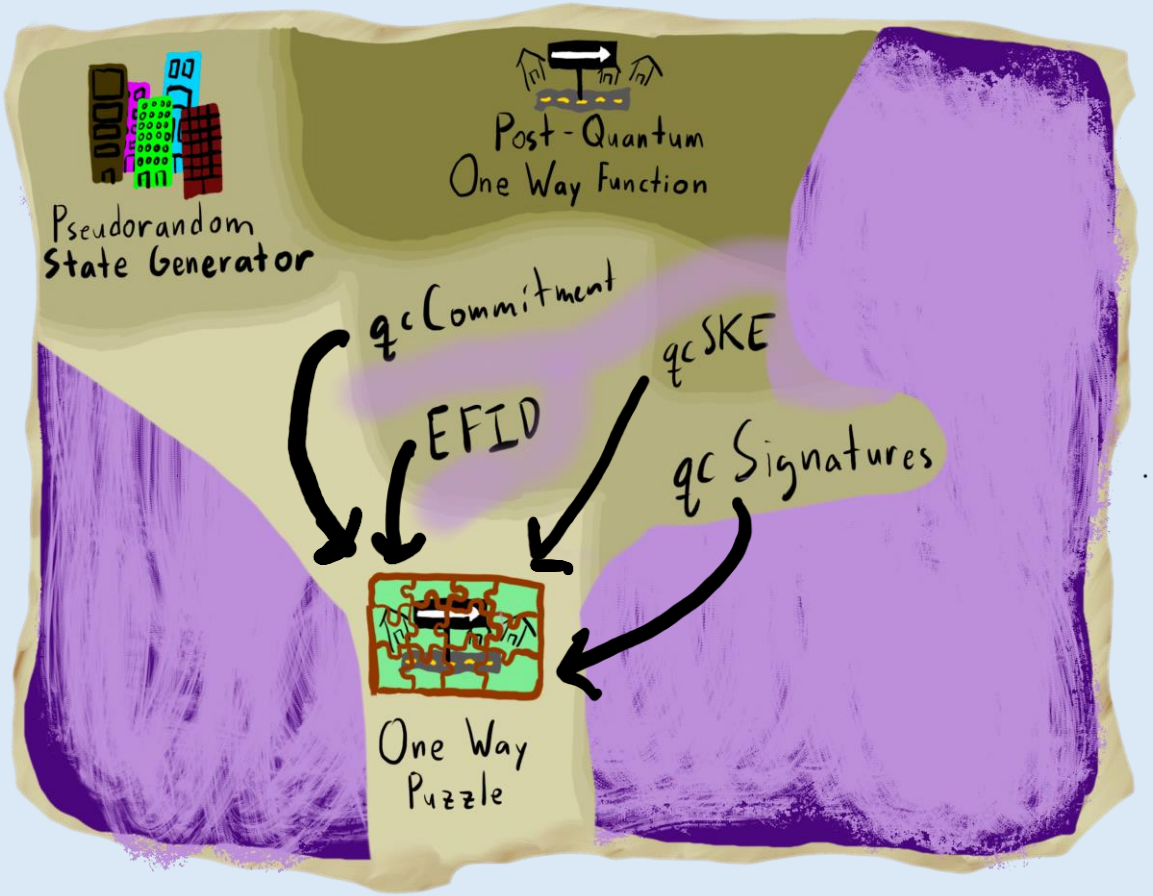
1. Simple ✓
2. **Minimal**
3. Useful
4. Flexible



Are one way puzzles a good central primitive?

Important properties of central primitives

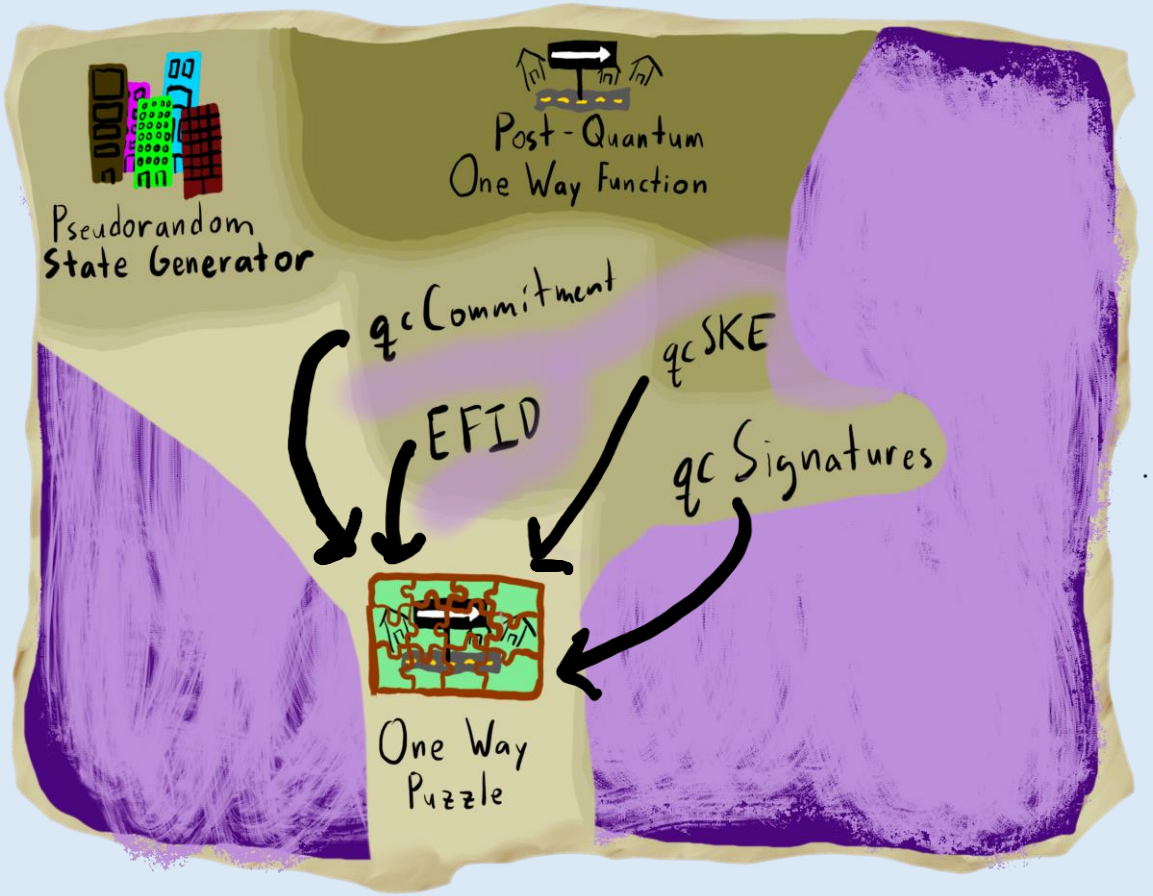
1. Simple ✓
2. **Minimal**
3. Useful
4. Flexible



Are one way puzzles a good central primitive?

Important properties of central primitives

1. Simple ✓
2. **Minimal** ✓
3. Useful
4. Flexible



Are one way puzzles a good central primitive?

Important properties of central primitives

1. Simple ✓
2. Minimal ✓
3. **Useful**
4. Flexible

Are one way puzzles a good central primitive?

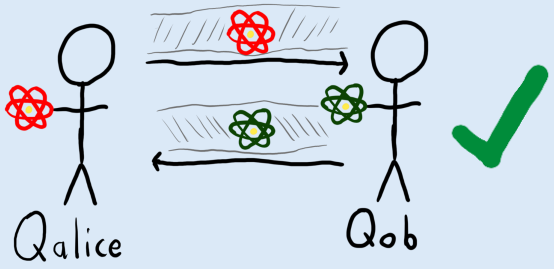
Important properties of central primitives

1. Simple ✓
2. Minimal ✓
3. **Useful**
4. Flexible

Are one way puzzles a good central primitive?

Important properties of central primitives

1. Simple ✓
2. Minimal ✓
3. **Useful**
4. Flexible

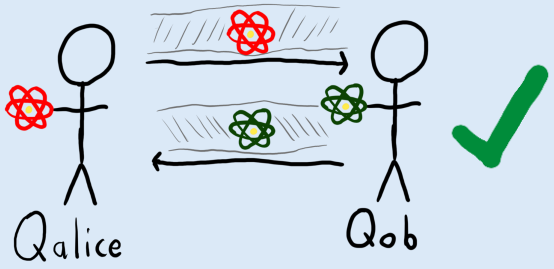


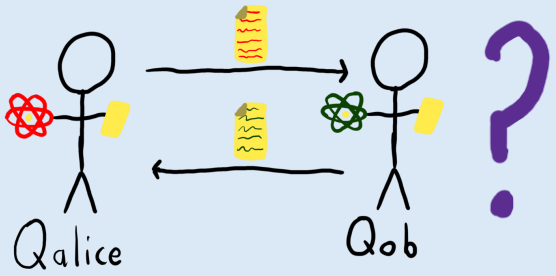
✓

Are one way puzzles a good central primitive?

Important properties of central primitives

1. Simple ✓
2. Minimal ✓
3. Useful
4. Flexible ?





Our Questions

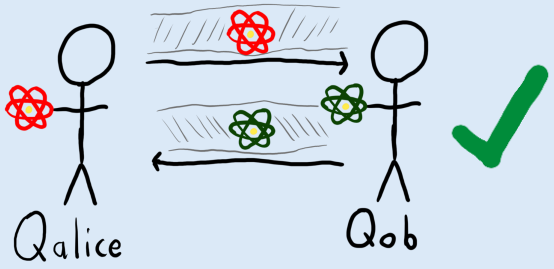
1. Are there any QC primitives implied by one way puzzles?
2. Are one way puzzles well-behaved?

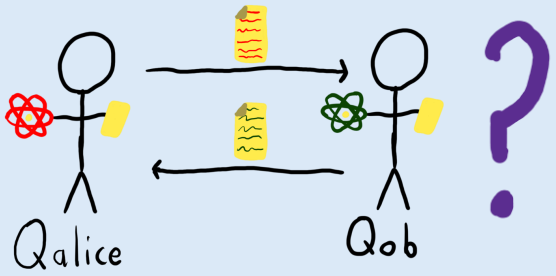
Our Results

Are one way puzzles a good central primitive?

Important properties of central primitives

1. Simple ✓
2. Minimal ✓
3. Useful
4. Flexible ?

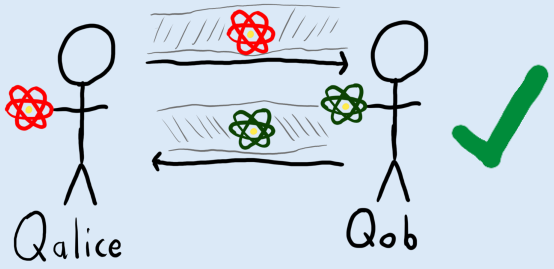




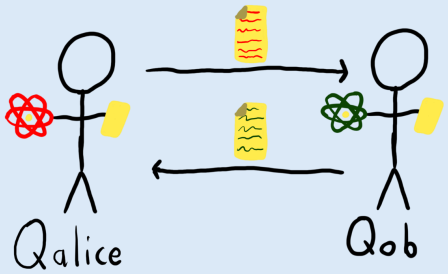
Are one way puzzles a good central primitive?

Important properties of central primitives

1. Simple ✓
2. Minimal ✓
3. Useful
4. Flexible ?



✓

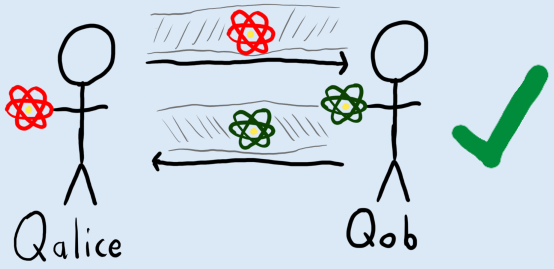


sorta

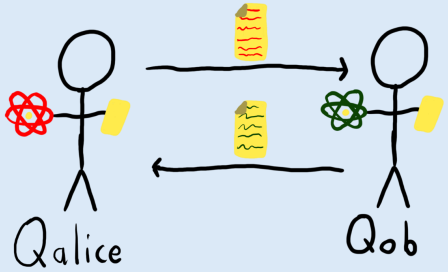
Are one way puzzles a good central primitive?

Important properties of central primitives

1. Simple ✓
2. Minimal ✓
3. Useful
4. Flexible ✓



✓



sorta

One Way Puzzles are Minimal [KT24]

Signature → One Way Puzzle

One Way Puzzles are Minimal [KT24]

Signature $\longrightarrow$ One Way Puzzle

$\mathsf{Gen} \rightarrow sk, vk$

$\mathsf{Sign}(sk, m) \rightarrow \sigma$

$\mathsf{VerSig}(vk, m, \sigma) \rightarrow 0/1$

One Way Puzzles are Minimal [KT24]

Signature → One Way Puzzle

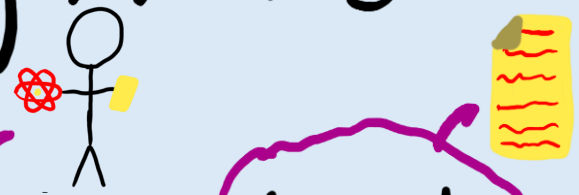
$\mathsf{Gen} \to sk, vk$

$\mathsf{Sign}(sk, m) \to \sigma$

$\mathsf{VerSig}(vk, m, \sigma) \to 0/1$

One Way Puzzles are Minimal [KT24]

Signature → One Way Puzzle



$\mathsf{Gen} \to sk, vk$

$\mathsf{Sign}(sk, m) \to \sigma$

$\mathsf{VerSig}(vk, m, \sigma) \to 0/1$

One Way Puzzles are Minimal [KT24]

Signature → One Way Puzzle

Gen → sk, vk

Sign(sk, m) → σ

VerSig(vk, m, σ) → 0/1

Samp →  = σ,  = vk

Sign(sk, 0)

k

s

One Way Puzzles are Minimal [KT24]

Signature → One Way Puzzle

$\mathrm{Gen} \to sk, vk$

$\mathrm{Sign}(sk, m) \to \sigma$

$\mathrm{VerSig}(vk, m, \sigma) \to 0/1$

$\mathrm{Samp} \to$  $= \sigma$,  $= vk$

$\mathrm{Sign}(sk, 0)$

k

s

$\mathrm{Ver}(\sigma, vk) = \mathrm{VerSig}(vk, 0, \sigma)$

One Way Puzzles are Minimal [KT24]

Signature → One Way Puzzle

Gen → sk, vk

Sign(sk, m) → σ

VerSig(vk, m, σ) → 0/1

Samp →  = σ,  = vk

Sign(sk, 0)

k

s

Ver(σ, vk) = VerSig(vk, 0, σ)

can be inefficient

Are One Way Puzzles Useful?

Signature → One Way Puzzle

Gen → sk, vk

Sign(sk, m) → σ

VerSig(vk, m, σ) → 0/1

Samp →  = σ,  = vk

k s

Sign(sk, 0)

Ver(σ, vk) = VerSig(vk, 0, σ)

efficient!

Are One Way Puzzles Useful?

Signature $\xrightarrow{\text{EV}}$ One Way Puzzle

$\mathrm{Gen} \to sk, vk$

$\mathrm{Sign}(sk, m) \to \sigma$

$\mathrm{VerSig}(vk, m, \sigma) \to 0/1$

$\mathrm{Samp} \to$  $= \sigma$,  $= vk$

$\mathrm{Sign}(sk, 0)$

k

s

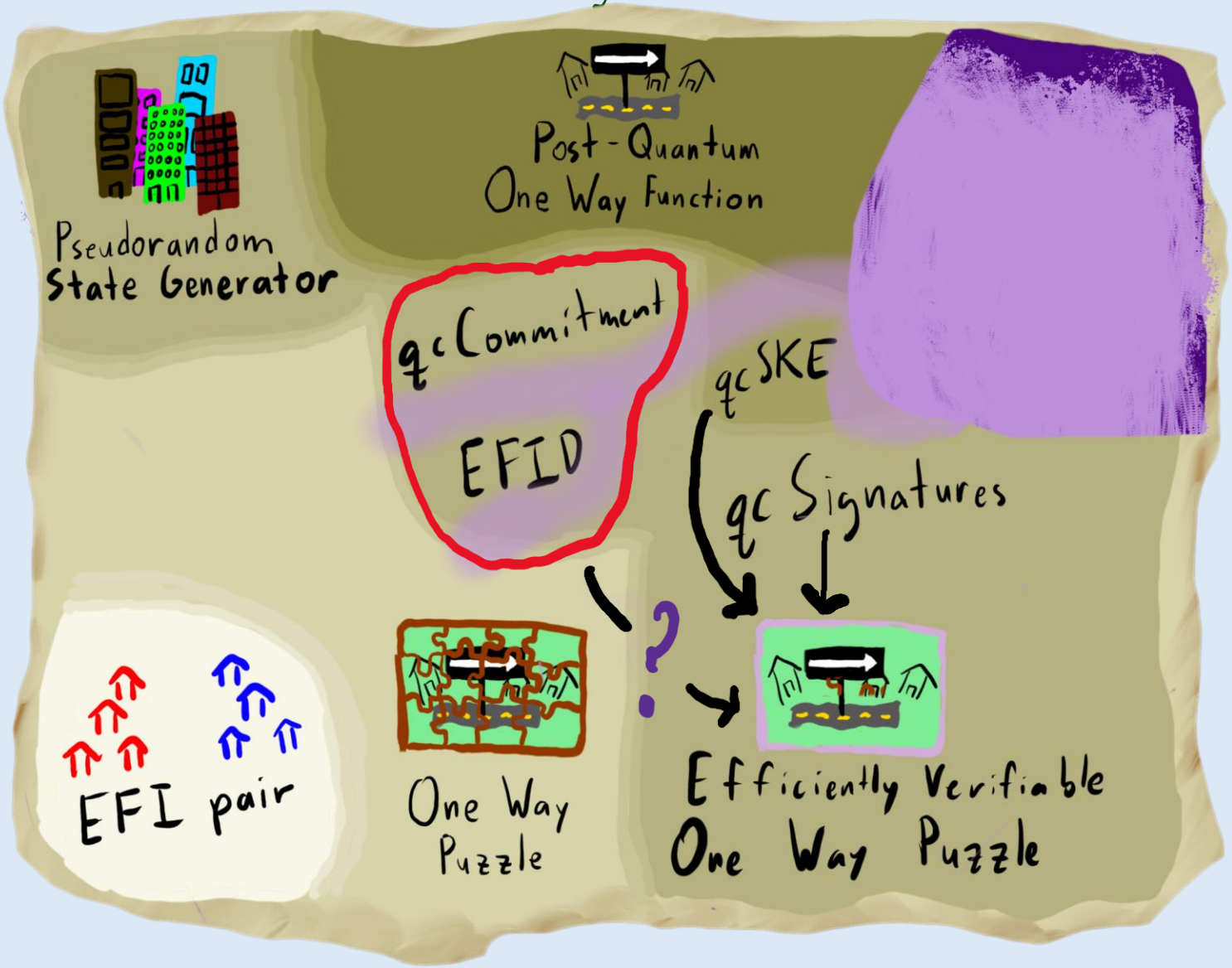
$\mathrm{Ver}(\sigma, vk) = \mathrm{VerSig}(vk, 0, \sigma)$

efficient!

Are One Way Puzzles Useful?

Are One Way Puzzles Useful?

Are One Way Puzzles Useful?

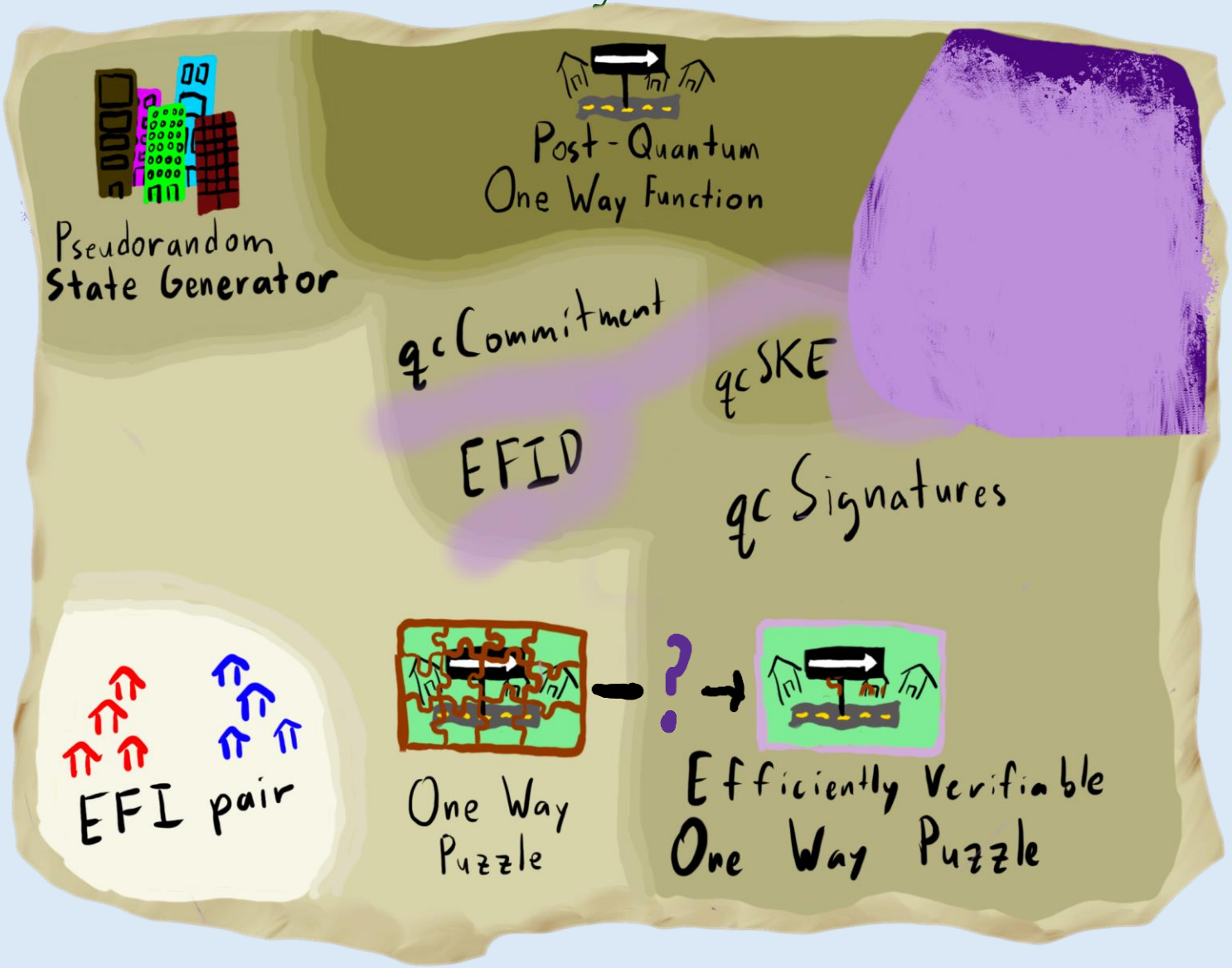


Notable exception: commitments

Are One Way Puzzles Useful?

EV-OWPuzz are (= 1-time sigs)

Are One Way Puzzles Useful?



Necessary and sufficient condition for usefulness of OWPuzz

Are One Way Puzzles Useful?

- Can we build other QC primitives from OWPuzz?

NO

exception: maybe commitments

Are One Way Puzzles Useful?

- Can we build other QC primitives from OWPuzz?

Are One Way Puzzles Useful?

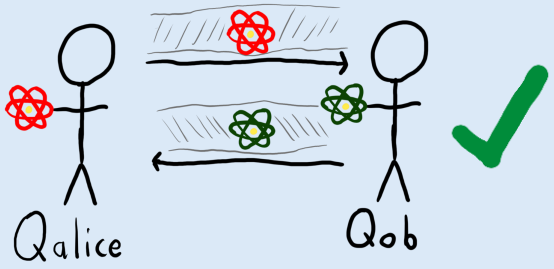
- Can we build other QC primitives from OWPuzz?

- OWPuzz can exist when BQP = QCMA [Kreschmer21]
- EV-OWPuzz broken in QCMA [INNRY22][ABOBS22]

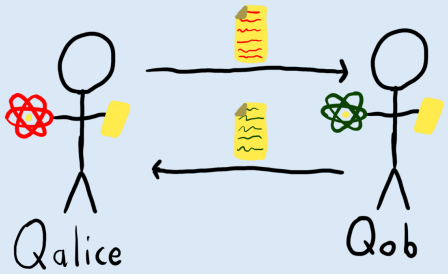
Are one way puzzles a good central primitive?

Important properties of central primitives

1. Simple ✓
2. Minimal ✓
3. **Useful**
4. Flexible ?



✓

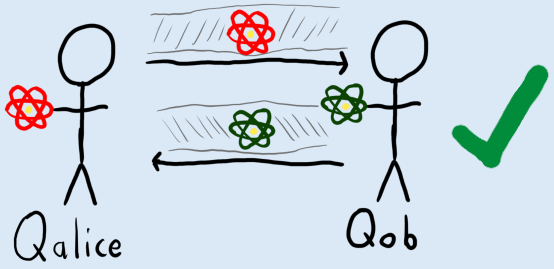


sorta

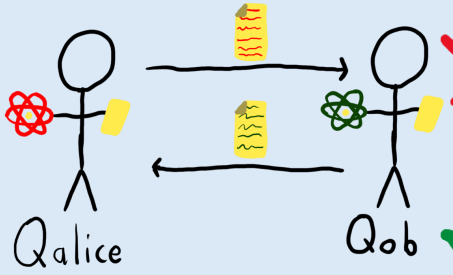
Are one way puzzles a good central primitive?

Important properties of central primitives

1. Simple ✓
2. Minimal ✓
3. **Useful**
4. Flexible ?



✓



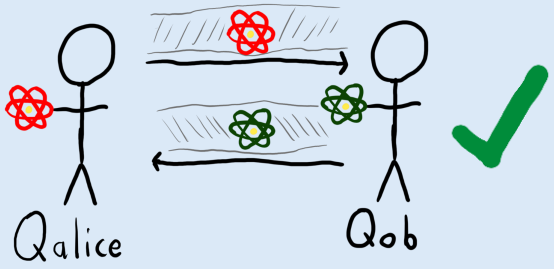
✗ OWPuzz

✓ EV-OWPuzz

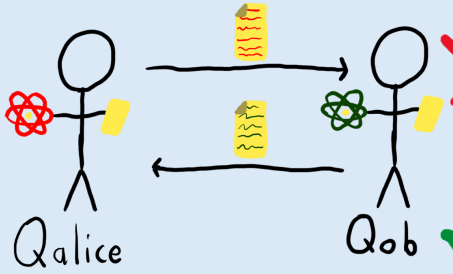
Are one way puzzles a good central primitive?

Important properties of central primitives

1. Simple ✓
2. Minimal ✓
3. Useful
4. **Flexible?**



✓



✗ OWPuzz

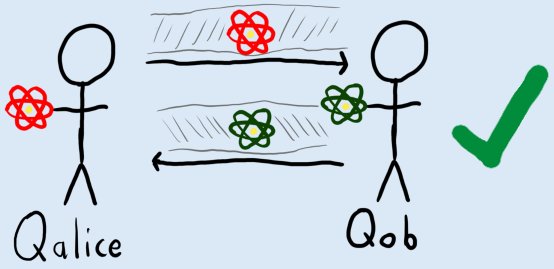
✓ EV-OWPuzz

$$(\mathsf{Samp}, \mathsf{Ver}) + (\mathsf{Samp}', \mathsf{Ver}') \to (\widetilde{\mathsf{Samp}}, \widetilde{\mathsf{Ver}})$$

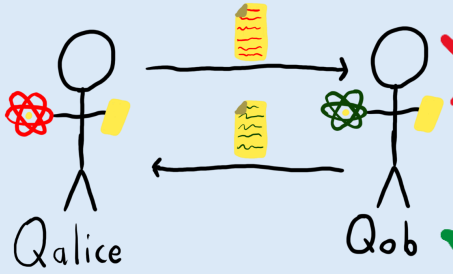
Are one way puzzles a good central primitive?

Important properties of central primitives

1. Simple ✓
2. Minimal ✓
3. Useful
4. **Flexible?**



✓



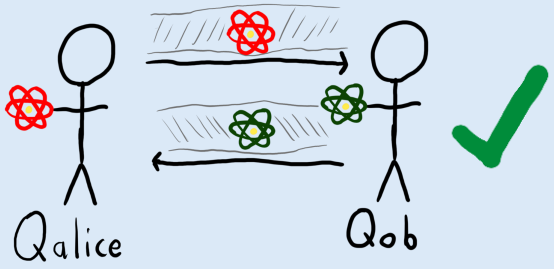
✗ OWPuzz

✓ EV-OWPuzz

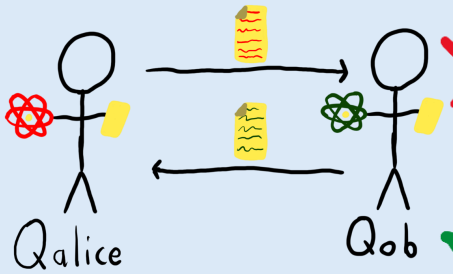
Are one way puzzles a good central primitive?

Important properties of central primitives

1. Simple ✓
2. Minimal ✓
3. Useful
4. **Flexible?**



✓

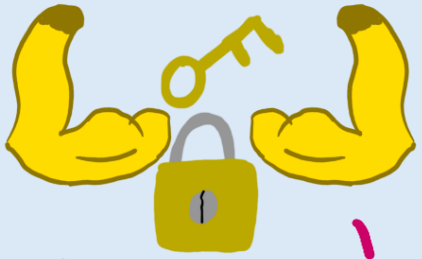


✗ OWPuzz

✓ EV-OWPuzz

"Dist OWPuzz"

"Weak OWPuzz"

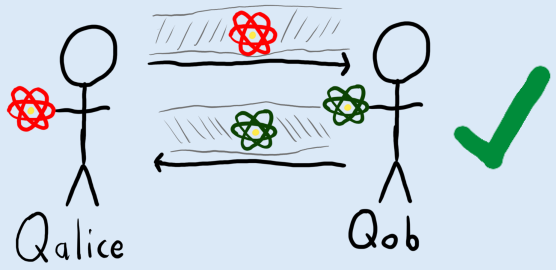


"Strong OWPuzz"

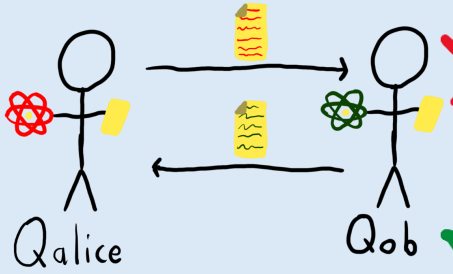
Are one way puzzles a good central primitive?

Important properties of central primitives

1. Simple ✓
2. Minimal ✓
3. Useful
4. **Flexible?**



✓



✗ OWPuzz

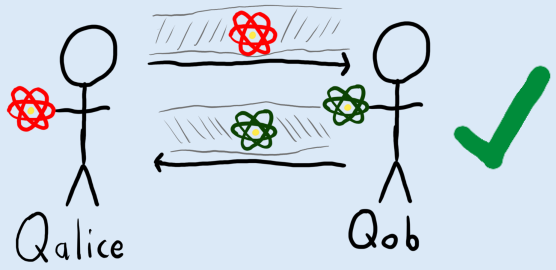
✓ EV-OWPuzz

"Dist OWPuzz" "Weak OWPuzz" "Strong OWPuzz"

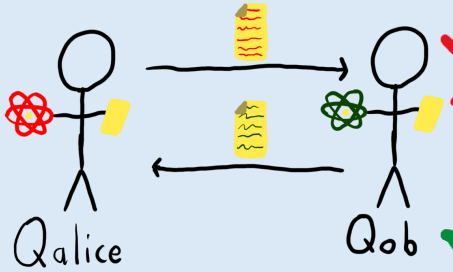
Are one way puzzles a good central primitive?

Important properties of central primitives

1. Simple ✓
2. Minimal ✓
3. Useful
4. **Flexible** ✓



✓



✗ OWPuzz

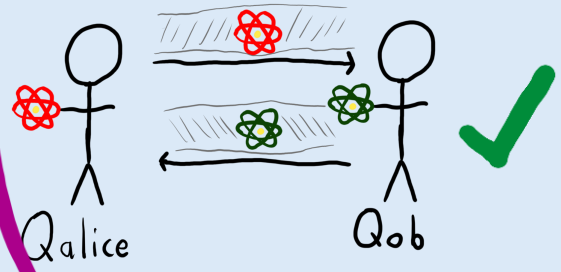
✓ EV-OWPuzz

"Dist OWPuzz" "Weak OWPuzz" "Strong OWPuzz"

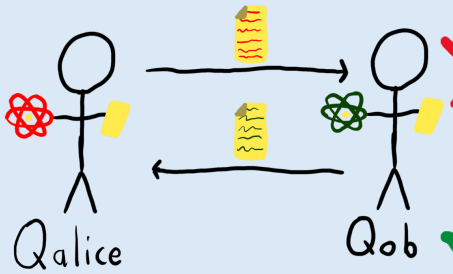
Are one way puzzles a good central primitive?

Important properties of central primitives

1. Simple ✓
2. Minimal ✓
3. Useful
4. **Flexible** ✓



✓



✗ OWPuzz

✓ EV-OWPuzz

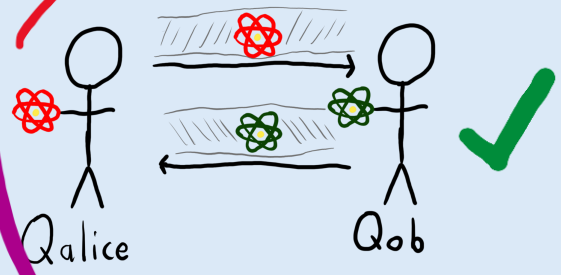
For both OWPuzz & EV-OWPuzz

Are one way puzzles a good central primitive?

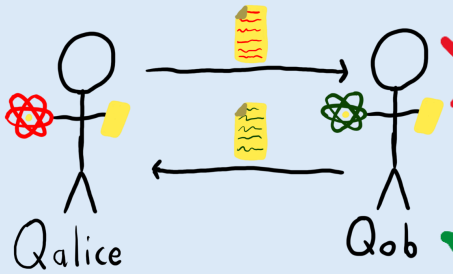
Important properties of central primitives

1. Simple ✓
2. Minimal ✓
3. Useful
4. **Flexible** ✓

exception: commitments



✓



✗ OWPuzz

✓ EV-OWPuzz

For both OWPuzz & EV-OWPuzz

QC Topography

QC Topography

One Way Puzzle Amplification

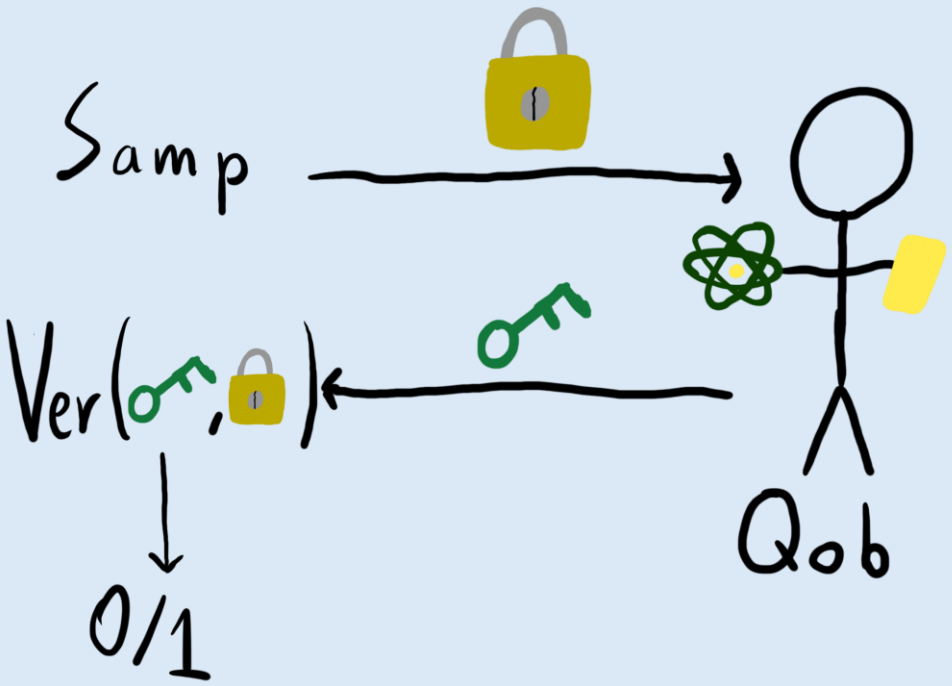
Why is this hard?

We *can* amplify soundness for efficient 3 round quantum interactive protocols via parallel repetition [BQSY23].

Why is this hard?

We *can* amplify soundness for efficient 3 round quantum interactive protocols via parallel repetition [BQSY23].

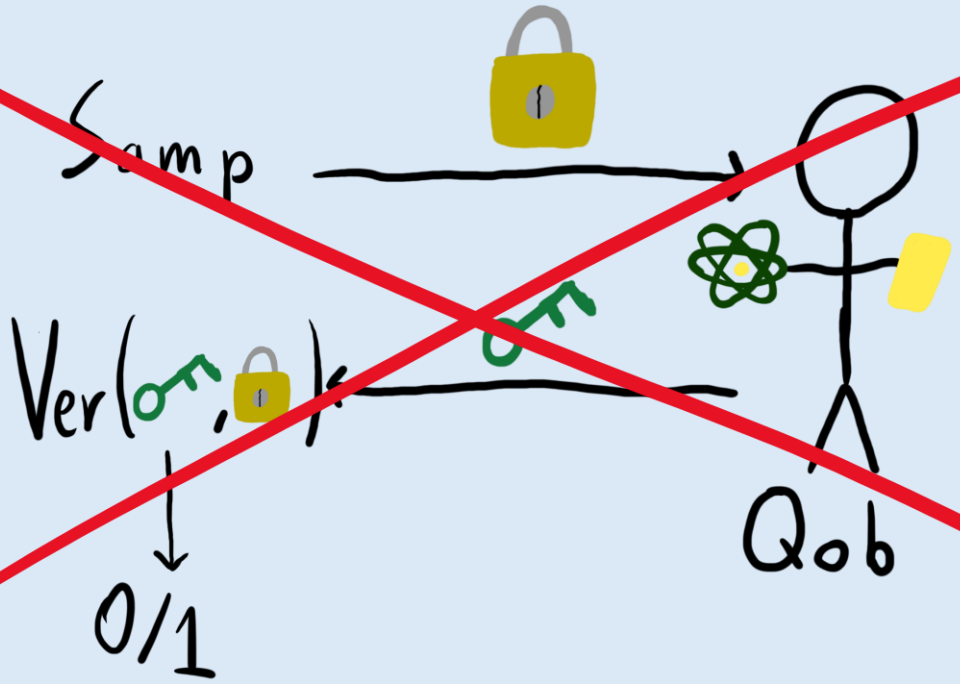
Security Game



Why is this hard?

We *can* amplify soundness for efficient 3 round quantum interactive protocols via parallel repetition [BQSY23].

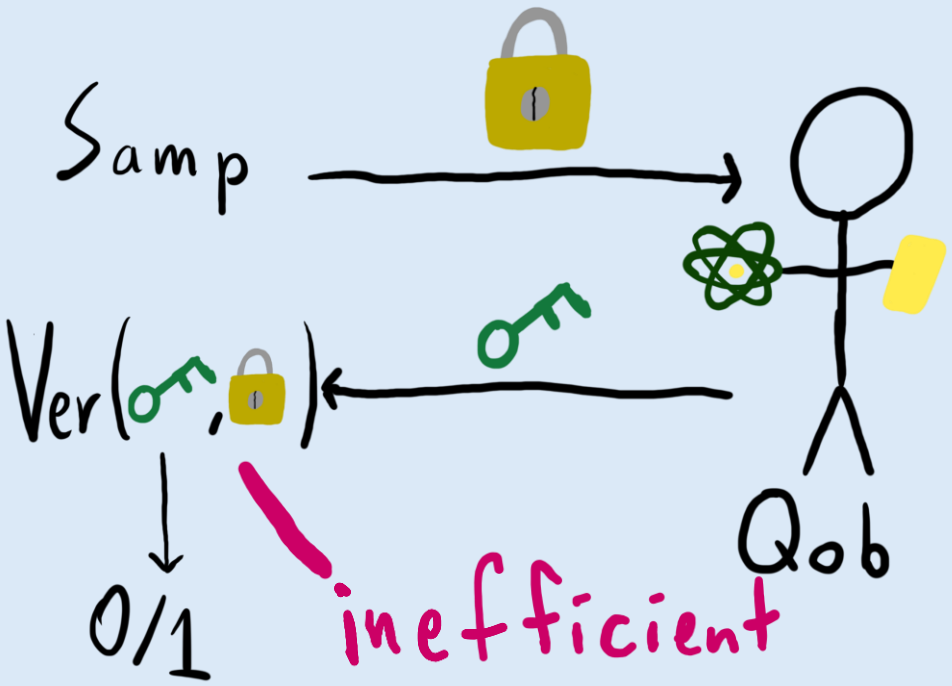
Security Game



Why is this hard?

We *can* amplify soundness for efficient 3 round quantum interactive protocols via parallel repetition [BQSY23].

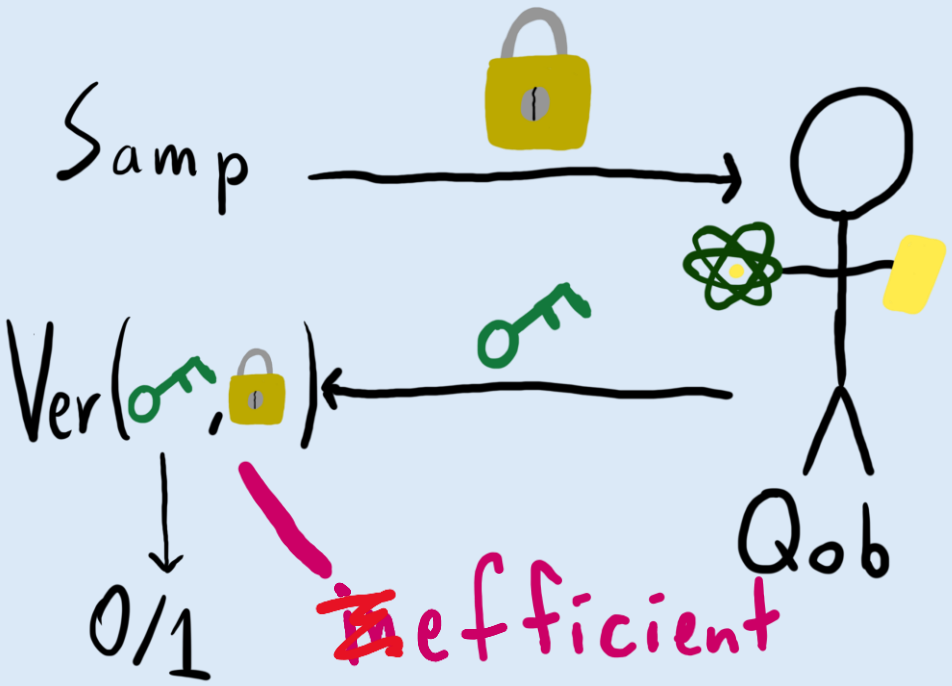
Security Game



Why is this hard?

We *can* amplify soundness for efficient 3 round quantum interactive protocols via parallel repetition [BQSY23].

Security Game



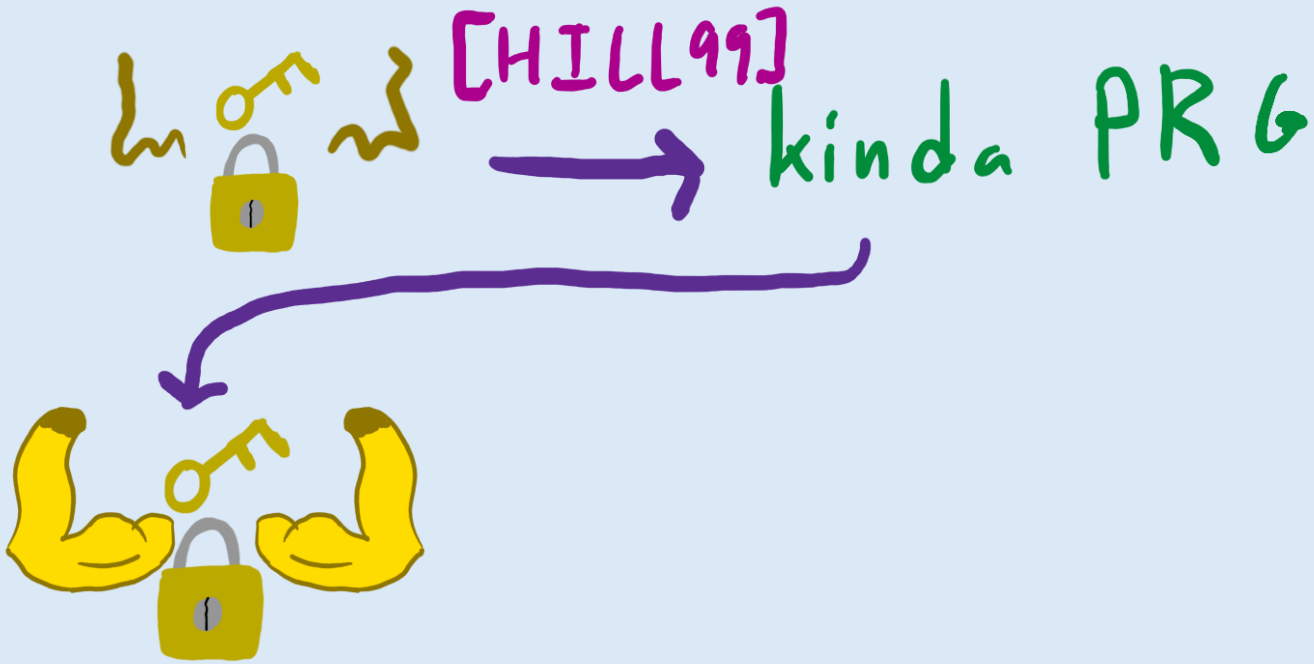
Works for EV-OWPuzz

Our approach

- [KT24] builds "kinda PRGs" (EFID) from OWPuzz using techniques of [HILL99]

Our approach

- [KT24] builds "kinda PRGs" (EFID) from OWPuzz using techniques of [HILL99]

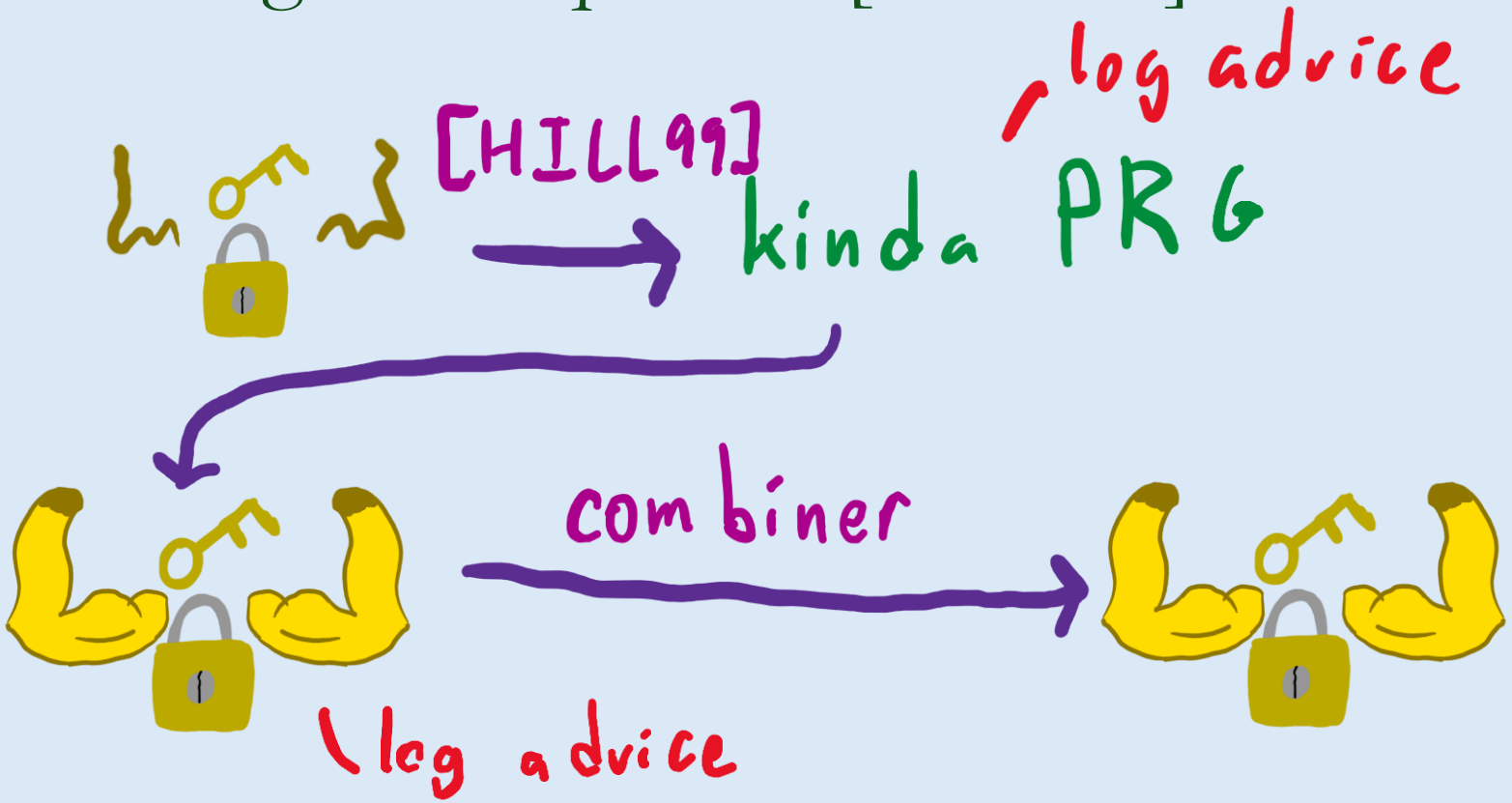


Our approach

- [KT24] builds "kinda PRGs" (EFID) from OWPuzz using techniques of [HILL99]

Our approach

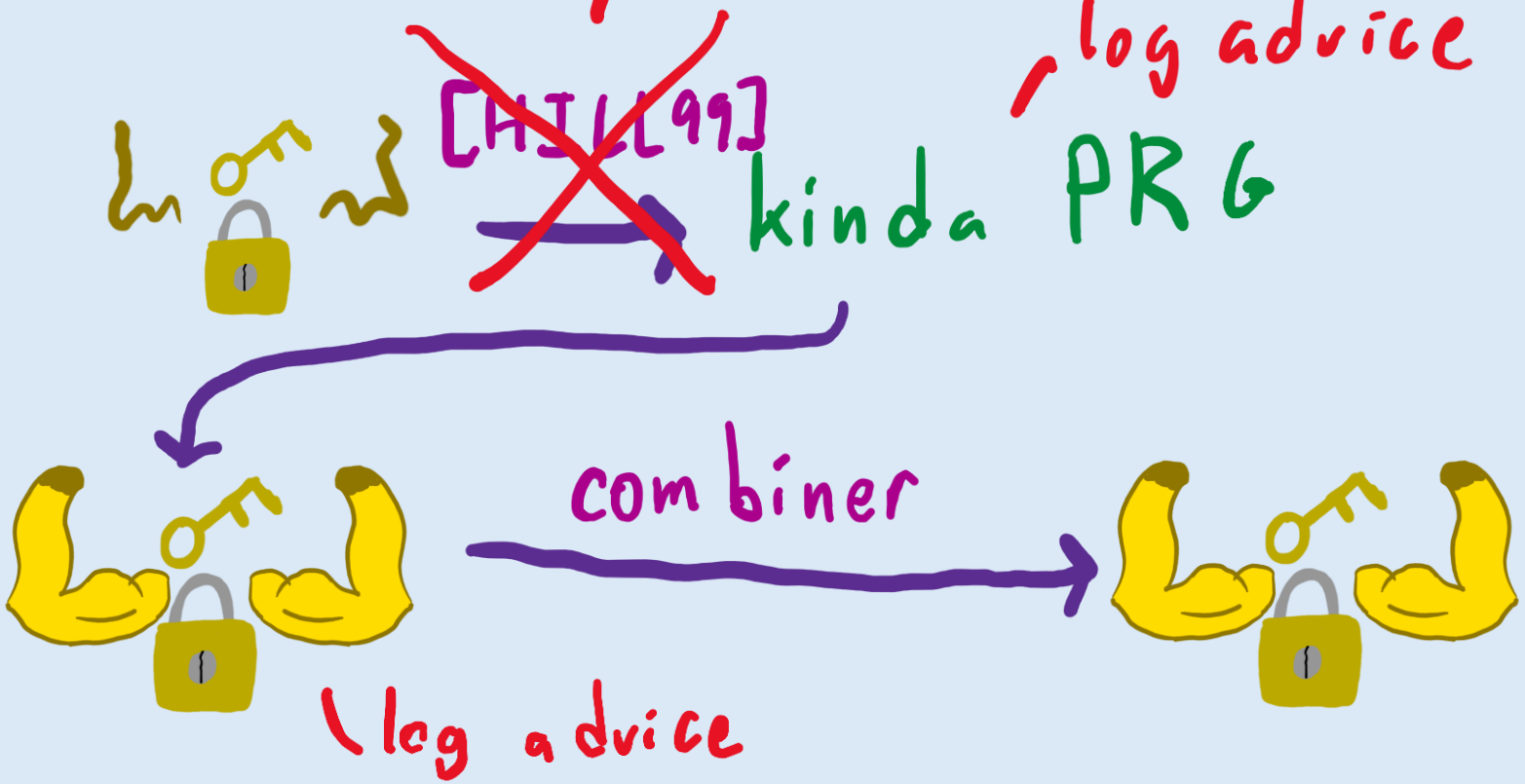
- [KT24] builds "kinda PRGs" (EFID) from OWPuzz using techniques of [HILL99]



Our approach

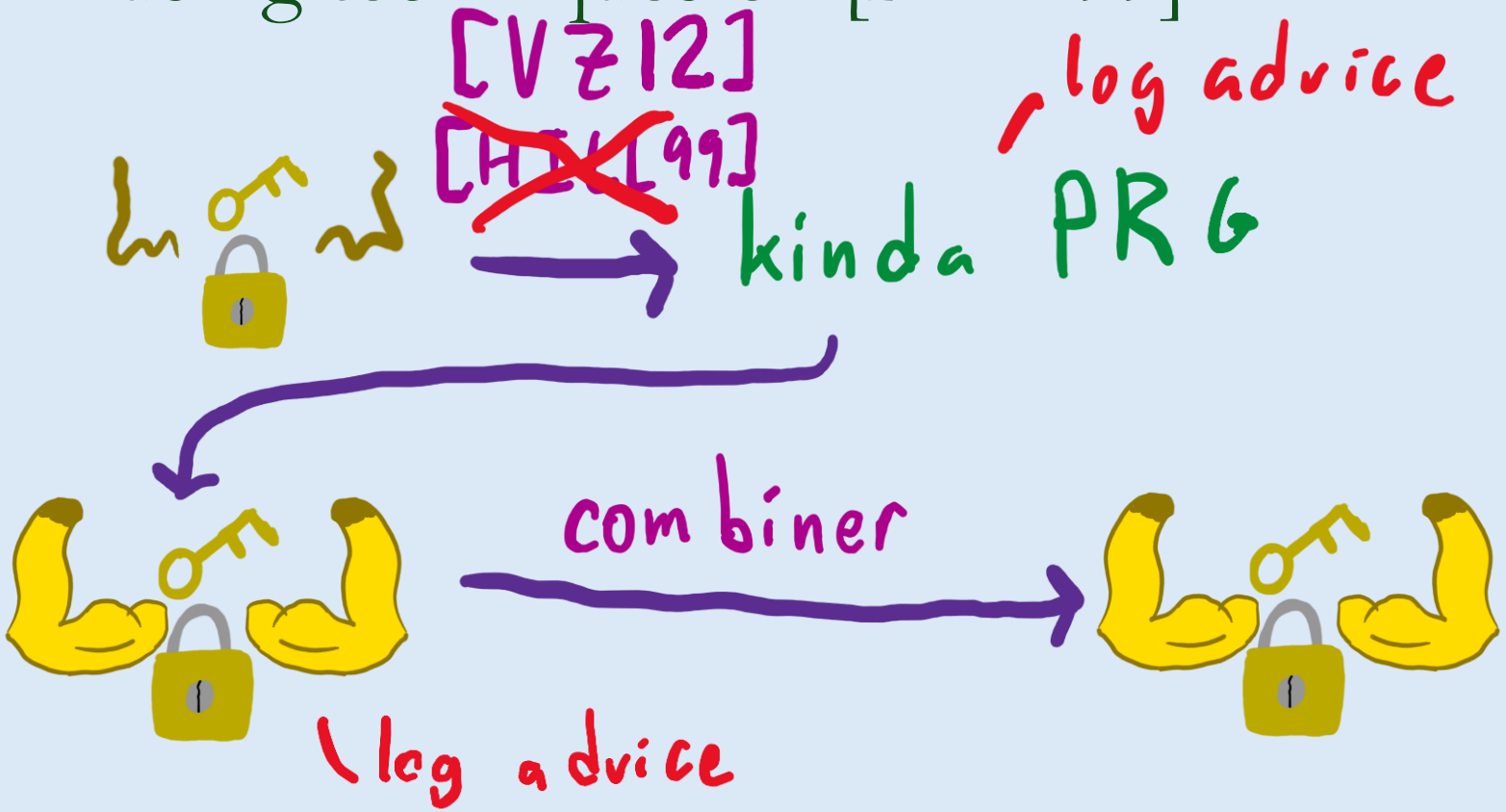
GL can only extract 1 bit of randomness

- [KT24] builds "kinda PRGs" (EFID) from OWPuzz using techniques of [HILL99]



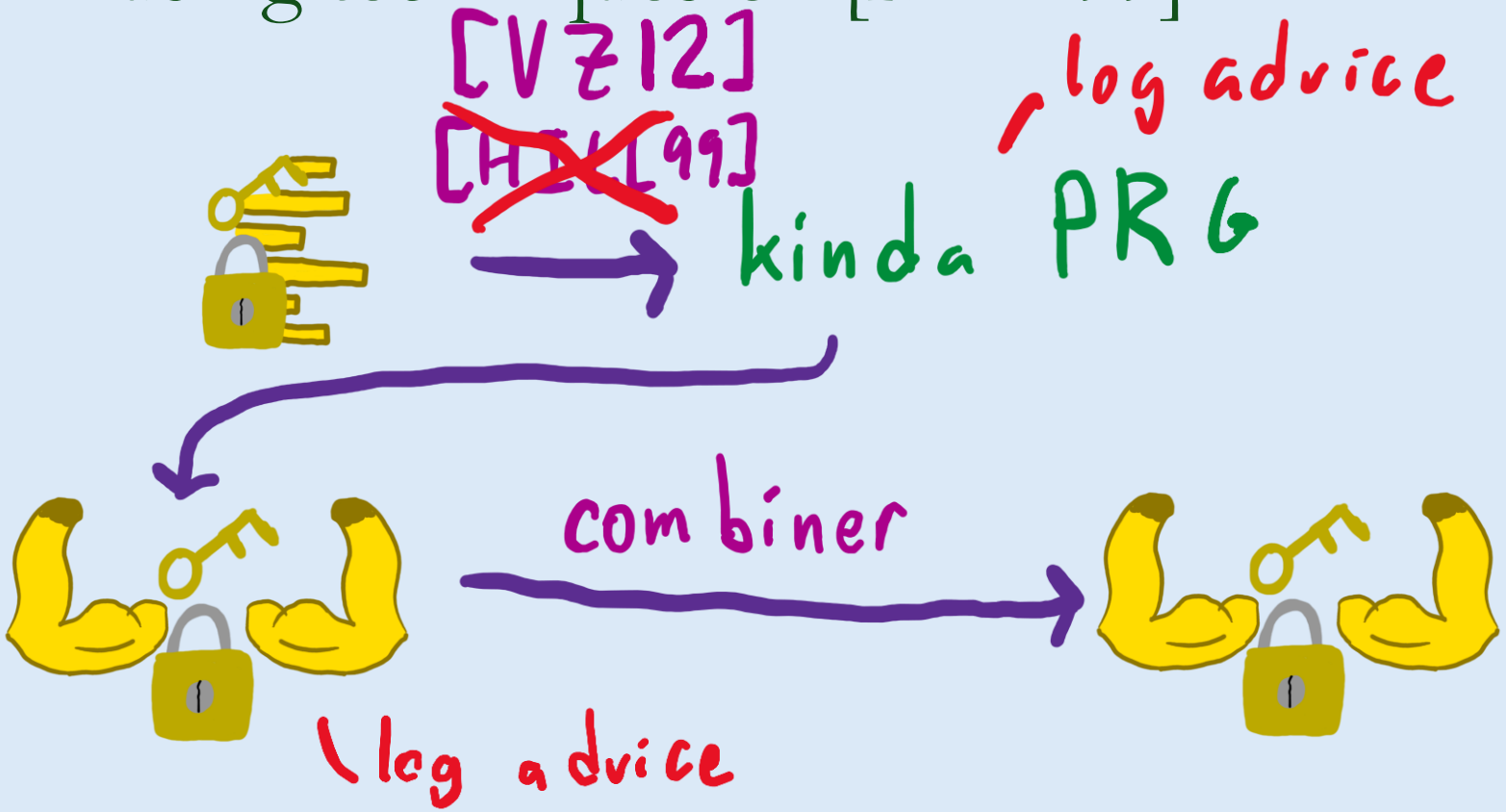
Our approach

- [KT24] builds "kinda PRGs" (EFID) from OWPuzz using techniques of [HILL99]



Our approach

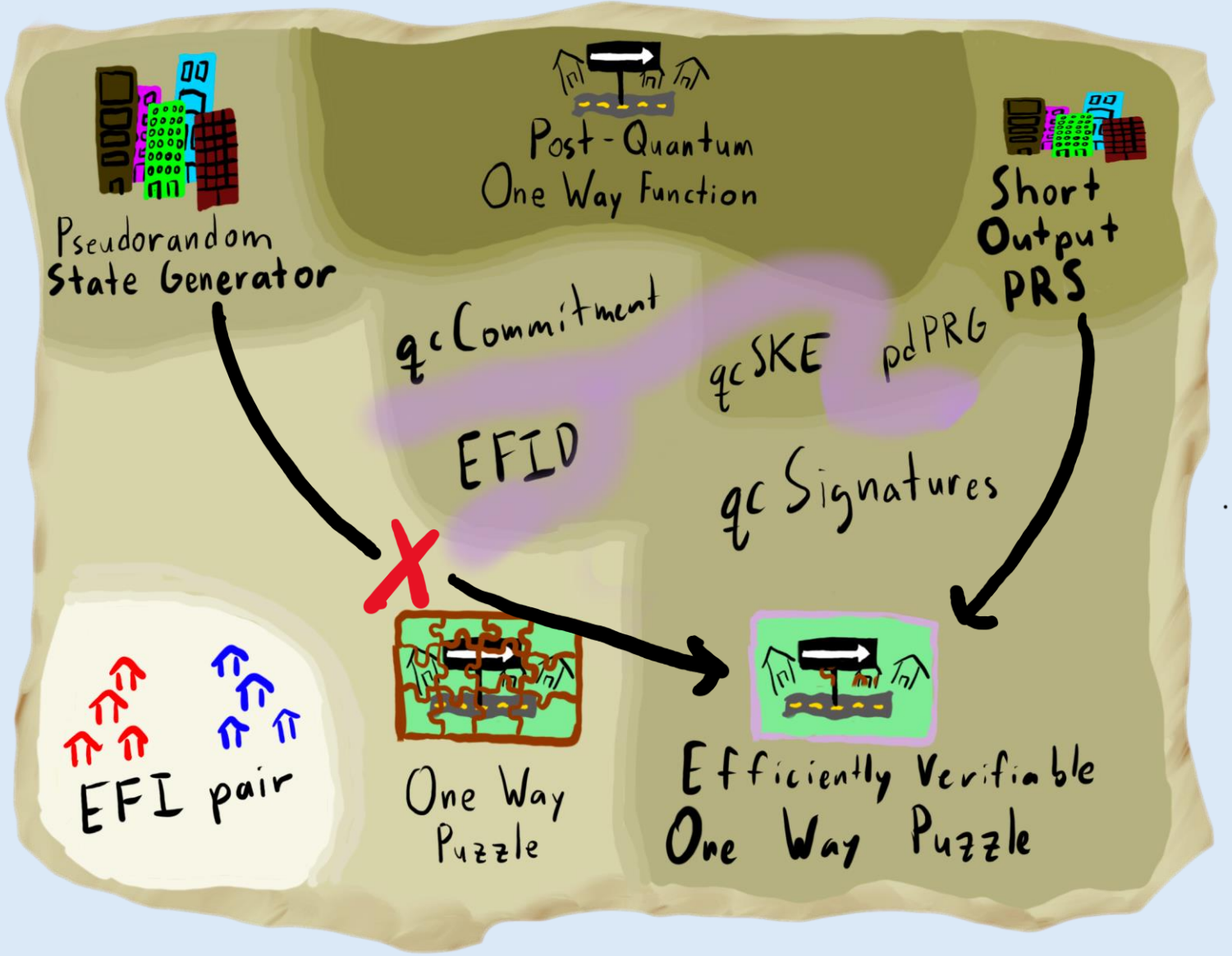
- [KT24] builds "kinda PRGs" (EFID) from OWPuzz using techniques of [HILL99]



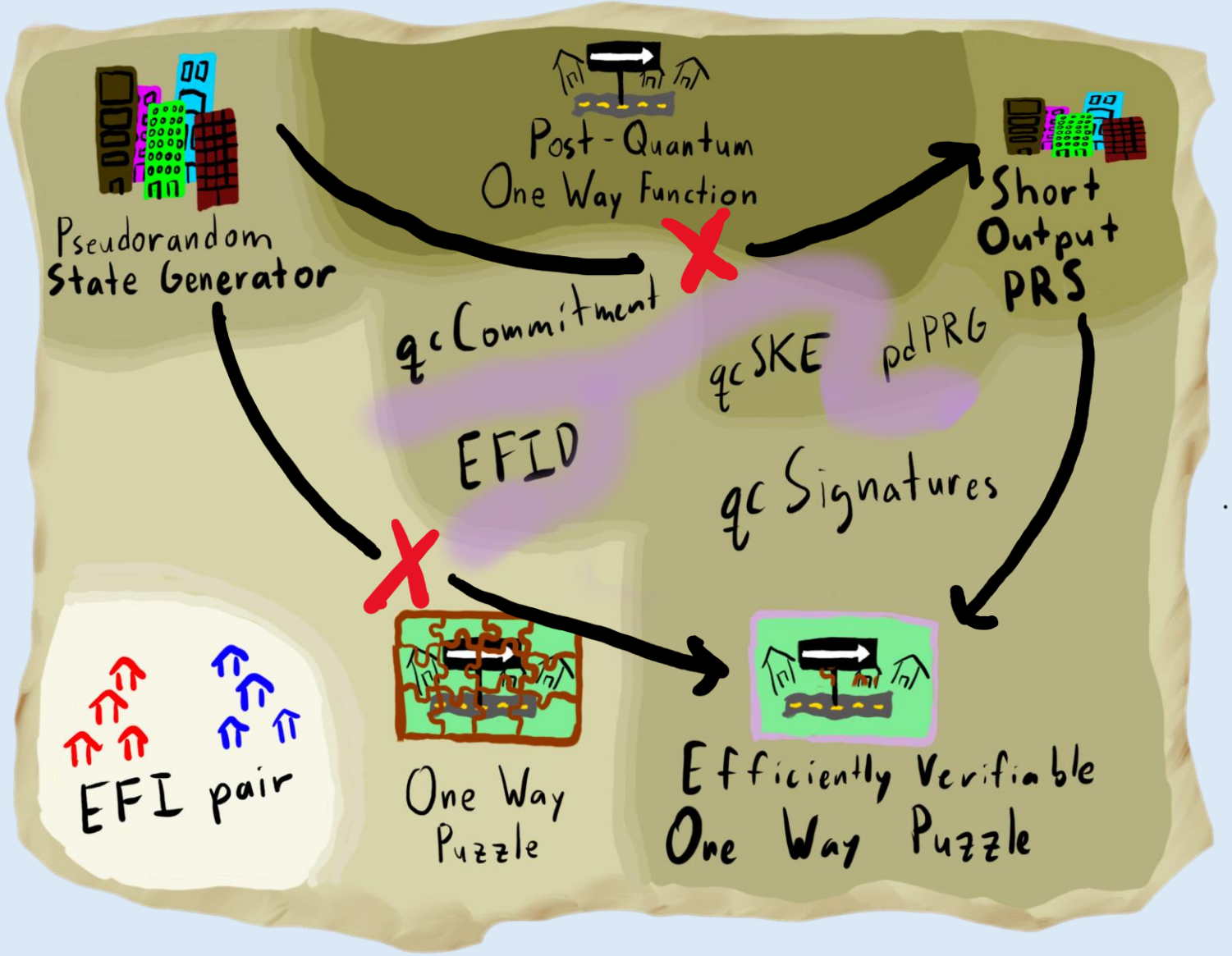
Additional Results

Additional Results

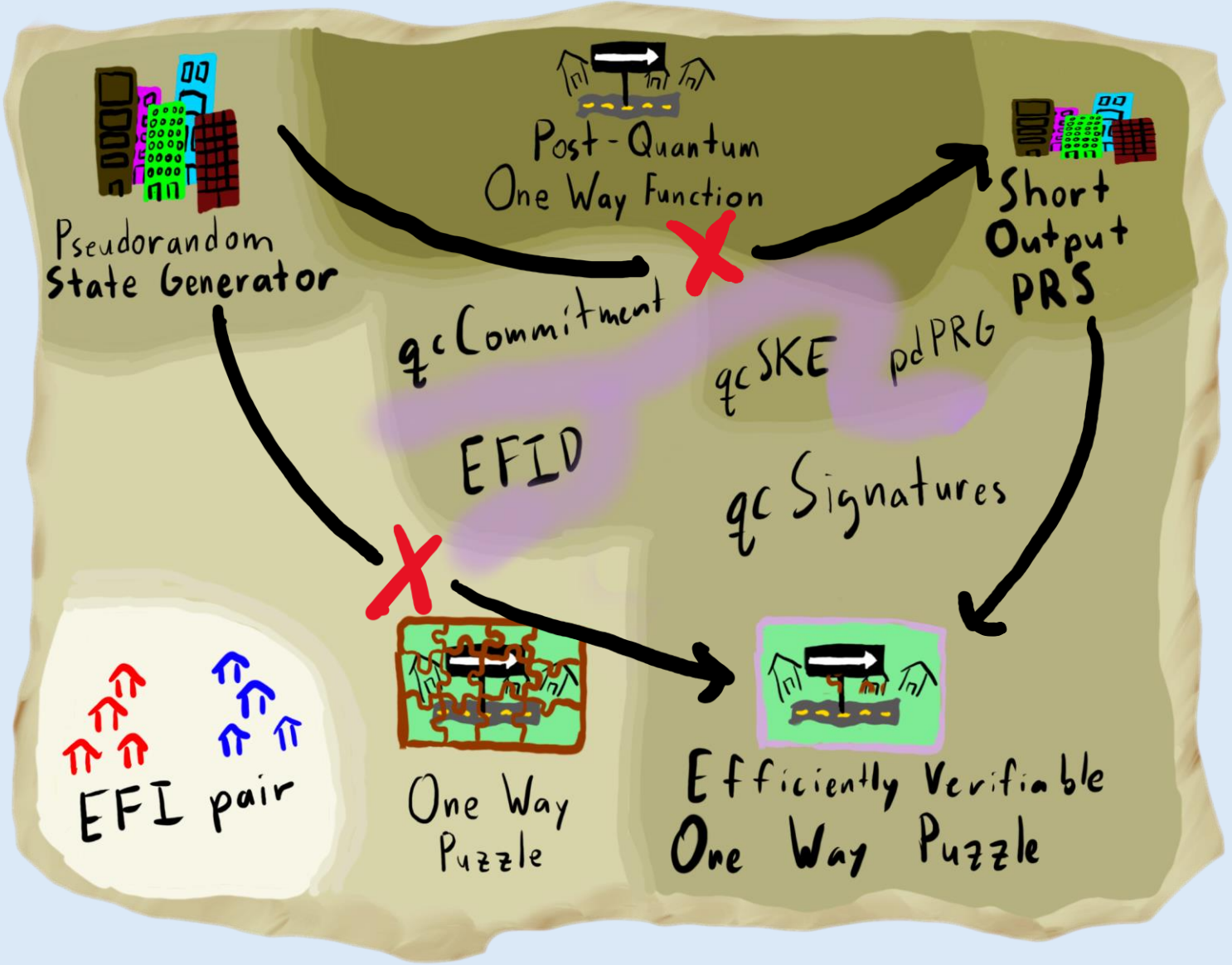
Additional Results



Additional Results



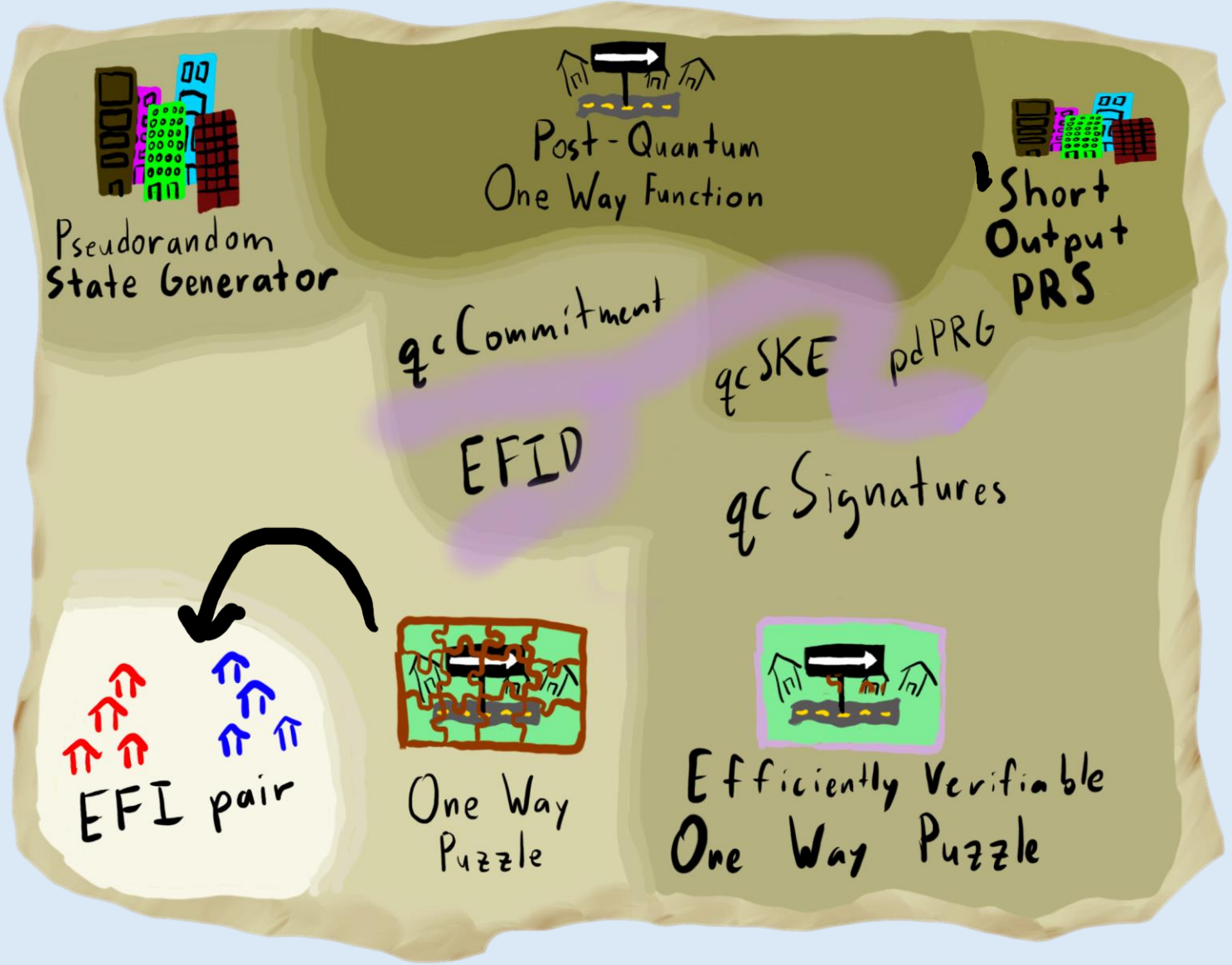
Additional Results



Separation between pseudorandom states with long output and short output.

Concurrently, [CM24][BM24]

Additional Results



Cleaner construction of EFI from OWPuzz using techniques of [VZ12]

Open Questions

$$\text{OWPuzz} \xrightarrow{?} \text{qc Commitments}$$

Open Questions

$$\text{OWPuzz} \xrightarrow{?} \text{qc Commitments}$$

$$\text{OWPuzz} \xrightarrow{?} \text{anything qc}$$

Open Questions

OWPuzz $\xrightarrow{?}$ qc Commitments

OWPuzz $\xrightarrow{?}$ anything qc

EV-OWPuzz $\xrightarrow{?}$ anything qc besides signatures