Quantum cryptography without one-way functions

Tomoyuki Morimae
(Yukawa Institute for Theoretical Physics, Kyoto University)

40min

Why cryptography for physicists?

Computational indistinguishability is strong tool

Consider two quantum states, $\rho_0 \; and \; \rho_1$

They are very different

$$|| \rho_0 - \rho_1 ||_1 \simeq 1$$

But no quantum polynomial-time operation can distinguish them

In that case, we can say $\rho_0 = \rho_1$, because operations in nature are polynomial-time

Applications

The state ρ should be thermal equilibrium state, but not…

The entanglement of ρ should large, but not…

If ρ is computationally indistinguishable from thermal equilibrium state or highly-entangled state, the paradox is solved!

Example 1: Pseudo entanglement

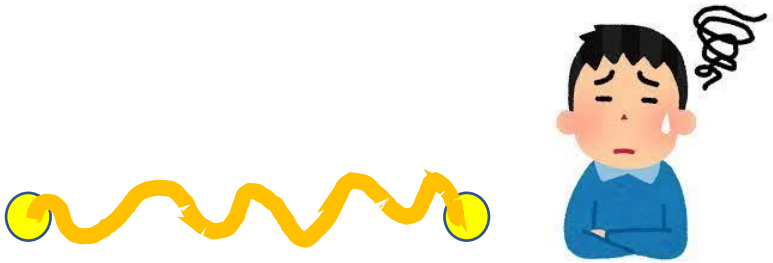
$m \gg n$

$$Q_0|0 \dots 0\rangle_{C,R} = \sum_{k\in\{0,1\}^n} |k\rangle_R \otimes |\phi_k\rangle_C$$ EE=n Pseudo EE=m

$$Q_1|0 \dots 0\rangle_{C,R} = \sum_{z\in\{0,1\}^m} |z\rangle_R \otimes |z\rangle_C$$ EE=m

Real entanglement is small, but it can be considered as large!

Example 2: Hayden-Harlow

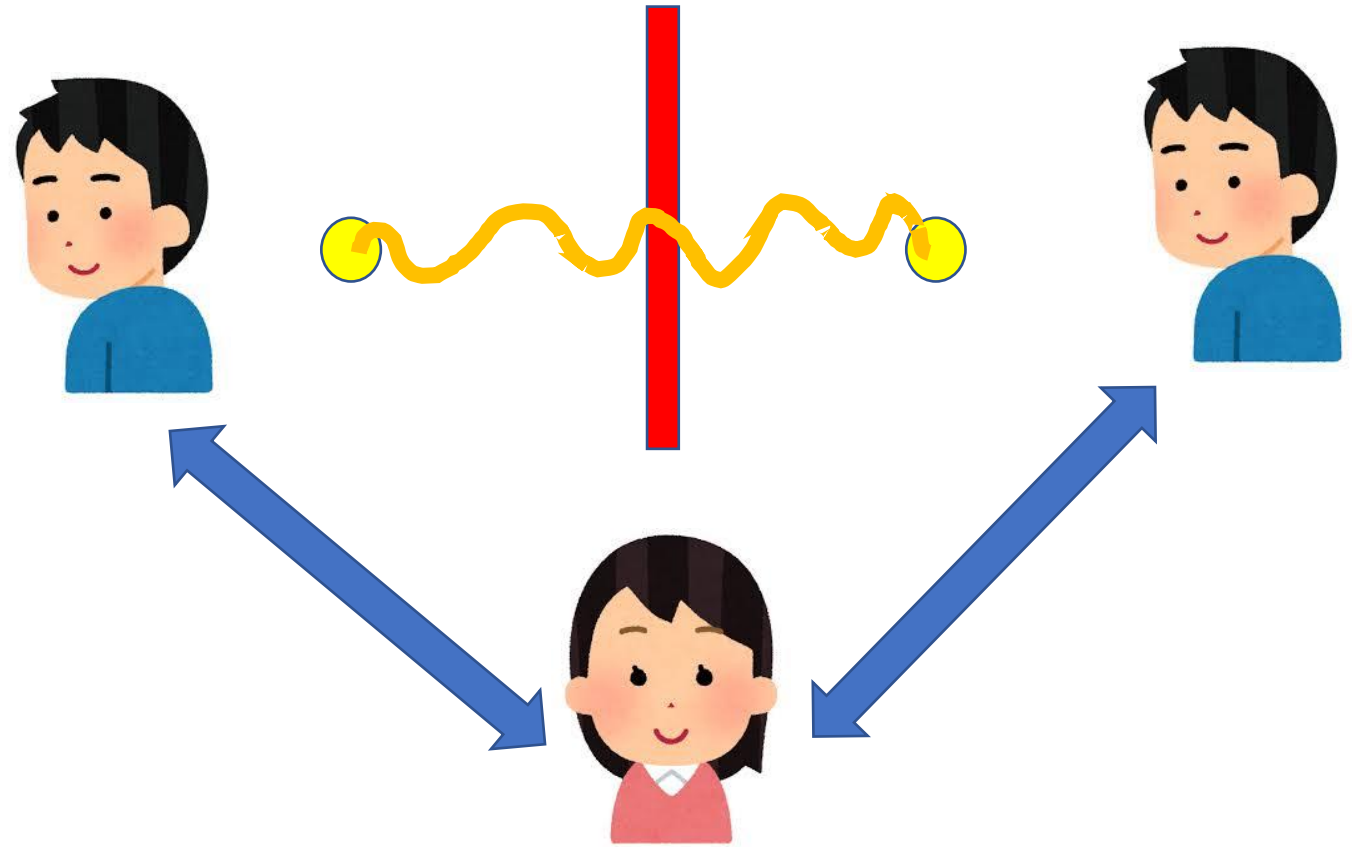


To explain a black-hole paradox, a ``hidden" entanglement that can be extracted in principle, but hard to extract is required.

Hayden-Harlow: such hidden entanglement exists if SZK $\neq$ BQP
Aaronson: such hidden entanglement exists if OWPs exist

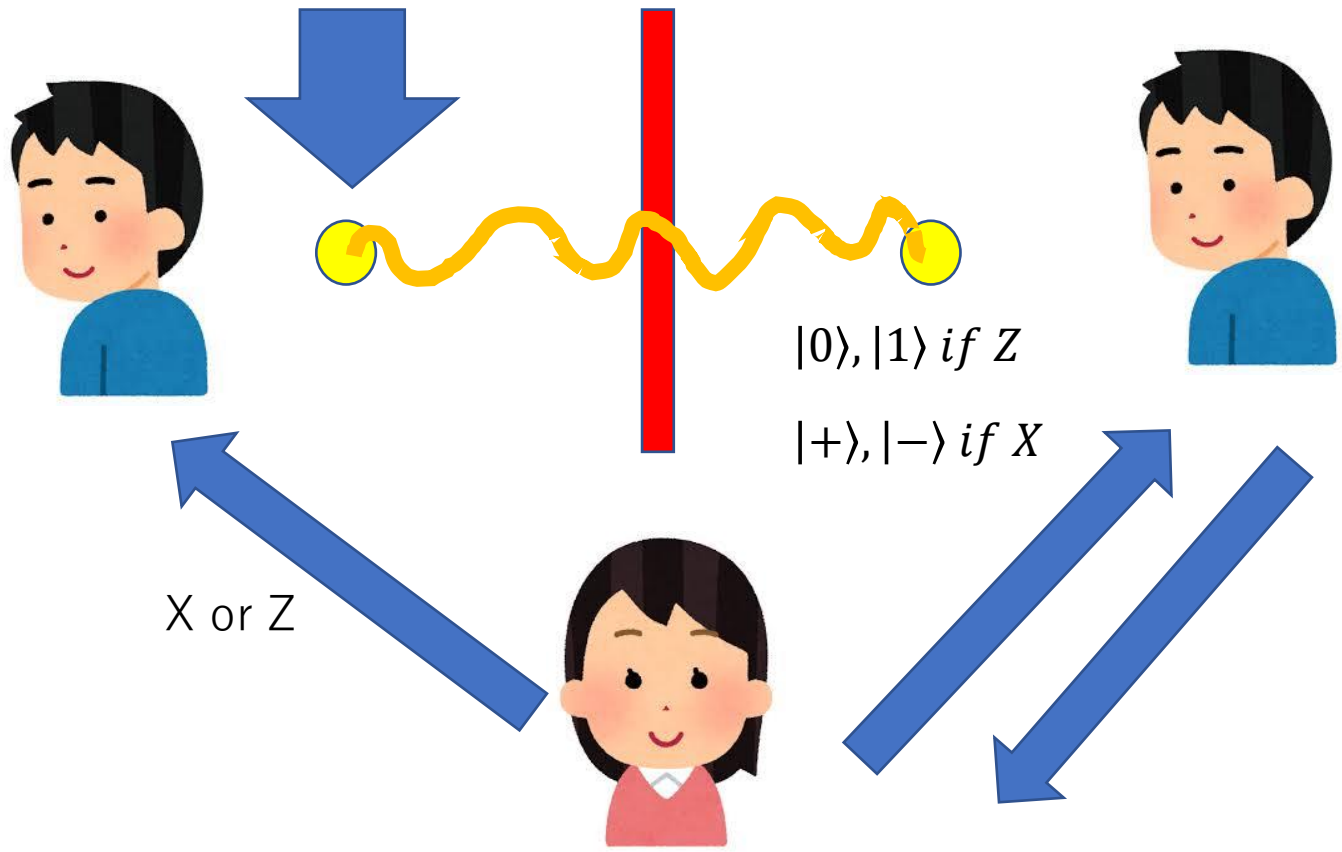
[Brakerski, arXiv: 2211.05491] showed such hidden entanglement exists if EFI exist

Example 3: Bell's inequality

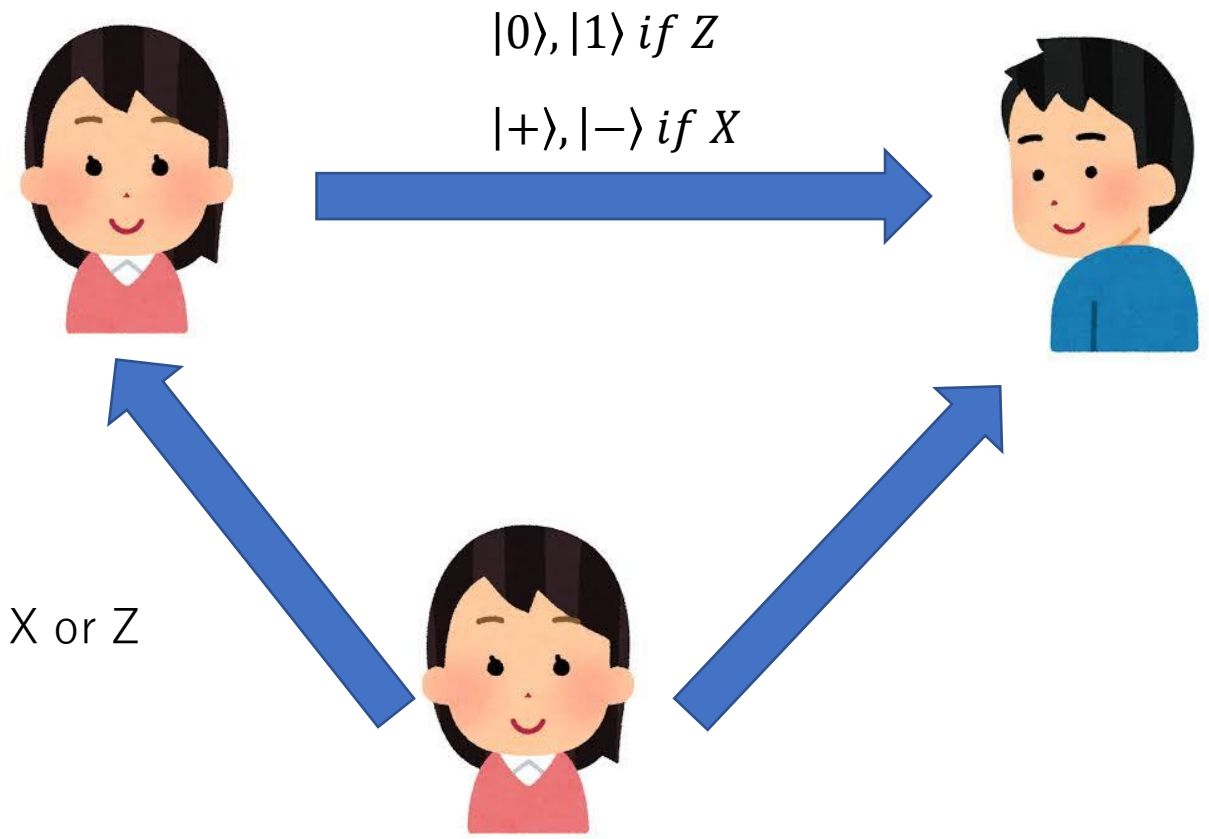


（1）Alice accepts if Bobs are entangled
（2）Alice rejects if Bobs are not entangled

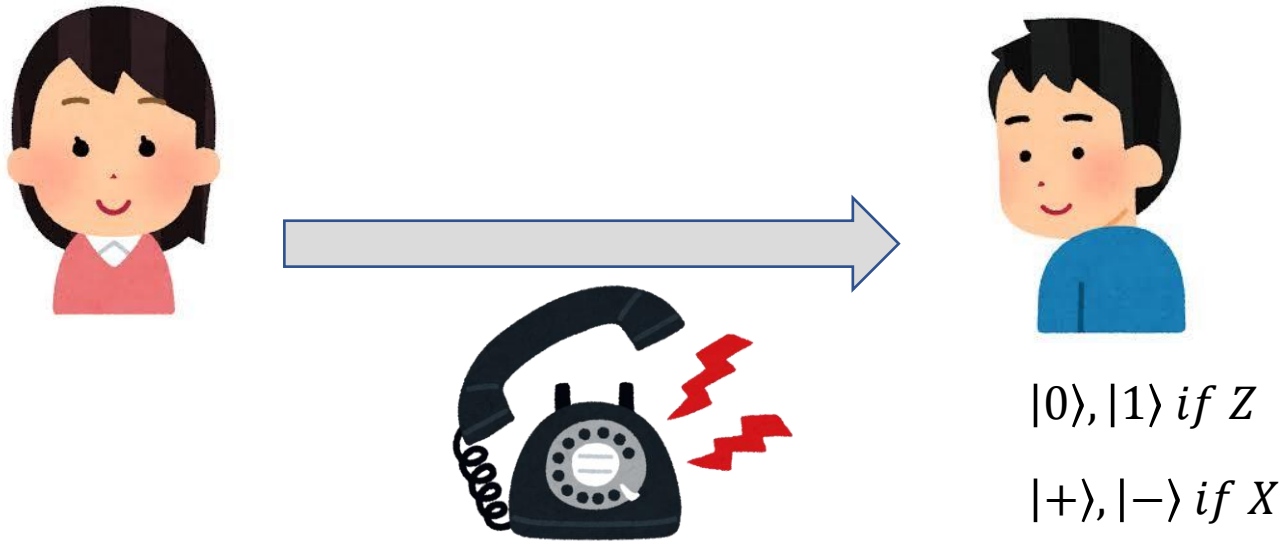
Quantum advantage can be shown unconditionally, but Bob should not talk with each other



Classical Bob 2 cannot answer the correct measurement result because he does not know the state



This is Bad because now Alice is quantum



How can Alice ``send" quantum state to Bob over only classical channel in such a way that Bob cannot learn the state?

We can use cryptography!

Computational Bell's inequality
[Kahanamoku-Meyer, Choi, Vazirani, Yao, Nature Phys. 2022]

(1)trapdoor
(2)2-to-1 collision resistant hash

td

f

$$\sum_x |x\rangle|f(x)\rangle$$

y

$$|x_0\rangle + |x_1\rangle$$

$$f(x_0) = f(x_1) = y$$

r

$$|r \cdot x_0\rangle|x_0\rangle + |r \cdot x_1\rangle|x_1\rangle$$

$$|r \cdot x_0\rangle + (-1)^{d\cdot(x_0 \oplus x_1)}|r \cdot x_1\rangle$$

$$|0\rangle, |1\rangle, |+\rangle, |-\rangle$$

We show that CRHFs can be replaced with TDP [Morimae and Yamakawa, ITCS2023]

Two types of security in cryptography

Statistical security: secure against any unbounded adversary（ex: One-time pad）

Statistically-secure primitives have some limitations

Computational security: secure under some complexity assumptions（ex: Public key encryption）

Trapdoor permutation $f: \{0,1\}^n \to \{0,1\}^n$

x→f(x) is easy
f(x)→x is hard (easy with td)

$f(m)$

$f(m) \to m$

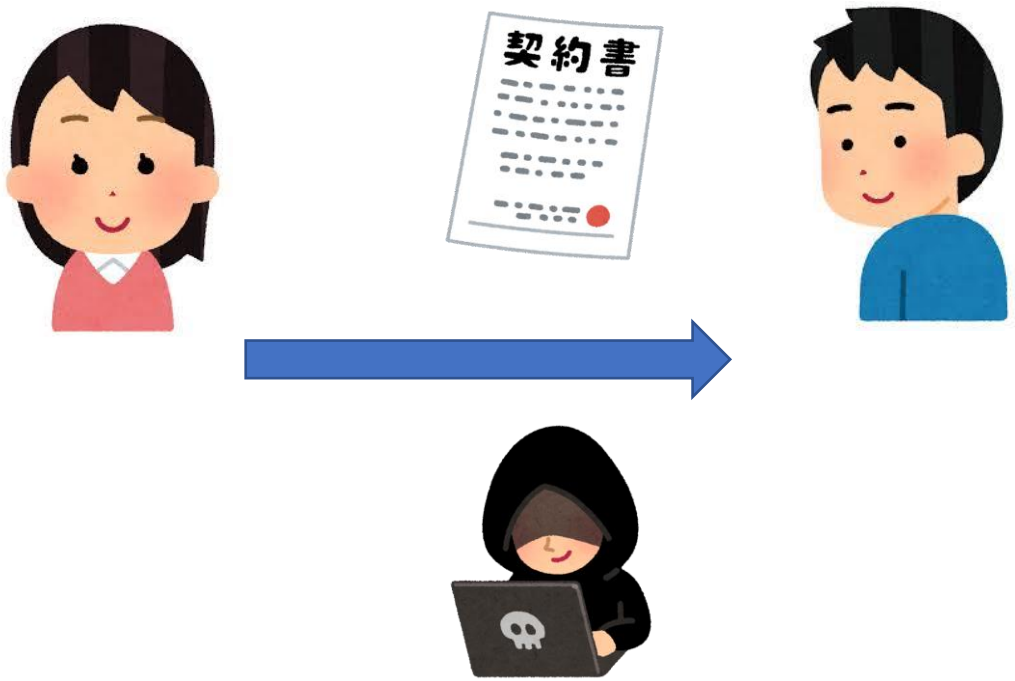
Limitations can be overcomed in computational settings

cryptography ≠ secret communication

For example,

Public key encryption
Digital signatures
Pseudorandom generators
Commitments
Zero-knowledge
Multiparty computation

Example1: Digital signatures



Computational security: brute-force attack can forge signatures

Example 2: Pseudorandom generators

$f: \{0,1\}^n \to \{0,1\}^{2n}$

$x \leftarrow \{0,1\}^n$

$f(x)$

$y \leftarrow \{0,1\}^{2n}$

y

indistinguishable

Example 3: Commitments

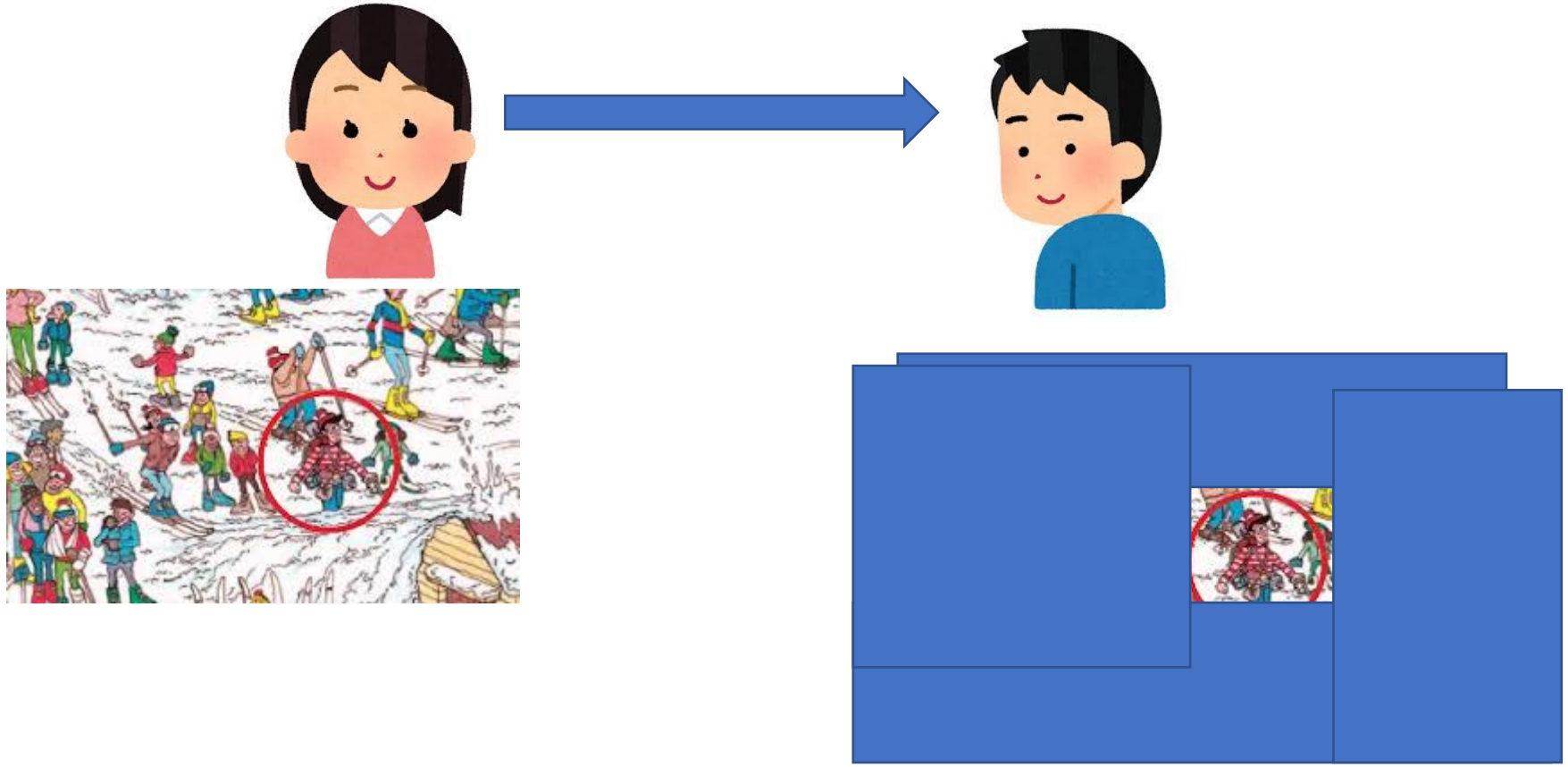
Hiding: committed bit is hidden to the receiver

Binding: committed bit cannot be changed by the sender

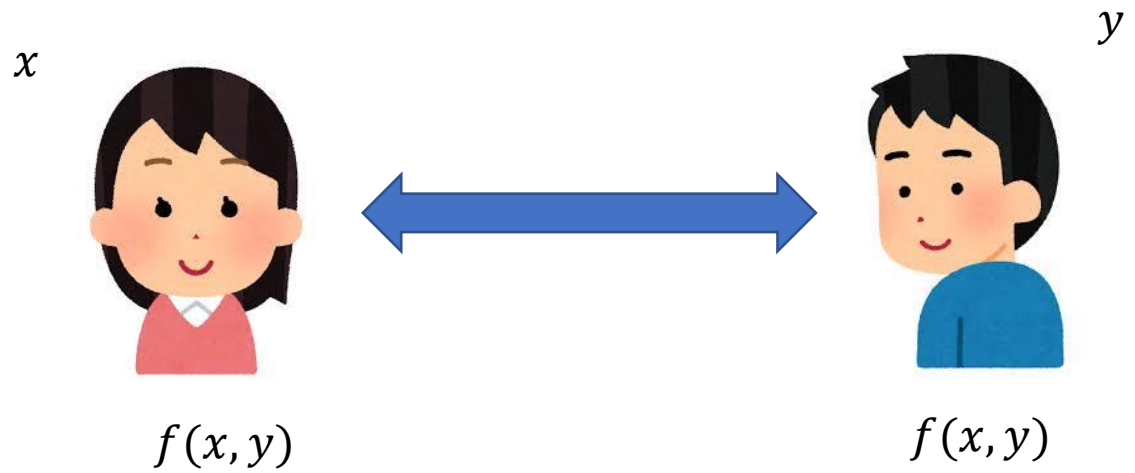
Even in the quantum world, statistically-hiding and statistically-binding is impossible

Example 4: zero knowledge

Showing a statement is correct without leaking any information beyond that

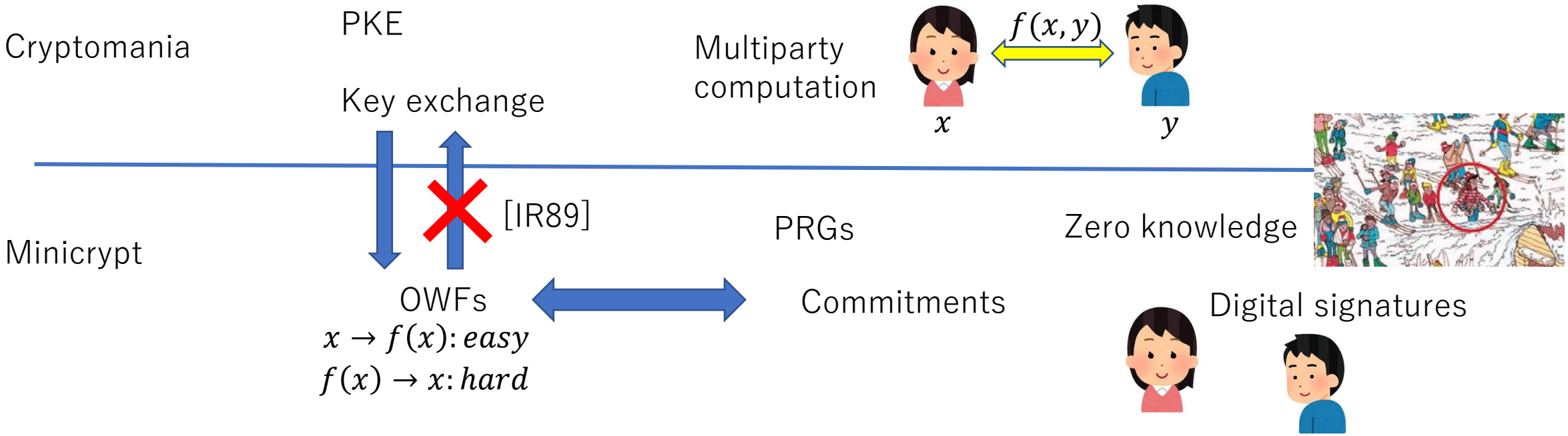


Example 5: multiparty computation



Computing f(x,y) without revealing x and y

Classical cryptography



OWF is the most fundamental element in classical cryptography

[Russell Impagliazzo and Michael Luby, 1989, One-way functions are essential for complexity based cryptography]

The same in quantum cryptography?

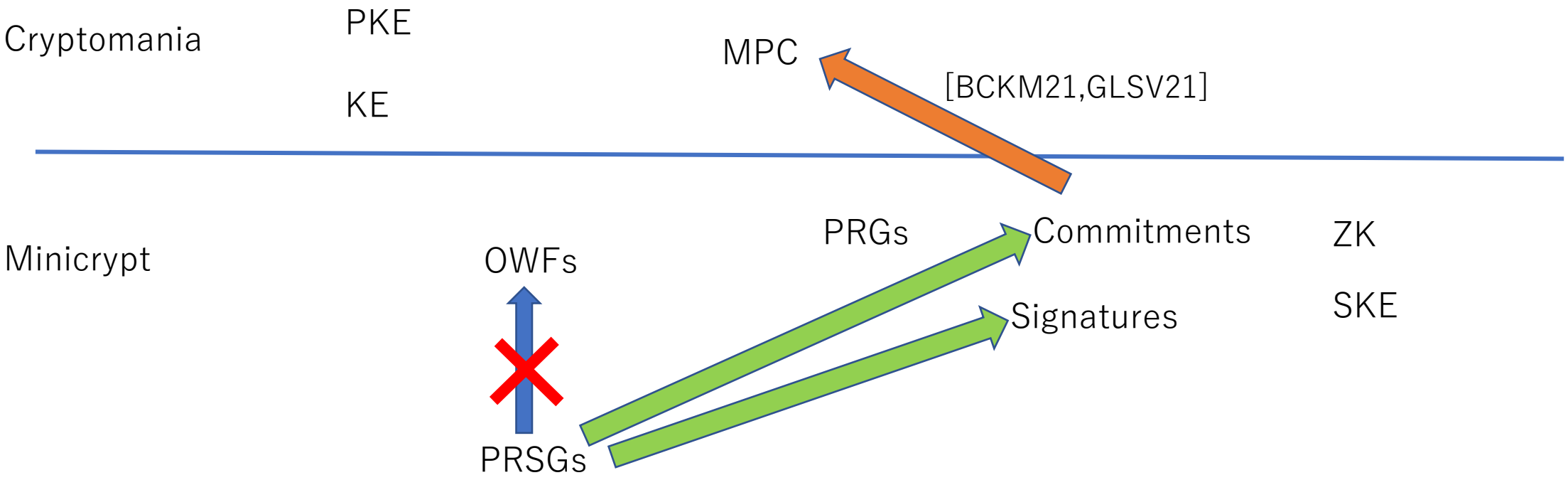
18

NO !

M and Yamakawa, CRYPTO2022
Ananth, Qian, Yuen, CRYPTO2022
Kretschmer, TQC2021

Results [M and Yamakawa, CRYPTO2022]

We construct Commitments and (q-time-secure) signatures from PRSGs



PRSGs exist even if BQP=QMA (relative to a Q oracle) [Kretschmer TQC2021]

→PRSGs exist even if OWFs do not exist

→Many cryptographic primitives exist even if OWFs do not exist

PRSGs [Ji, Liu, Song, CRYPTO2018]

Quantum analogue of PRGs

$StateGen(k) \to \phi_k$: QPT algorithm

n bit　　m qubit

$b = 0$　　$k \leftarrow \{0,1\}^n$　　$\phi_k^{\otimes t}$

$b = 1$　　$|\psi\rangle^{\otimes t} \leftarrow \mu$

For any QPT A and poly t,

$$\Pr[b \leftarrow A] \leq \frac{1}{2} + negl$$

For special case t=1, we call it 1-PRSGs

$E_\mu |\psi\rangle\langle\psi| = I^{\otimes m}/2^m$

JLS constructed PRSGs from OWFs

PRSGs → Private-key quantum money [JLS18]

$k \leftarrow \{0,1\}^n$

$\$_k \leftarrow Mint(k)$

QPT

$\$_k^{\otimes t}$

ρ

$\Pr[count\ (k, \rho) \geq t + 1\ ] \leq negl$

PRSGs → Pseudo entanglement

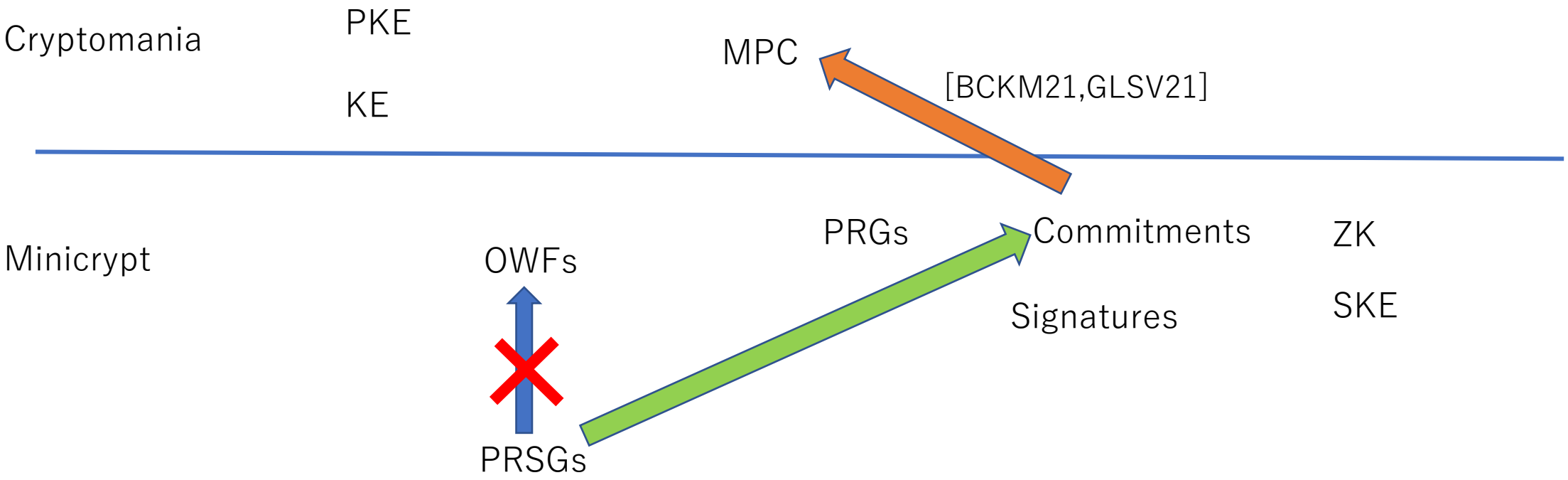
$m \gg n$

$$Q_0|0 \dots 0\rangle_{C,R} = \sum_{k\in\{0,1\}^n} |k\rangle_R \otimes |\phi_k\rangle_C$$ EE=n Pseudo EE=m

$$Q_1|0 \dots 0\rangle_{C,R} = \sum_{z\in\{0,1\}^m} |z\rangle_R \otimes |z\rangle_C$$ EE=m

Results [M and Yamakawa, CRYPTO2022]

We construct Commitments and (q-time-secure) signatures from PRSGs



1-PRSG→ comp-hiding stat-binding Commitments

Canonical form [YWLQ15]

$$Q_0|0\dots0\rangle_{C,R} = \sum_{k\in\{0,1\}^n} |k\rangle_R \otimes |\phi_k\rangle_C$$

$$Q_1|0\dots0\rangle_{C,R} = \sum_{z\in\{0,1\}^m} |z\rangle_R \otimes |z\rangle_C$$

b, R

$Q_{b|0\dots0\rangle_{C,R}}$?

Comp Hiding: $Tr_R(Q_0|0\rangle_{C,R}) \sim_c Tr_R(Q_1|0\rangle_{C,R})$

Stat Binding: $||Tr_R(Q_0|0\rangle_{C,R}) - Tr_R(Q_1|0\rangle_{C,R})|| \sim 1$

From the flavor conversion theorem [Yan20, Hahn-Morimae-Yamakawa22], we also get stat-hiding comp-binding commitments

Results [M and Yamakawa, CRYPTO2022]

We construct Commitments and (q-time-secure) signatures from PRSGs

Cryptomania

PKE

KE

MPC

Minicrypt

OWFs

PRSGs

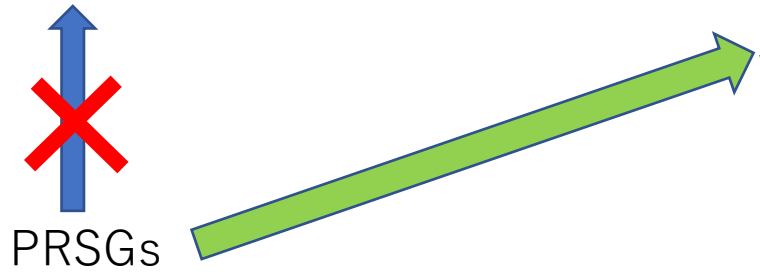
PRGs

Commitments

Signatures

ZK

SKE



One-time secure signature from OWFs

sk

(k_0, k_1)

pk

$f(k_0), f(k_1)$

$k_0 \leftarrow Sign(0, sk)$

$k_1 \leftarrow Sign(1, sk)$

$Ver(\sigma, pk, b): f(\sigma) = f(k_b)?$

OWSGs

Quantum analogue of OWFs

$StateGen(k) \to \phi_k$: QPT algorithm

n bit　m qubit

$k \leftarrow \{0,1\}^n$

$\phi_k^{\otimes t}$

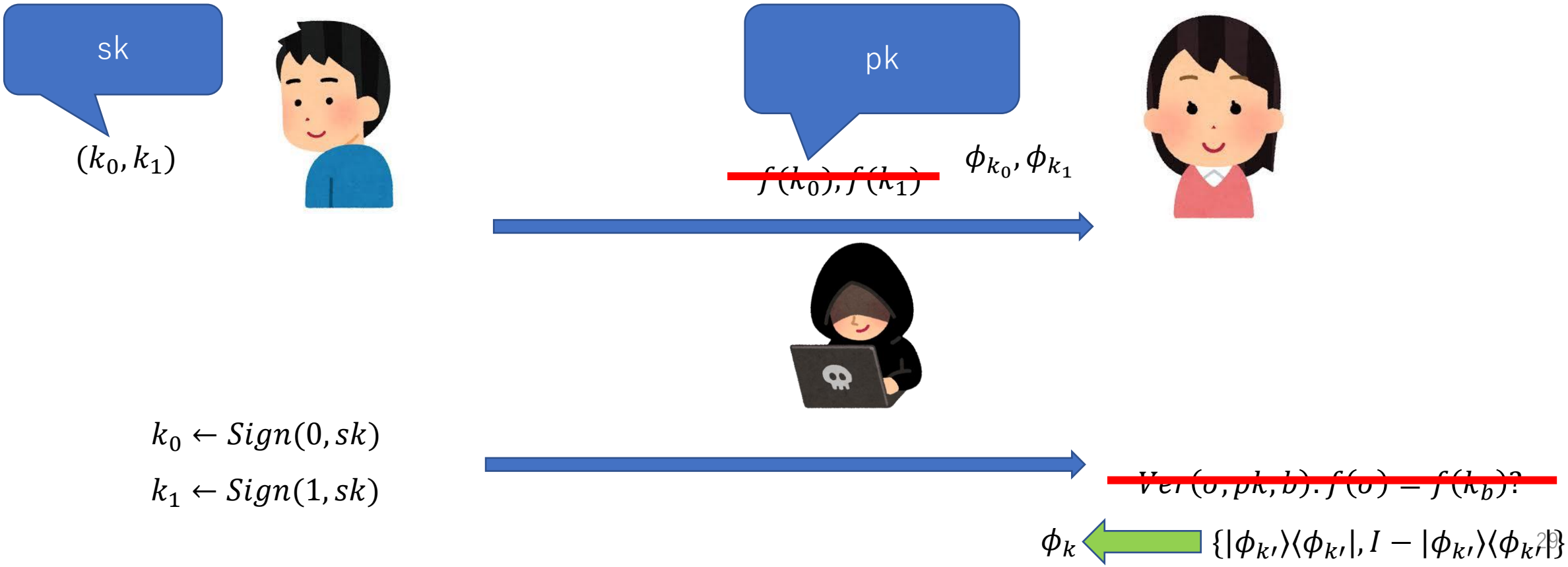
k'

ϕ_k $\{|\phi_{k'}\rangle\langle\phi_{k'}|, I - |\phi_{k'}\rangle\langle\phi_{k'}|\}$

$\Pr[C \to \mathsf{T}] \leq negl$

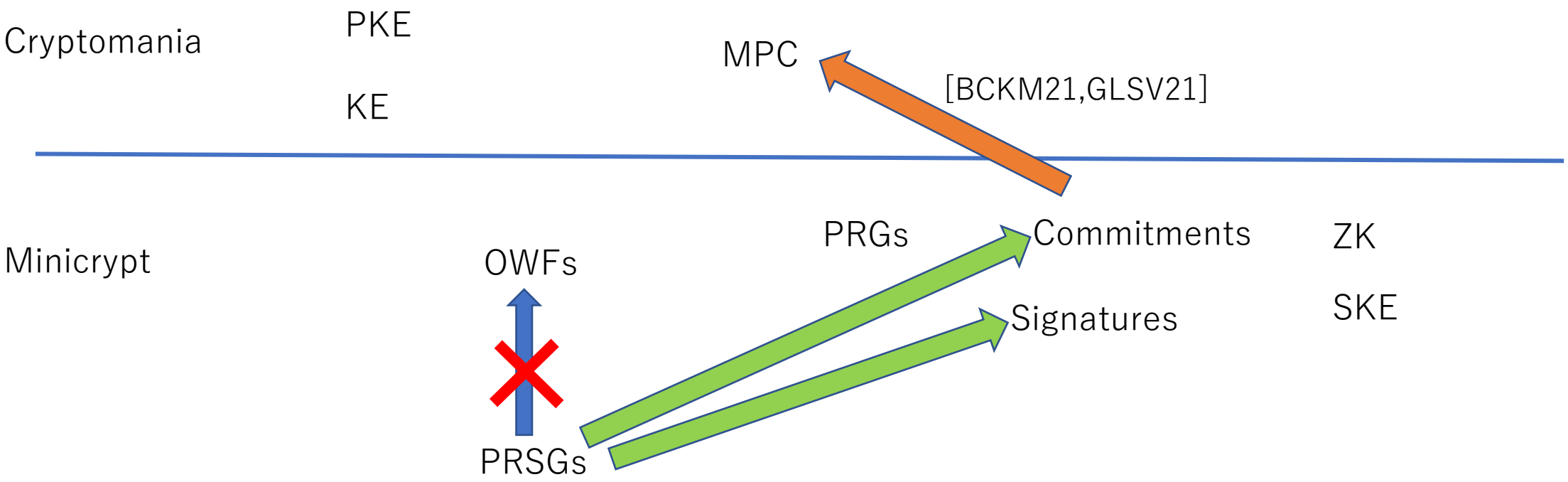
We construct OWSGs from PRSGs

OWSGs→One-time secure signatures



One-time can be made q-time [M and Yamakawa, arXiv: 2210.03394]
→open problem: many-time signatures?

Summary [M and Yamakawa, CRYPTO2022]



(1) We construct commitments (and MPC) from PRSGs

(2) We construct digital signatures from PRSGs

(3) PRSGs can exist even if OWFs do not exist. [Kretschmer TQC2021]

Open problem: What is the most fundamental element in quantum cryptography?

Brakerski, Canetti, Qian introduced EFI (Yan also implicitly introduced it)

$StateGen(1^\lambda, b) \to \rho_b$: QPT algorithm

(1) Statistically distinguishable: $||\rho_0 - \rho_1||_1 \geq 1/poly(\lambda)$

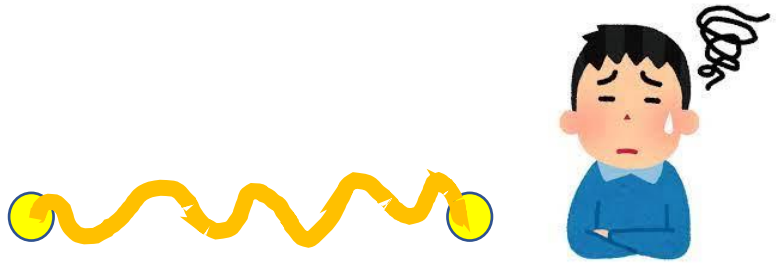
(2) Computationally indistinguishable: For any QPT A,

$$|\Pr[1 \leftarrow A(\rho_0)] - \Pr[1 \leftarrow A(\rho_1)| \leq negl(\lambda)$$

Its classical version is equivalent to OWFs [Goldreich 90]

BCQ showed that EFI is equivalent to commitment, OT, ZK, etc.
→open problem: EFI is the most fundamental element in Q cryptography?

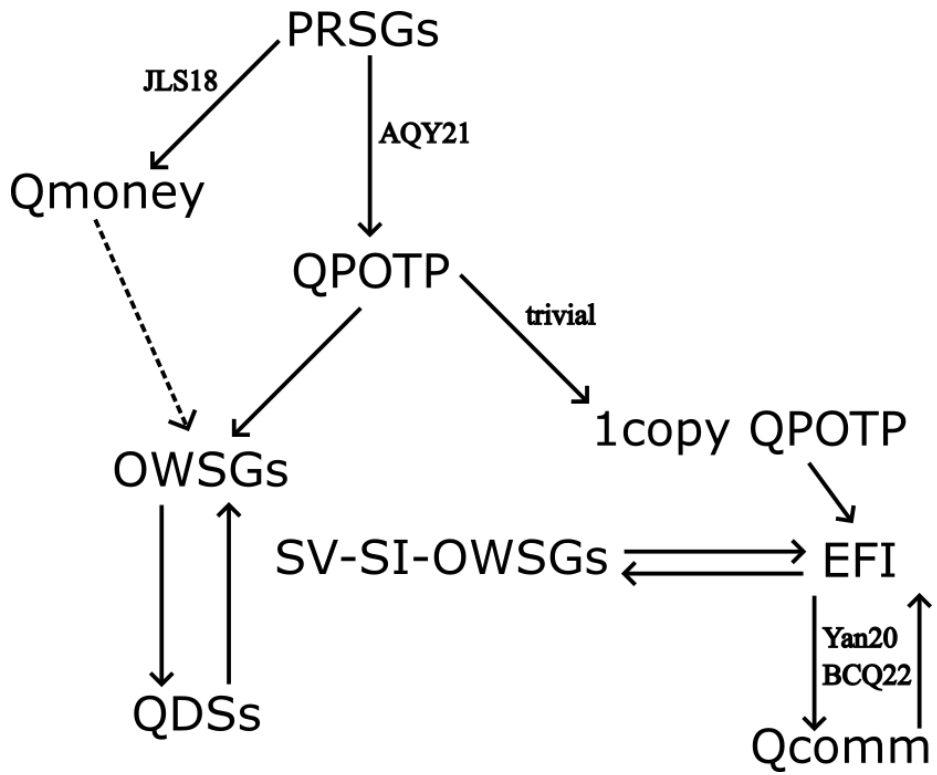
Black-hole from Q crypto?



To explain a black-hole paradox, a ``hidden" entanglement that can be extracted in principle, but hard to extract is required.

Hayden-Harlow: such hidden entanglement exists if SZK $\neq$ BQP
Aaronson: such hidden entanglement exists if OWPs exist

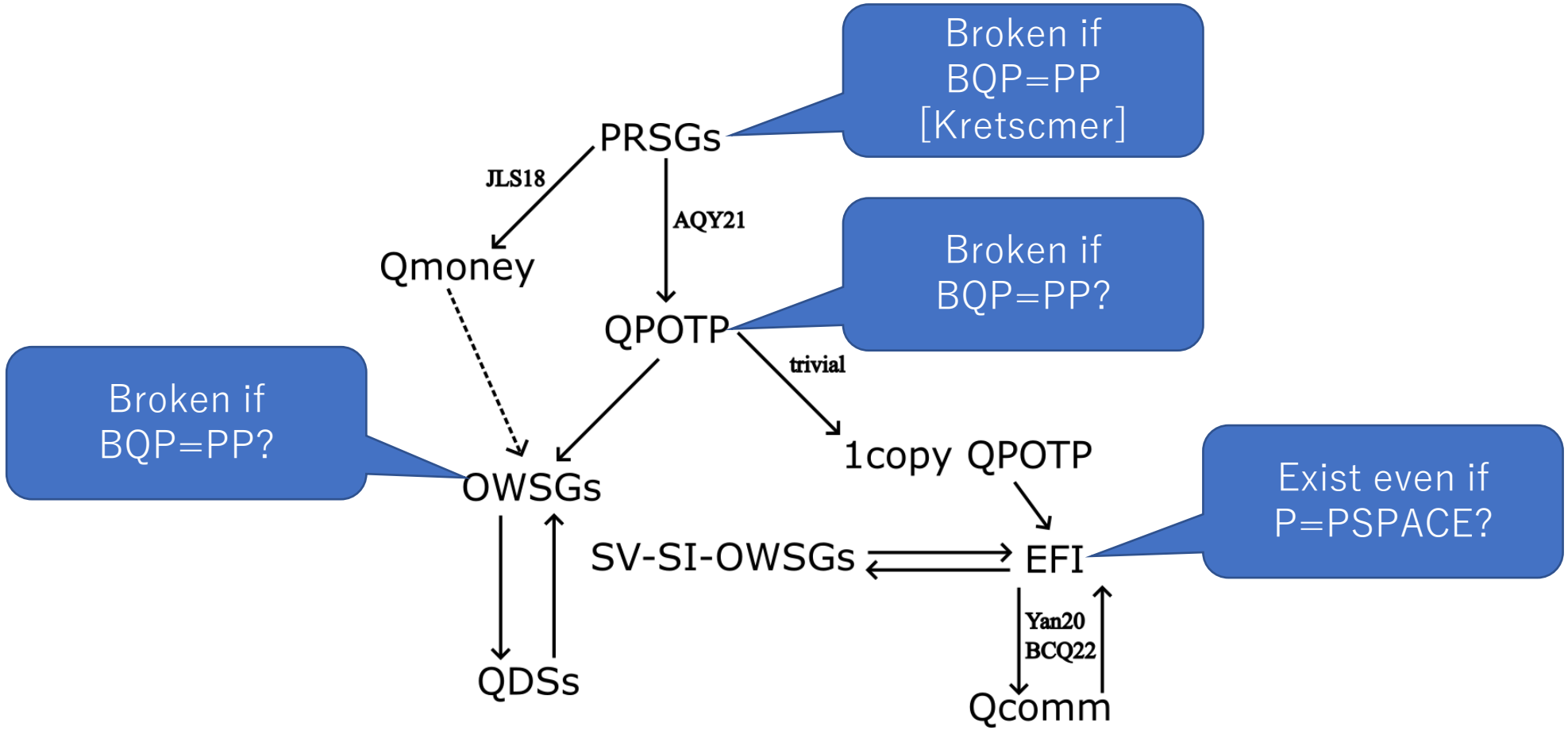
[Brakerski, arXiv: 2211.05491] such hidden entanglement exists if EFI exist



M and Yamakawa, arXiv:2210.03394

Open problem:
OWSG=EFI?
Any other primitives? Other relations?

Open problem: which complexity assumptions necessary?



PRSGs are broken if BQP=QCMA?

$StateGen(k) \to \phi_k$: QPT algorithm

n bit　m qubit

$b = 0$　$k \leftarrow \{0,1\}^n$　$\phi_k^{\otimes t}$

$b = 1$　$|\psi\rangle^{\otimes t} \leftarrow \mu$

k^*

QCMA oracle

$\rho = StateGen(k^*)$?

This does not work, because QCMA oracle takes classical inputs

In fact, Kretschmer showed PRSGs exist even if BQP=QMA

Shadow tomography

[Aaronson, STOC2018]
[Huang, Kueng, Preskill, Nature Physics, 2020]

$\rho^{\otimes t}$

For each copy,

$U_j \leftarrow C$

Measure $U_j \rho U_j^+$

$\{U_j, b_j\}_{j=1}^t$

Quantum poly(t) time

$For\ any\ set\ of\ operators\ \{O_k\}_{k=1}^M$

Alice can compute $\{\eta_k\}_{k=1}^M$ such that

$$|\eta_k - Tr(\rho O_k)| \leq \frac{1}{poly(t)}$$

Classical exp(t) time

$t = O(\log M)!$

PRSGs are broken if BQP=PP

$b = 0$ $\quad k \leftarrow \{0,1\}^n \quad \phi_k^{\otimes t}$

$b = 1 \quad |\psi\rangle^{\otimes t} \leftarrow \mu$

For each copy,

$U_j \leftarrow C$

Measure $U_j \rho U_j^+$

$\{U_j, b_j\}_{j=1}^t$

Quantum poly(t) time

Alice can compute $\{\eta_k\}_{k=1}^M$ such that

$$|\eta_k - Tr(\rho|\phi_k\rangle\langle\phi_k|)| \leq \frac{1}{poly(t)}$$

Classical exp(t) time

$b = 0: \exists k\ s.t.\ \eta_k \sim 1$

$b = 1: \forall k, \quad \eta_k \sim 0$

PRSGs are broken if BQP=PP

[Kretschmer TQC2021]

$b = 0$ $k \leftarrow \{0,1\}^n$ $\phi_k^{\otimes t}$

$b = 1$ $|\psi\rangle^{\otimes t} \leftarrow \mu$

For each copy,

$U_j \leftarrow C$

Measure $U_j \rho U_j^+$

$\{U_j, b_j\}_{j=1}^t$

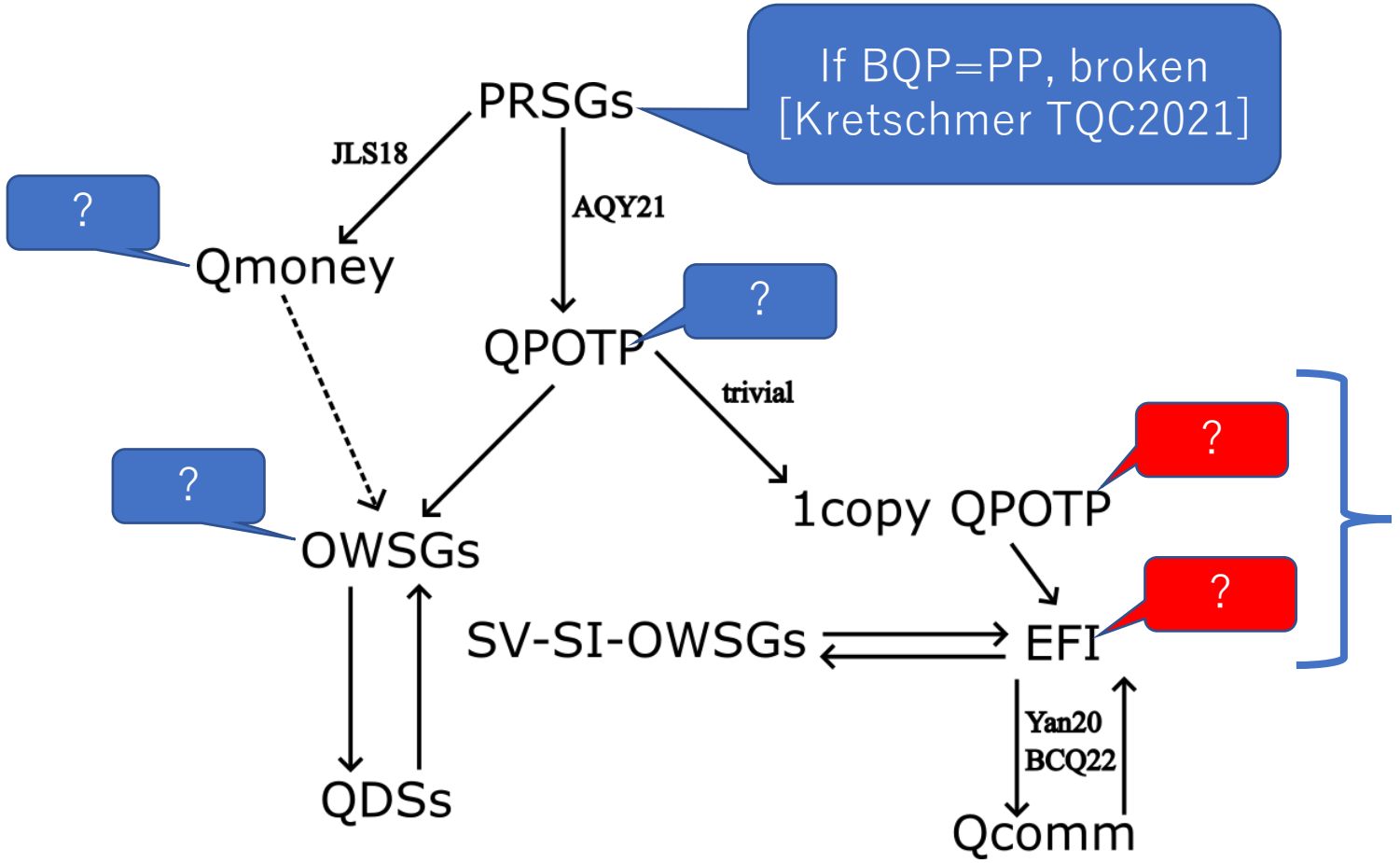
Quantum poly(t) time

$$|0\rangle\langle 0| \otimes \sum_k \phi_k^{\otimes t} + |1\rangle\langle 1| \otimes E_\mu[|\psi\rangle\langle\psi|]$$

Postselect this!

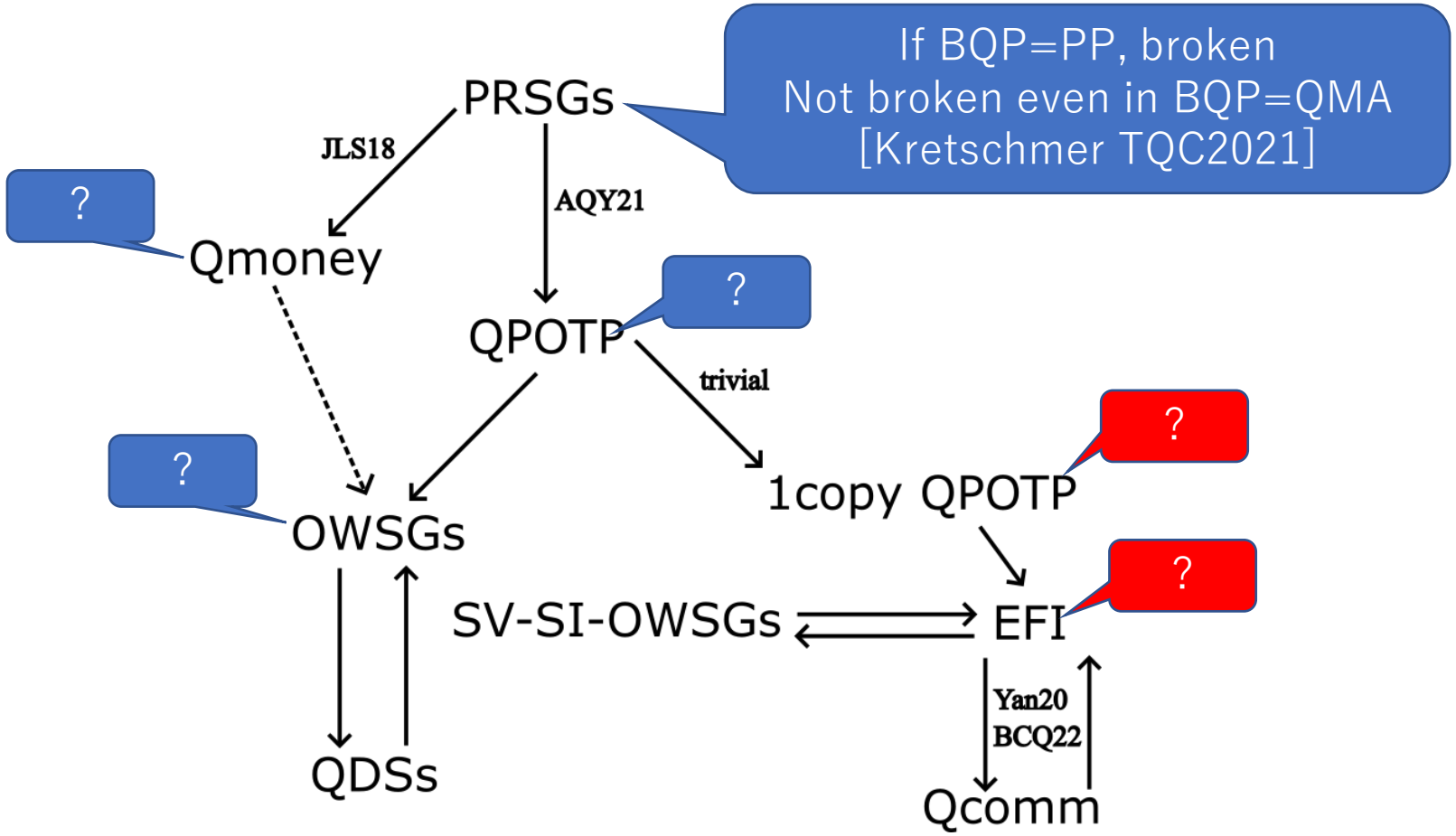
postBQP=PP

Open problems: what is necessary classical complexity assumption?

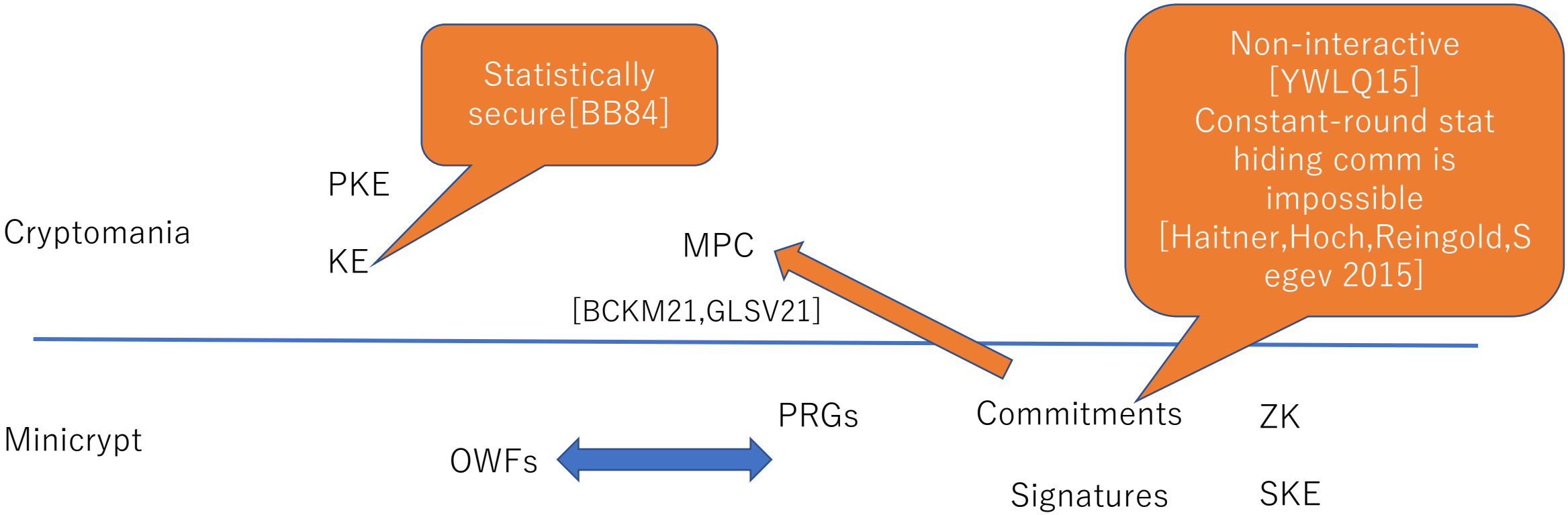


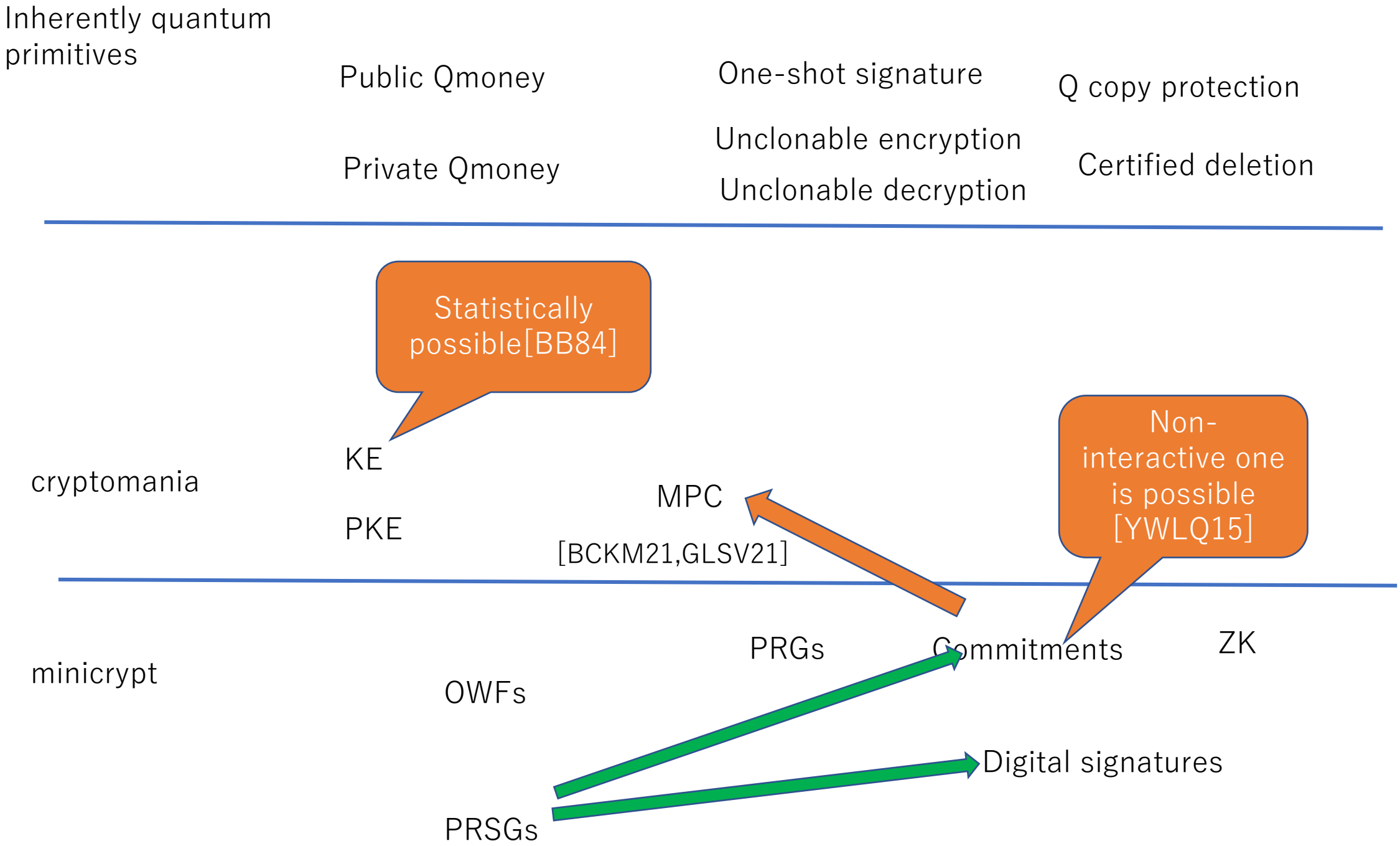
Shadow tomography cannot be used!

Necessary classical complexity assumption



``Quantum advantage" in crypto




Inherently quantum primitives
Public Qmoney
Private Qmoney
One-shot signature
Unclonable encryption
Unclonable decryption
Q copy protection
Certified deletion
Statistically possible[BB84]
cryptomania
KE
PKE
MPC
[BCKM21,GLSV21]
Non-interactive one is possible [YWLQ15]
minicrypt
PRGs
Commitments
ZK
OWFs
Digital signatures
PRSGs

PRSGs→Commitment

$$Q_0|0\rangle_{C,R} = \sum_k |k\rangle_R \otimes |\phi_k\rangle_C$$

$$Q_1|0\rangle_{C,R} = \sum_k |k\rangle_R \otimes |k\rangle_C$$

Comp hiding:

Comp hiding:

$$F\left(\sum_k |\phi_k\rangle\left\langle\phi_k\right|, \frac{I}{2^m}\right) \leq negl$$