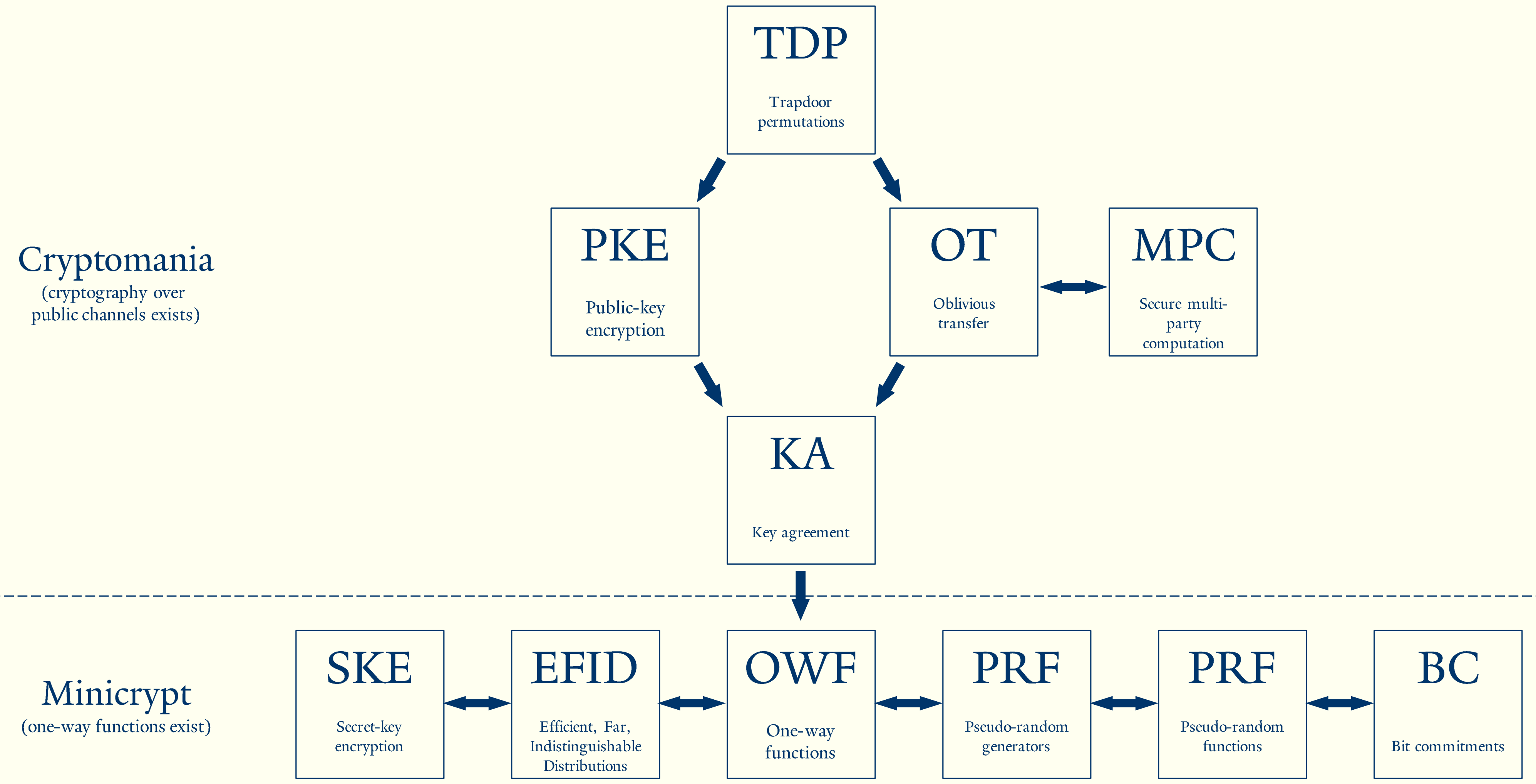
Oracle Separation Between Quantum Commitments and One-Wayness

John Bostanci (Columbia University)

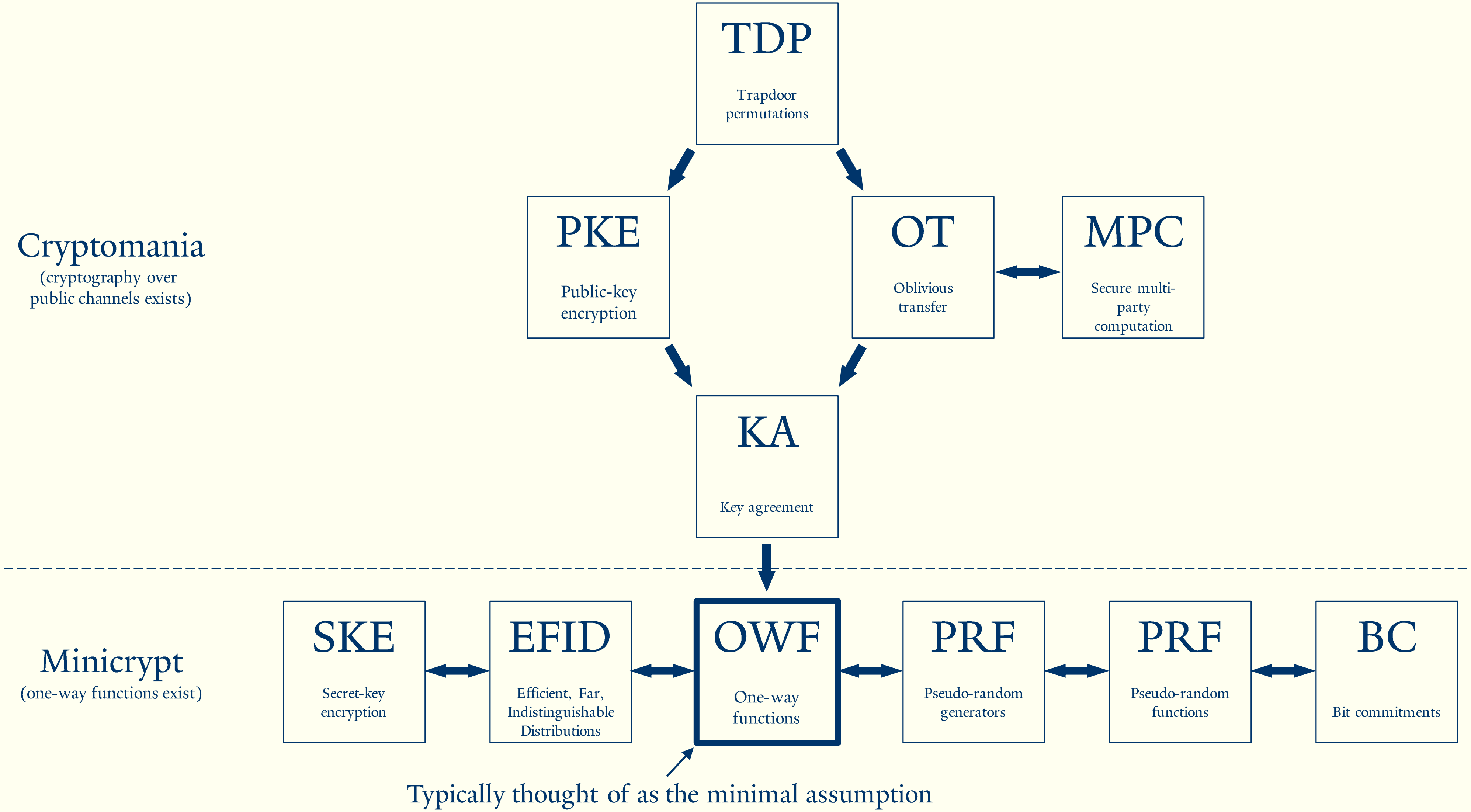
joint with Barak Nehoran (Princeton University) and

Boyang Chen (Tsinghua Univerity)

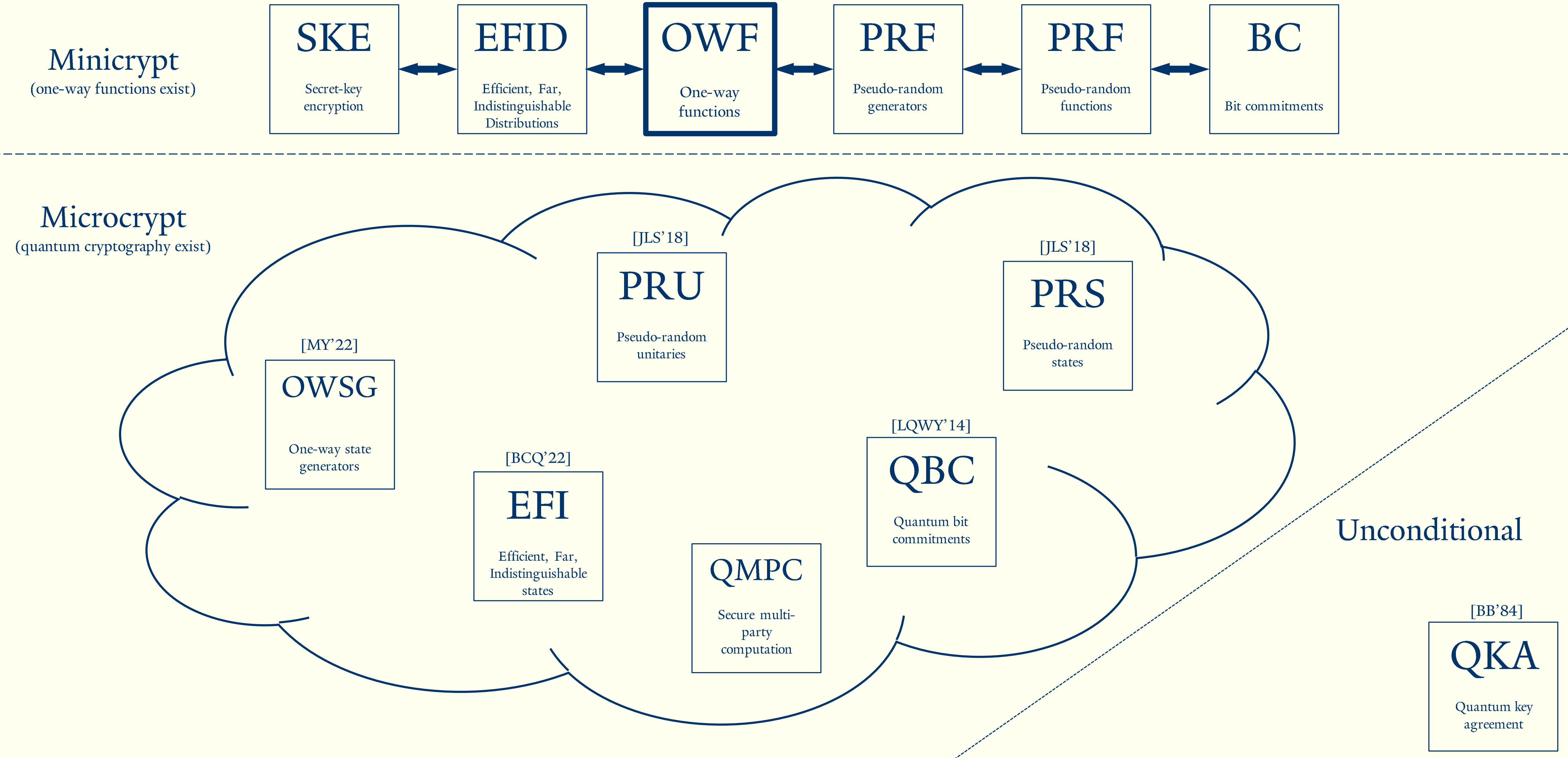
Landscape of (classical) cryptography



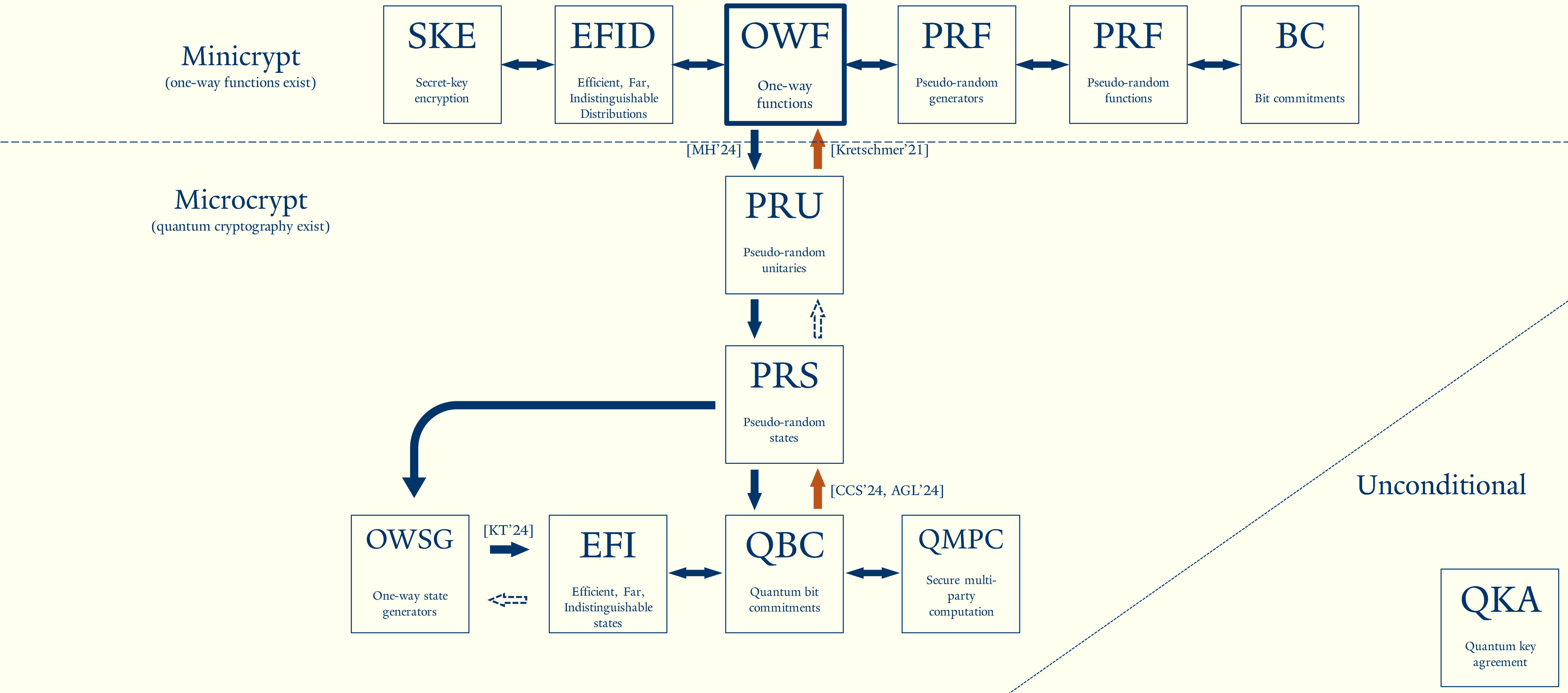
Landscape of (classical) cryptography



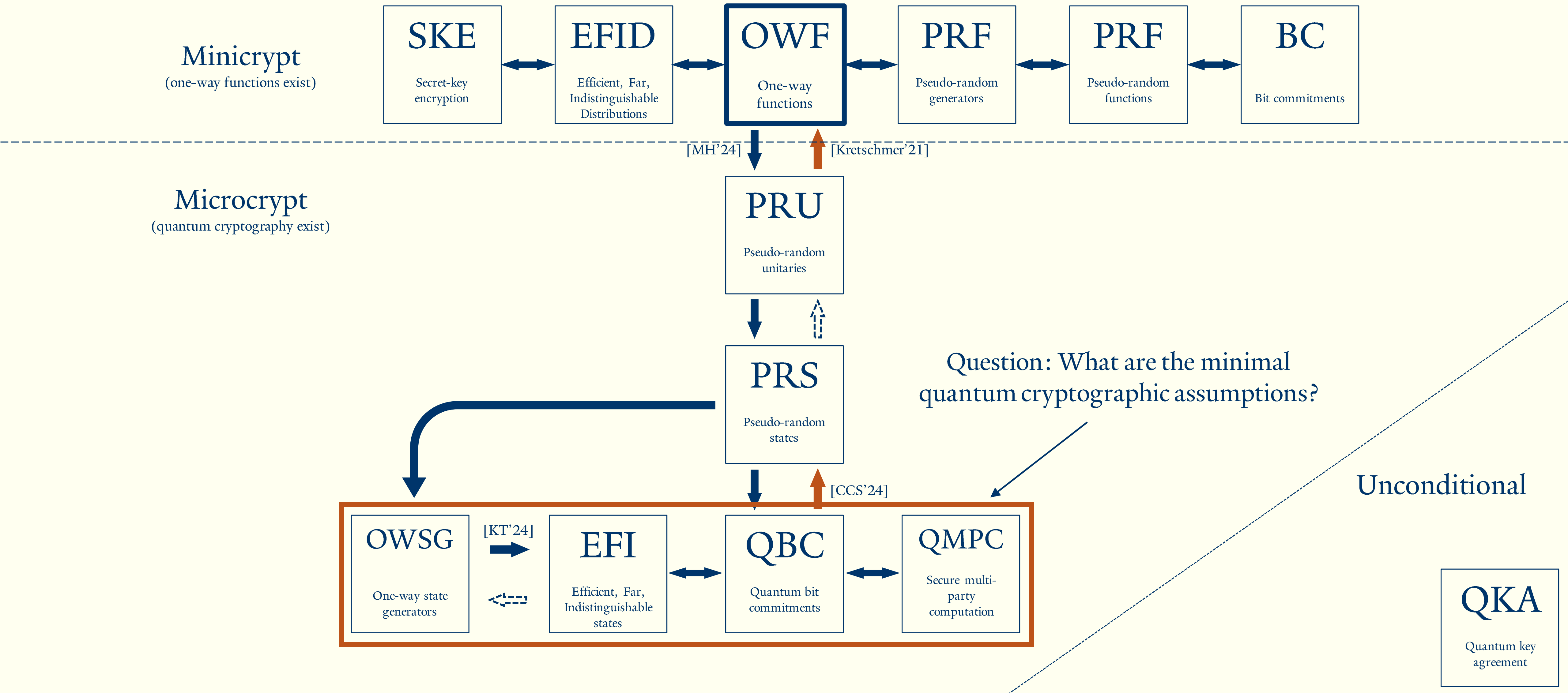
Landscape of quantum cryptography



Landscape of quantum cryptography



Landscape of quantum cryptography



One-way state generators

$$k \xrightarrow{\text{Gen}} \rho_k$$

One-way state generators

$$k \xrightarrow{\text{Gen}} \rho_k \qquad\qquad k, \rho_k \xrightarrow{\text{Ver}} \top$$

One-way state generators

$$k \xrightarrow{\text{Gen}} \rho_k \qquad\qquad k, \rho_k \xrightarrow{\text{Ver}} \top$$

$$k \overset{\text{Adversary}}{\not\longleftarrow} \rho_k$$

One-way state generators

- (Correctness) There is an efficient algorithm $\mathrm{Ver}(k, \rho)$ such that

$$\Pr_k[\top \leftarrow \mathrm{Ver}(k, \rho_k)] \geq 1 - \mathrm{negl}(\lambda).$$

One-way state generators

- (Correctness) There is an efficient algorithm $\mathrm{Ver}(k, \rho)$ such that

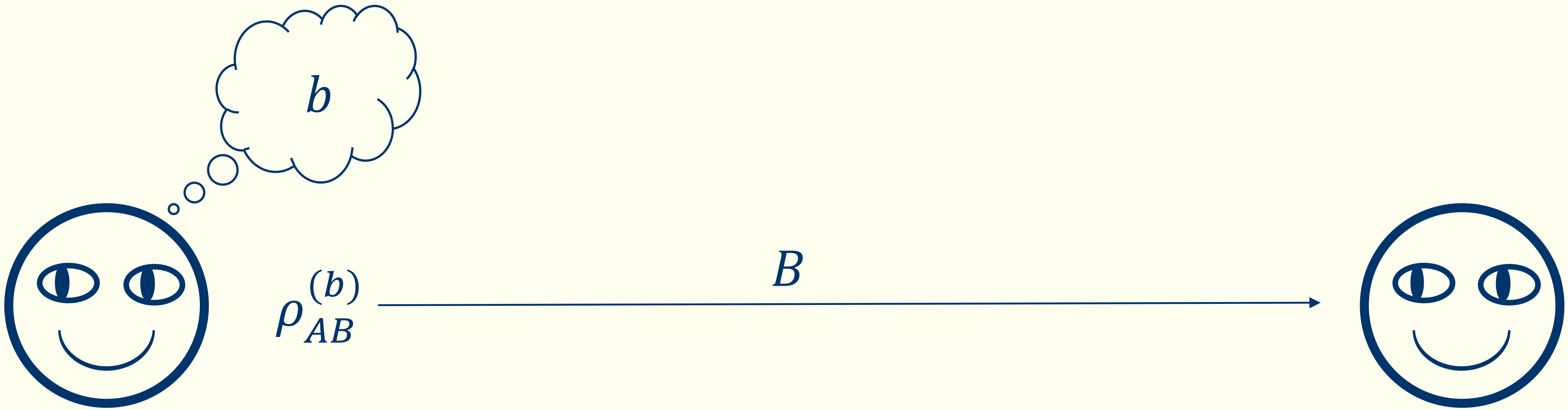
$$\Pr_{k}[\top \leftarrow \mathrm{Ver}(k, \rho_k)] \geq 1 - \mathrm{negl}(\lambda).$$

- (Security) For all efficient adversaries A,

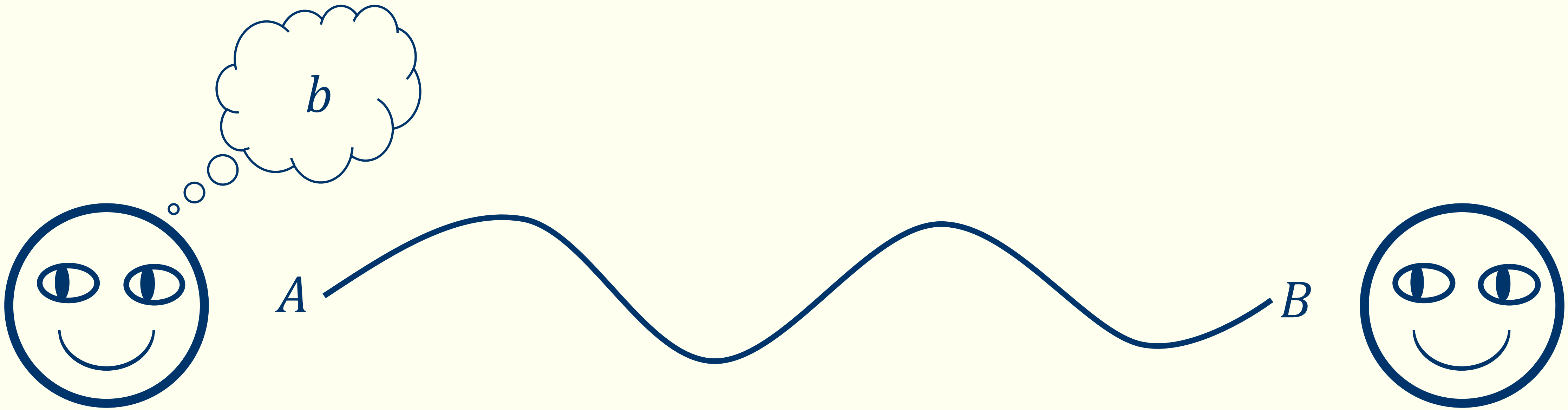
$$\Pr_{k}\left[\top \leftarrow \mathrm{Ver}(k', \rho_k) \mid k' \leftarrow \mathrm{A}(\rho_k^{\otimes t(\lambda)})\right] \leq \mathrm{negl}(\lambda).$$

Quantum bit commitments

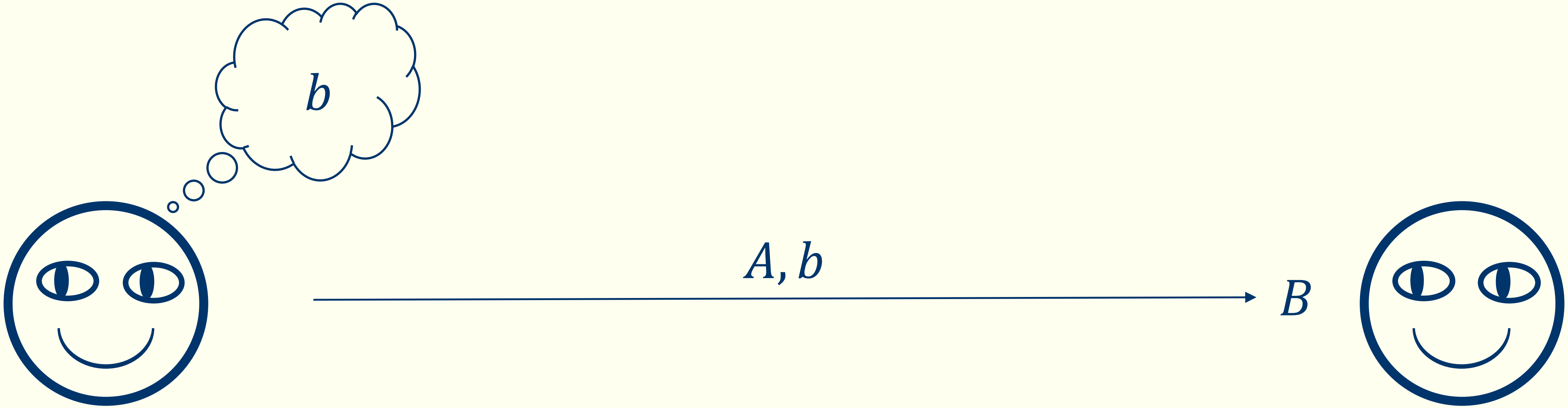
Quantum bit commitments



Quantum bit commitments



Quantum bit commitments



Quantum bit commitments

Quantum bit commitments

- (Hiding) For all efficient adversaries A,

$$\Pr\left[\top \leftarrow \mathrm{A}\left(\rho_B^{(0)}\right)\right] - \Pr\left[\top \leftarrow \mathrm{A}\left(\rho_B^{(1)}\right)\right] \leq \mathrm{negl}(\lambda).$$

Quantum bit commitments

- (Hiding) For all efficient adversaries A,

$$\Pr\left[\top \leftarrow \mathrm{A}\left(\rho_B^{(0)}\right)\right] - \Pr\left[\top \leftarrow \mathrm{A}\left(\rho_B^{(1)}\right)\right] \leq \mathrm{negl}(\lambda).$$

- (Binding) For all (possibly inefficient) adversaries A,

$$\mathrm{F}\left(\mathrm{A}\left(\rho_A^{(0)}\right), \rho_A^{(1)}\right) \leq \mathrm{negl}(\lambda).$$

EFI pairs

The states $\left(\rho_B^{(0)}, \rho_B^{(1)}\right)$ used in a canonical quantum commitment are also an EFI pair:

EFI pairs

The states $\left(\rho_B^{(0)}, \rho_B^{(1)}\right)$ used in a canonical quantum commitment are also an EFI pair:

- Efficient: The committer can generate them in polynomial time.

EFI pairs

The states $\left(\rho_B^{(0)}, \rho_B^{(1)}\right)$ used in a canonical quantum commitment are also an EFI pair:

- Efficient: The committer can generate them in polynomial time.
- Statistically Far: Binding gives us that the two states have high trace distance.

EFI pairs

The states $\left(\rho_B^{(0)}, \rho_B^{(1)}\right)$ used in a canonical quantum commitment are also an EFI pair:

- Efficient: The committer can generate them in polynomial time.
- Statistically Far: Binding gives us that the two states have high trace distance.
- Computationally Indistinguishable: Hiding guarantees that no efficient adversary can distinguish them.

The common Haar random state model

In the common Haar random state model (CHRS) [CCS'24, AGL'24], there are a collection of states $\{|\psi_\ell\rangle\}_{\ell \in \mathbb{N}}$ that are sampled uniformly at random from the Haar measure, and all parties get sample access to the states.

Our main result

Relative to a common Haar random state and a unitaryPSPACE oracle,
one-way state generators do not exist.

Our main result

Relative to a common Haar random state and a unitaryPSPACE oracle,
one-way state generators do not exist.

Since quantum bit commitments exist in the common Haar random state model [CCS’24, AGL’24], this separates quantum bit commitments and one-way state generators.

Ruling out OWSG in the CHRS

Ruling out OWSG in the CHRS

Given copies $\rho_k^{\otimes\lambda}$ and many copies of the Haar random state, consider the following algorithm that learns k:

Ruling out OWSG in the CHRS

Given copies $\rho_k^{\otimes\lambda}$ and many copies of the Haar random state, consider the following algorithm that learns k:

For i from 0 to 2^λ:

Ruling out OWSG in the CHRS

Given copies $\rho_k^{\otimes\lambda}$ and many copies of the Haar random state, consider the following algorithm that learns k:

For i from 0 to 2^λ:

- Sample a "random" k'.

Ruling out OWSG in the CHRS

Given copies $\rho_k^{\otimes \lambda}$ and many copies of the Haar random state, consider the following algorithm that learns k:

For i from 0 to 2^λ:

- Sample a "random" k'.
- Run $\mathrm{Ver}^{\{|\psi_\ell\rangle\}}(k', \rho_k)$, λ many times.

Ruling out OWSG in the CHRS

Given copies $\rho_k^{\otimes \lambda}$ and many copies of the Haar random state, consider the following algorithm that learns k:

For i from 0 to 2^λ:

- Sample a "random" k'.
- Run $\mathrm{Ver}^{\{|\psi_\ell\rangle\}}(k', \rho_k)$, λ many times.
- If all accept, halt and output k'.

Ruling out OWSG in the CHRS

Given copies $\rho_k^{\otimes\lambda}$ and many copies of the Haar random state, consider the following algorithm that learns k:

For i from 0 to 2^λ:

- Sample a "random" k'.
- Run $\mathsf{Ver}^{\{|\psi_\ell\rangle\}}(k', \rho_k)$, λ many times.
- If all accept, halt and output k'.
- Otherwise, uncompute every $\mathsf{Ver}(k', \rho_k)$, and continue.

Ruling out OWSG in the CHRS

From the gentle random measurement lemma [WB23], this algorithm outputs a k' such that $k' = k$ with constant probability.

Ruling out OWSG in the CHRS

From the gentle random measurement lemma [WB23], this algorithm outputs a k' such that $k' = k$ with constant probability.

Using a pseudo-random generator (against PSPACE) and deferred measurement, the entire algorithm can be described by a deterministic PSPACE quantum circuit.

Interpretations of the result

It seems like quantum bit commitments (and equivalent primitives) are a minimal world for quantum cryptography (at least, mathematically). How should we interpret this world?

Interpretations of the result

It seems like quantum bit commitments (and equivalent primitives) are a minimal world for quantum cryptography (at least, mathematically). How should we interpret this world?

Efficient verification versus inefficient verification?

Interpretations of the result

It seems like quantum bit commitments (and equivalent primitives) are a minimal world for quantum cryptography (at least, mathematically). How should we interpret this world?

~~Efficient verification versus inefficient verification?~~

Un-entangled versus entangled?

Landscape of quantum cryptography now