Secure Quantum Computation over Classical Networks

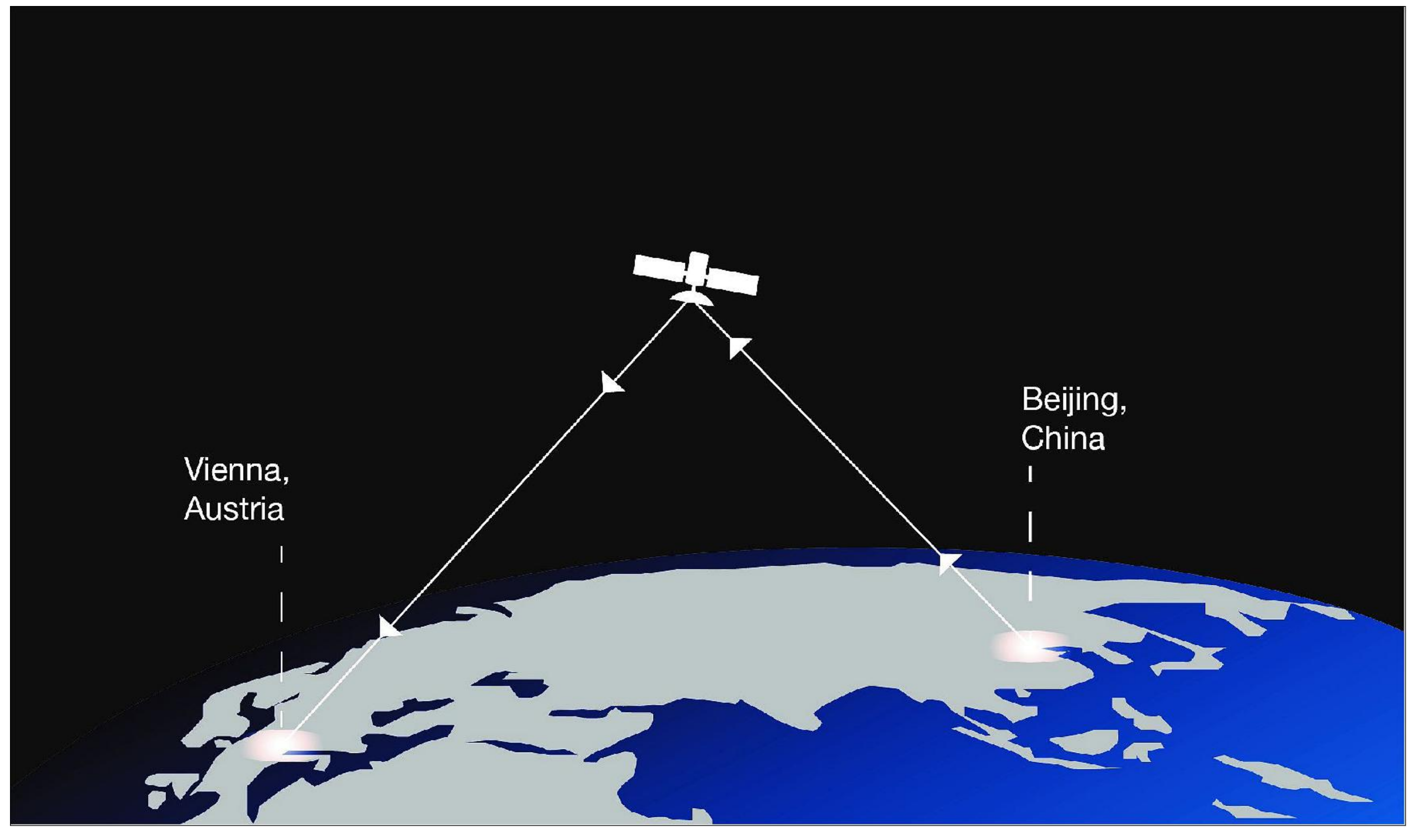
Atul Mantri | February 15th, 2021

The Joint Center for Quantum Information and Computer Science
(QuICS)
University of Maryland

Quantum Wave of Computing

Classical devices cannot efficiently simulate quantum systems!

Important Milestones!



Secure Communication over 7600km (2017)

Entanglement-based secure quantum cryptography over 1,120 kilometres

Article

Quantum supremacy using a programmable superconducting processor

https://doi.org/10.1038/s41586-019-1666-5
Received: 22 July 2019
Accepted: 20 September 2019
Published online: 23 October 2019

Frank Arute[1], Kunal Arya[1], Ryan Babbush[1], Dave Bacon[1], Joseph C. Bardin[1,2], Rami Barends[1], Rupak Biswas[3], Sergio Boixo[1], Fernando G. S. L. Brandao[1,4], David A. Buell[1], Brian Burkett[1], Yu Chen[1], Zijun Chen[1], Ben Chiaro[5], Roberto Collins[1], William Courtney[1], Andrew Dunsworth[1], Edward Farhi[1], Brooks Foxen[1,5], Austin Fowler[1], Craig Gidney[1], Marissa Giustina[1], Rob Graff[1], Keith Guerin[1], Steve Habegger[1], Matthew P. Harrigan[1], Michael J. Hartmann[1,6], Alan Ho[1], Markus Hoffmann[1], Trent Huang[1], Travis S. Humble[7], Sergei V. Isakov[1], Evan Jeffrey[1], Zhang Jiang[1], Dvir Kafri[1], Kostyantyn Kechedzhi[1], Julian Kelly[1], Paul V. Klimov[1], Sergey Knysh[1], Alexander Korotkov[1,8], Fedor Kostritsa[1], David Landhuis[1], Mike Lindmark[1], Erik Lucero[1], Dmitry Lyakh[9], Salvatore Mandrà[3,10], Jarrod R. McClean[1], Matthew McEwen[5], Anthony Megrant[1], Xiao Mi[1], Kristel Michielsen[11,12], Masoud Mohseni[1], Josh Mutus[1], Ofer Naaman[1], Matthew Neeley[1], Charles Neill[1], Murphy Yuezhen Niu[1], Eric Ostby[1], Andre Petukhov[1], John C. Platt[1], Chris Quintana[1], Eleanor G. Rieffel[3], Pedram Roushan[1], Nicholas C. Rubin[1], Daniel Sank[1], Kevin J. Satzinger[1], Vadim Smelyanskiy[1], Kevin J. Sung[1,13], Matthew D. Trevithick[1], Amit Vainsencher[1], Benjamin Villalonga[1,14], Theodore White[1], Z. Jamie Yao[1], Ping Yeh[1], Adam Zalcman[1], Hartmut Neven[1] & John M. Martinis[1,5*]

The promise of quantum computers is that certain computational tasks might be executed exponentially faster on a quantum processor than on a classical processor[1]. A fundamental challenge is to build a high-fidelity processor capable of running quantum algorithms in an exponentially large computational space. Here we report the use of a processor with programmable superconducting qubits[2–7] to create quantum states on 53 qubits, corresponding to a computational state-space of dimension 2^{53} (about 10^{16}). Measurements from repeated experiments sample the resulting probability distribution, which we verify using classical simulations. Our Sycamore processor takes about 200 seconds to sample one instance of a quantum circuit a million times—our benchmarks currently indicate that the equivalent task for a state-of-the-art classical supercomputer would take approximately 10,000 years. This dramatic increase in speed compared to all known classical algorithms is an experimental realization of quantum supremacy[8–14] for this specific computational task, heralding a much-anticipated computing paradigm.

Google (2019)

QUANTUM COMPUTING

Quantum computational advantage using photons

Han-Sen Zhong[1,2*], Hui Wang[1,2*], Yu-Hao Deng[1,2*], Ming-Cheng Chen[1,2*], Li-Chao Peng[1,2], Yi-Han Luo[1,2], Jian Qin[1,2], Dian Wu[1,2], Xing Ding[1,2], Yi Hu[1,2], Peng Hu[3], Xiao-Yan Yang[3], Wei-Jun Zhang[3], Hao Li[3], Yuxuan Li[4], Xiao Jiang[1,2], Lin Gan[4], Guangwen Yang[4], Lixing You[3], Zhen Wang[3], Li Li[1,2], Nai-Le Liu[1,2], Chao-Yang Lu[1,2†], Jian-Wei Pan[1,2†]

Quantum computers promise to perform certain tasks that are believed to be intractable to classical computers. Boson sampling is such a task and is considered a strong candidate to demonstrate the quantum computational advantage. We performed Gaussian boson sampling by sending 50 indistinguishable single-mode squeezed states into a 100-mode ultralow-loss interferometer with full connectivity and random matrix—the whole optical setup is phase-locked—and sampling the output using 100 high-efficiency single-photon detectors. The obtained samples were validated against plausible hypotheses exploiting thermal states, distinguishable photons, and uniform distribution. The photonic quantum computer, *Jiuzhang*, generates up to 76 output photon clicks, which yields an output state-space dimension of 10^{30} and a sampling rate that is faster than using the state-of-the-art simulation strategy and supercomputers by a factor of ~10^{14}.

USTC, China (2020)

Building quantum computers is very hard but not impossible!

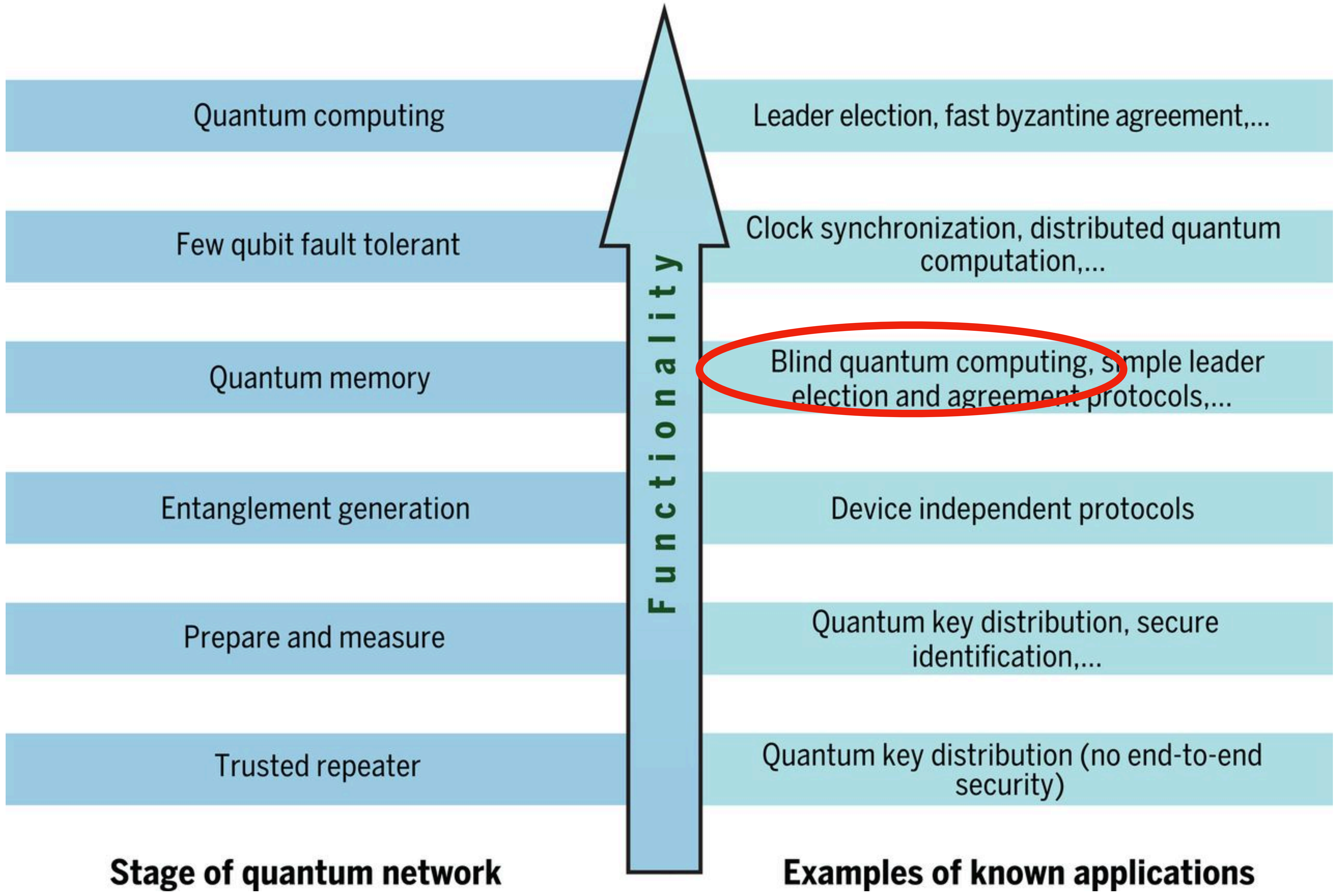
Hardware is working, what's next..?

Towards a Quantum Internet

Future of Internet

Quantum Internet promises to provide radically new internet technologies.

Some maybe not possible to accomplish on the modern internet.



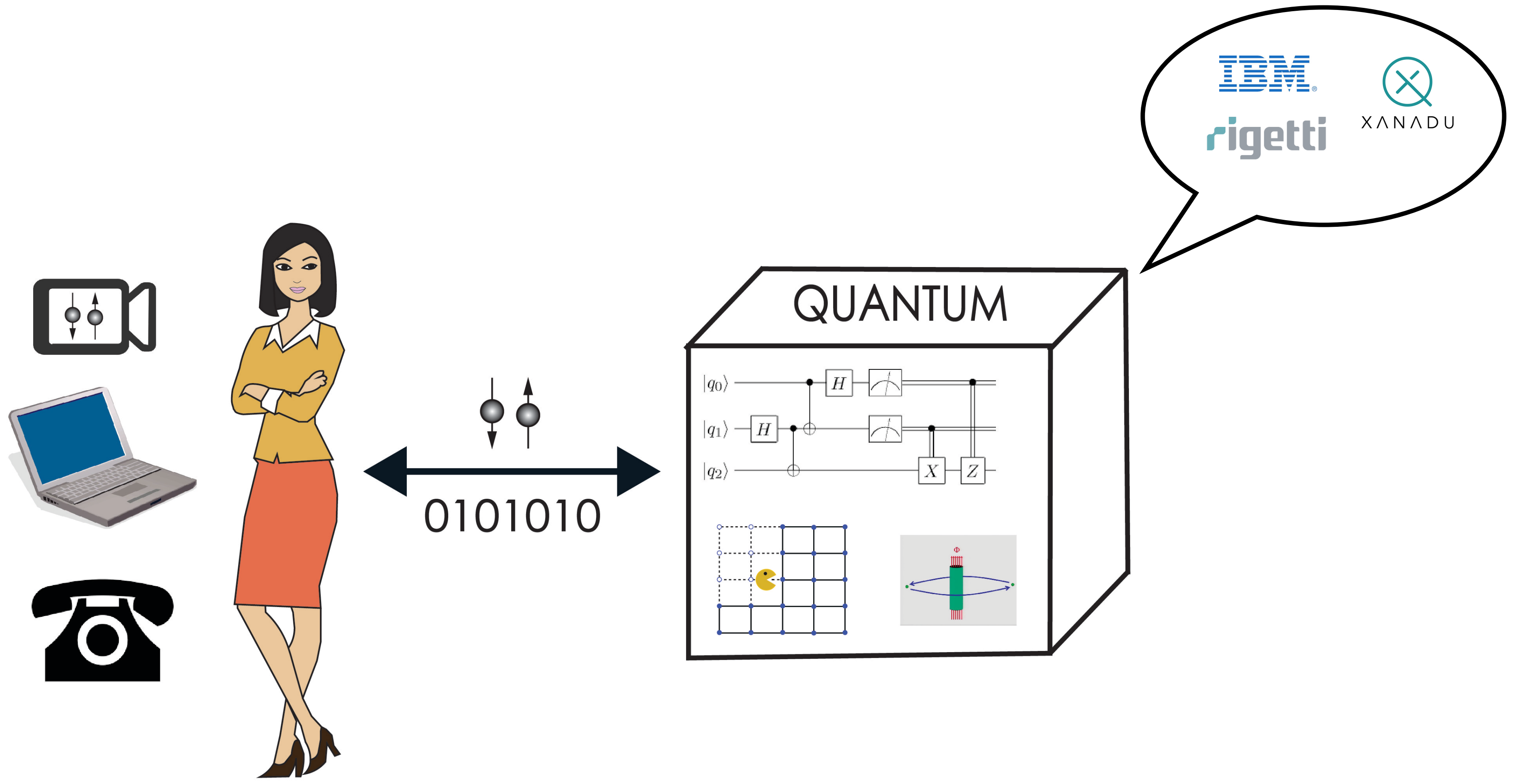
Wehner, S., Elkouss, D., & Hanson, R. (2018). Quantum internet: A vision for the road ahead. Science, 362(6412).

A more realistic setting is where both quantum and classical channel co-exists!

Secure Cloud Quantum Computing

Client

- Has limited computational resources.
- Wants to use quantum computer.
- Doesn’t want to reveal the data.
- Problems may involve confidential data or be commercially sensitive.

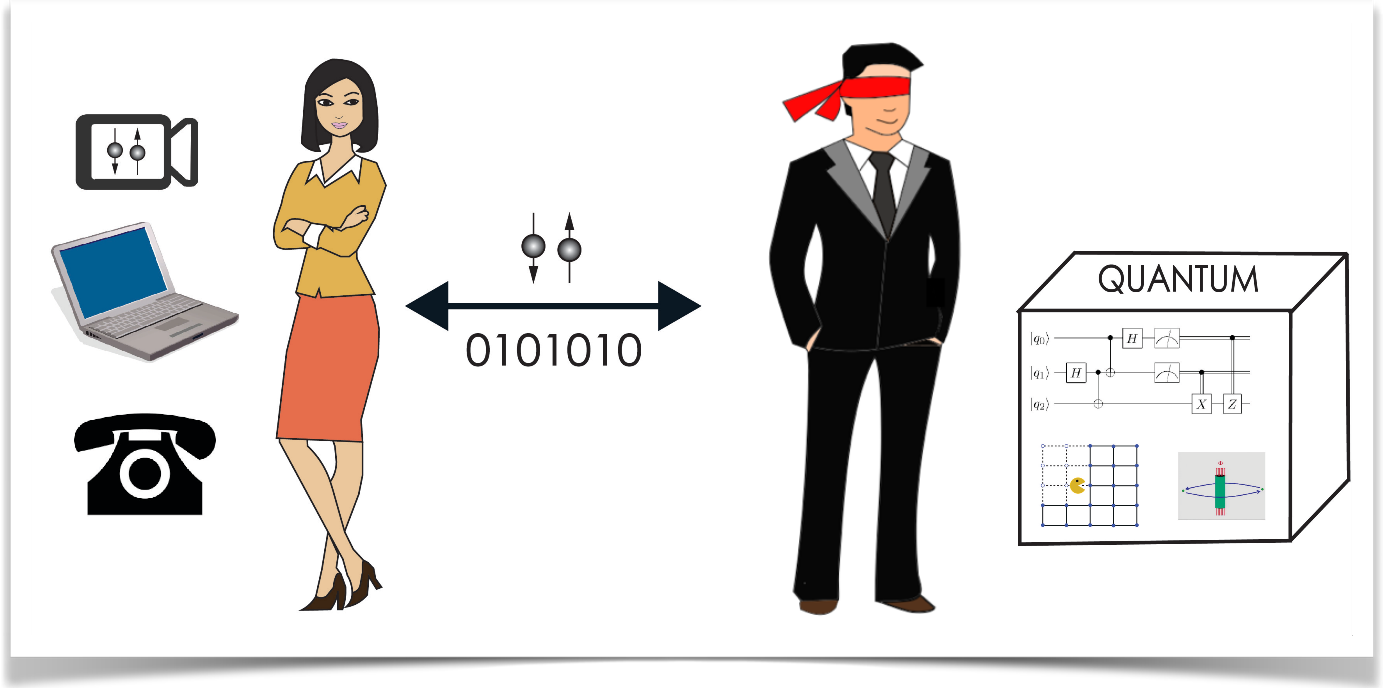


Server

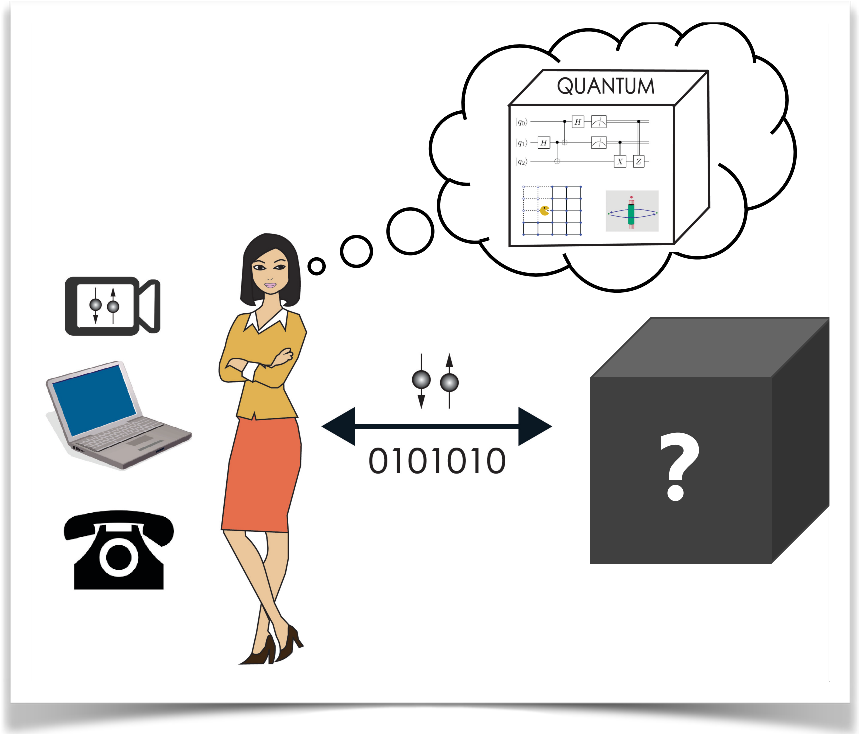
- Has a full quantum computer.
- Willing to help and provide cloud-based services.
- Cannot be trusted.

Blindness

privacy of client’s computation is preserved.



Verification



Integrity of the desired computation is maintained

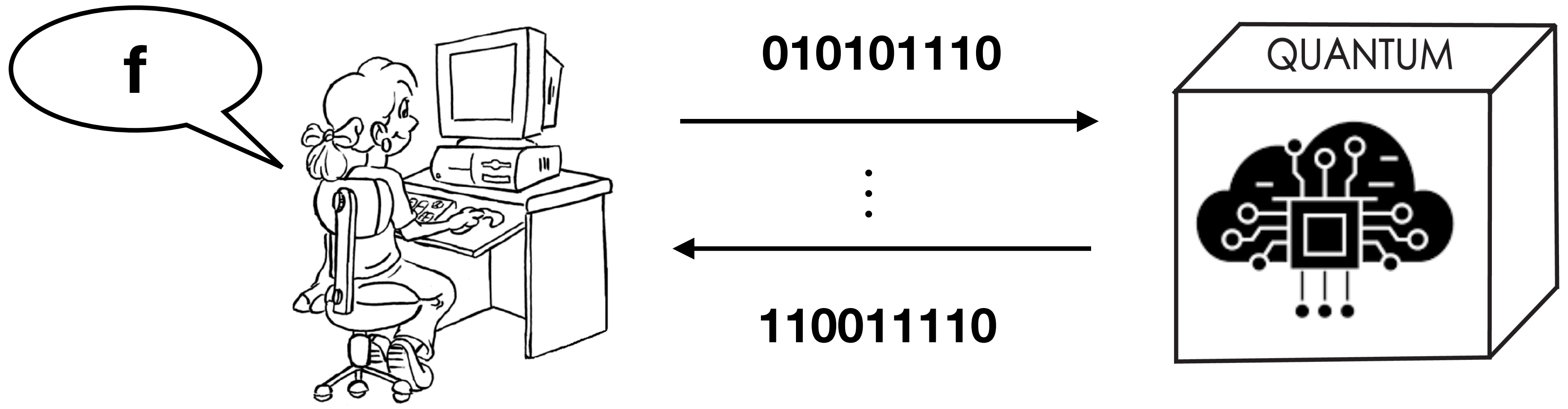
Requirements

Round Complexity

Minimum resources

Verification

Design



Class of Computations

Security

Information-theoretic vs computational

Standalone vs Composable

<u>Information-theoretic</u> — Against Unbounded Adversaries (Ideal)

<u>Computational</u> — Against Computationally-Bounded Adversaries (say, Quantum poly-time adversaries)

Classical User - Classical Server
Abadi, Feigenbaum and Kilian (1987)

computing NP-hard function securely

↓

Unlikely consequences in complexity theory*

*polynomial hierarchy collapses at the third level

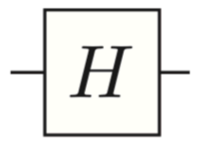
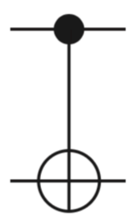
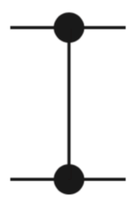
<u>functions that are harder to compute are harder to encrypt…</u>

Fully homomorphic encryption (FHE) schemes!

Quantum functions?

Classical vs Quantum Computing

Bits	Qubits
AND/OR/NOT Gates	Unitary Quantum Gates
Reading the output bit	Measuring: final state -> classical output

	Name	Matrix	Circuit Element
Single qubit gates	Hadamard	$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$	
Two qubit gates - entangling gates	CNOT	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$	
	CZ	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$	

Single qubit state

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Superposition

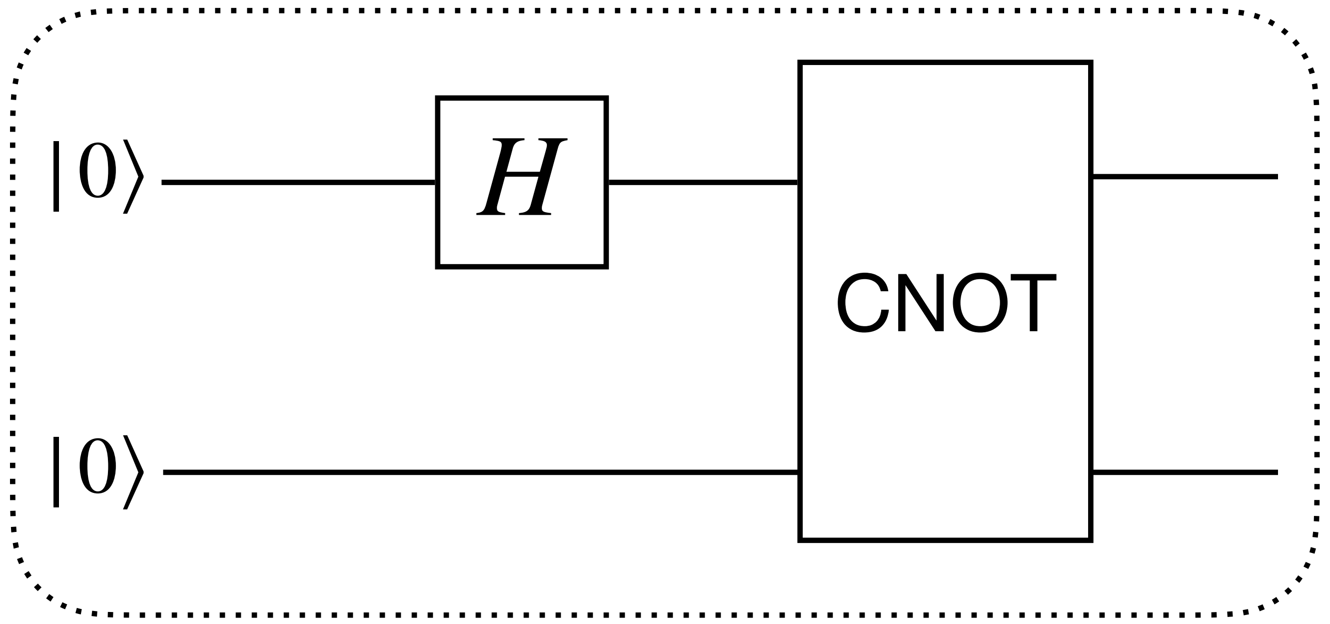
$$\alpha|0\rangle + \beta|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \qquad |\alpha|^2 + |\beta|^2 = 1$$

n-qubit state

$$|\psi\rangle = \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle \qquad \sum_{x \in \{0,1\}^n} |\alpha_x|^2 = 1$$

Example

Input state



Output state

$$|00\rangle \rightarrow \frac{|00\rangle + |10\rangle}{\sqrt{2}} \rightarrow \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

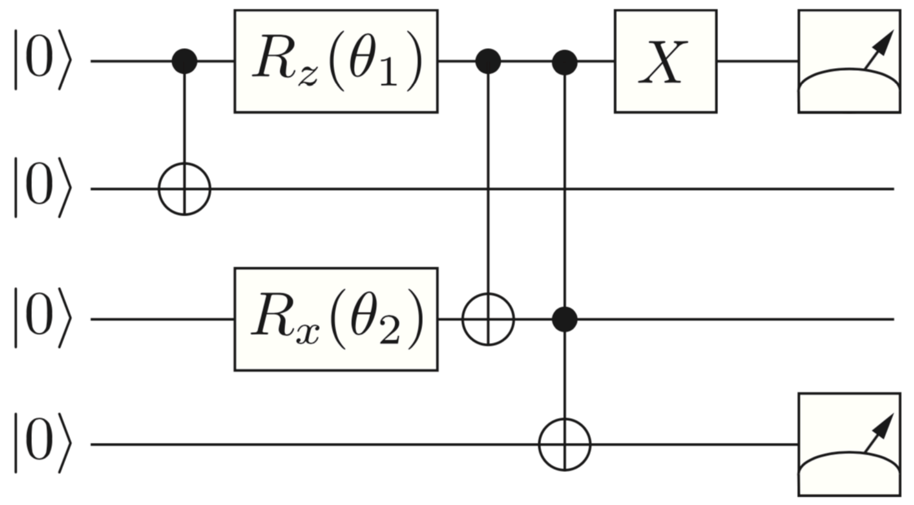
Entanglement

Models for Quantum Computing

Quantum Circuit Model

- Prepare a quantum state in the computational basis.
- Apply a sequence of unitary operations.
- Perform a measurement of one or more of the qubits.

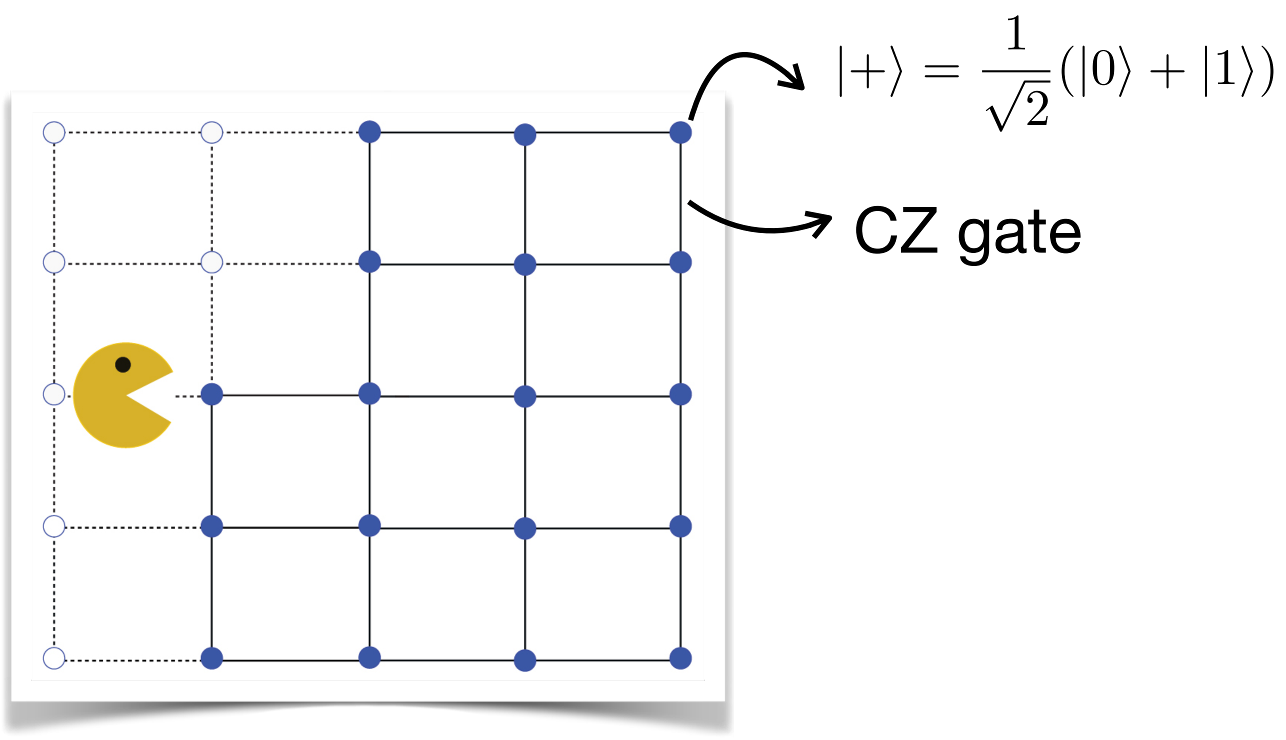
Example



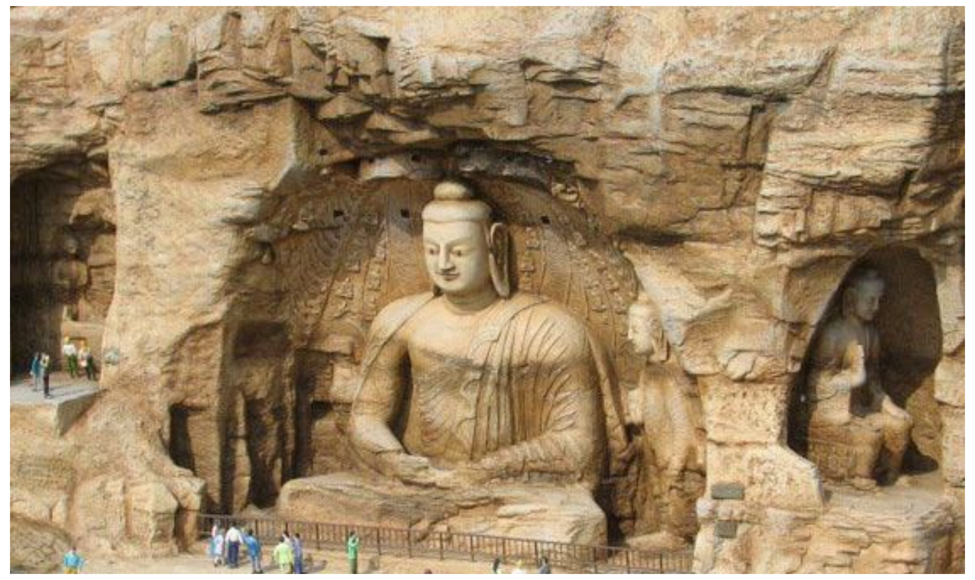
Adding stone by stone to make a sculpture

Measurement-Based Model

A computation is performed by means of single-qubit projective measurements that drive the quantum information across a highly entangled state.



single qubit measurements

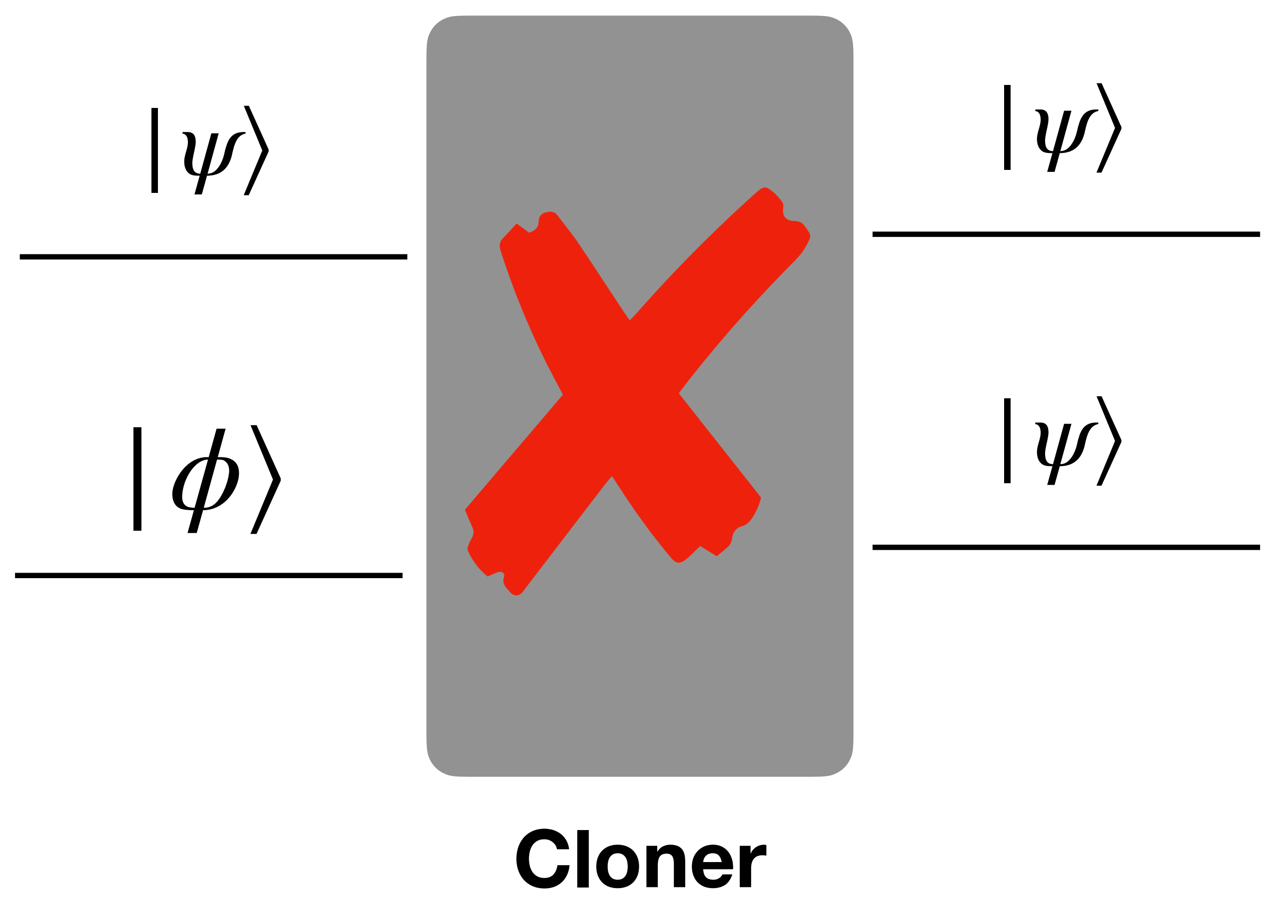


Rock cut sculpture

Highly Entangled State + (Adaptive) Measurements

Quantum No-Cloning

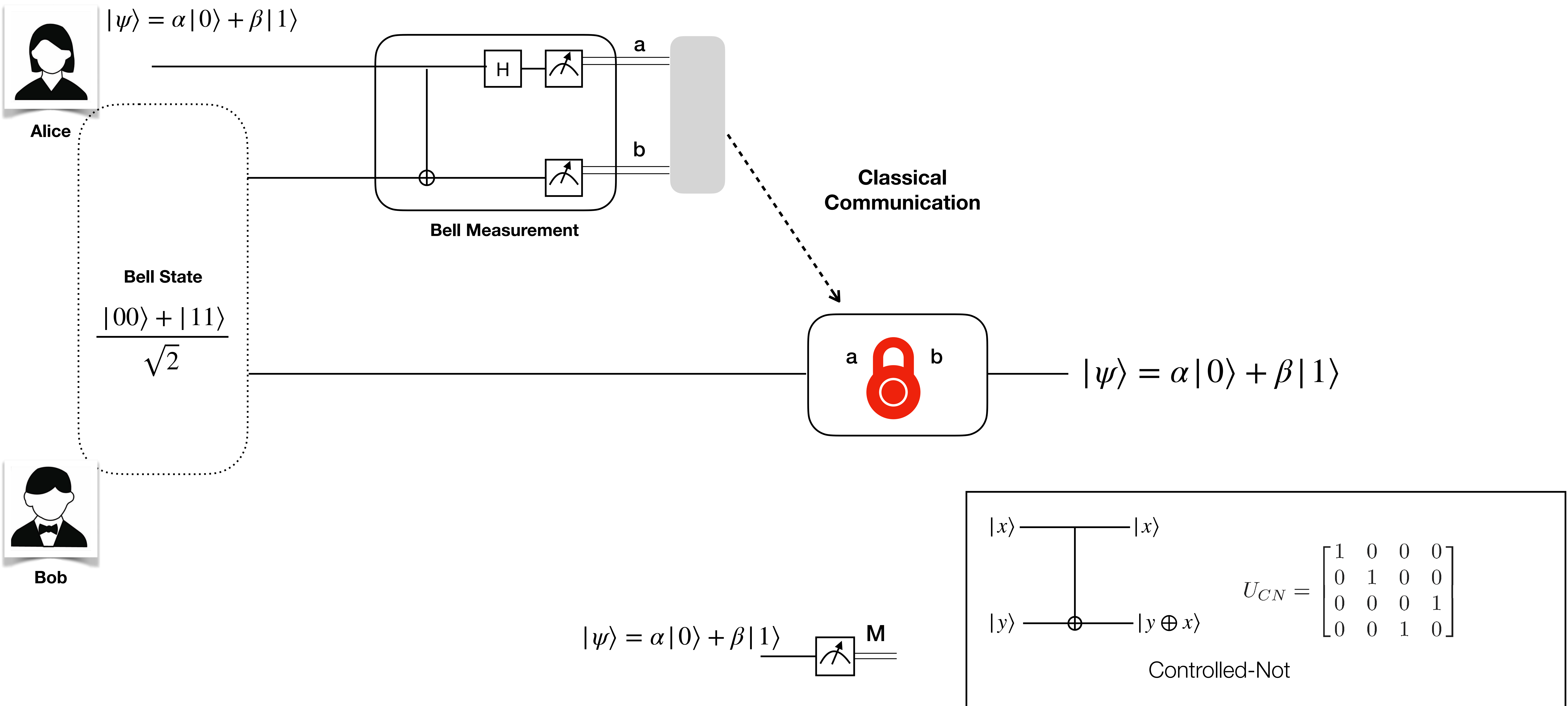
There does not exist any physical device that can output two perfectly identical copies of an unknown quantum state $|\psi\rangle$ when given a single copy of $|\psi\rangle$.



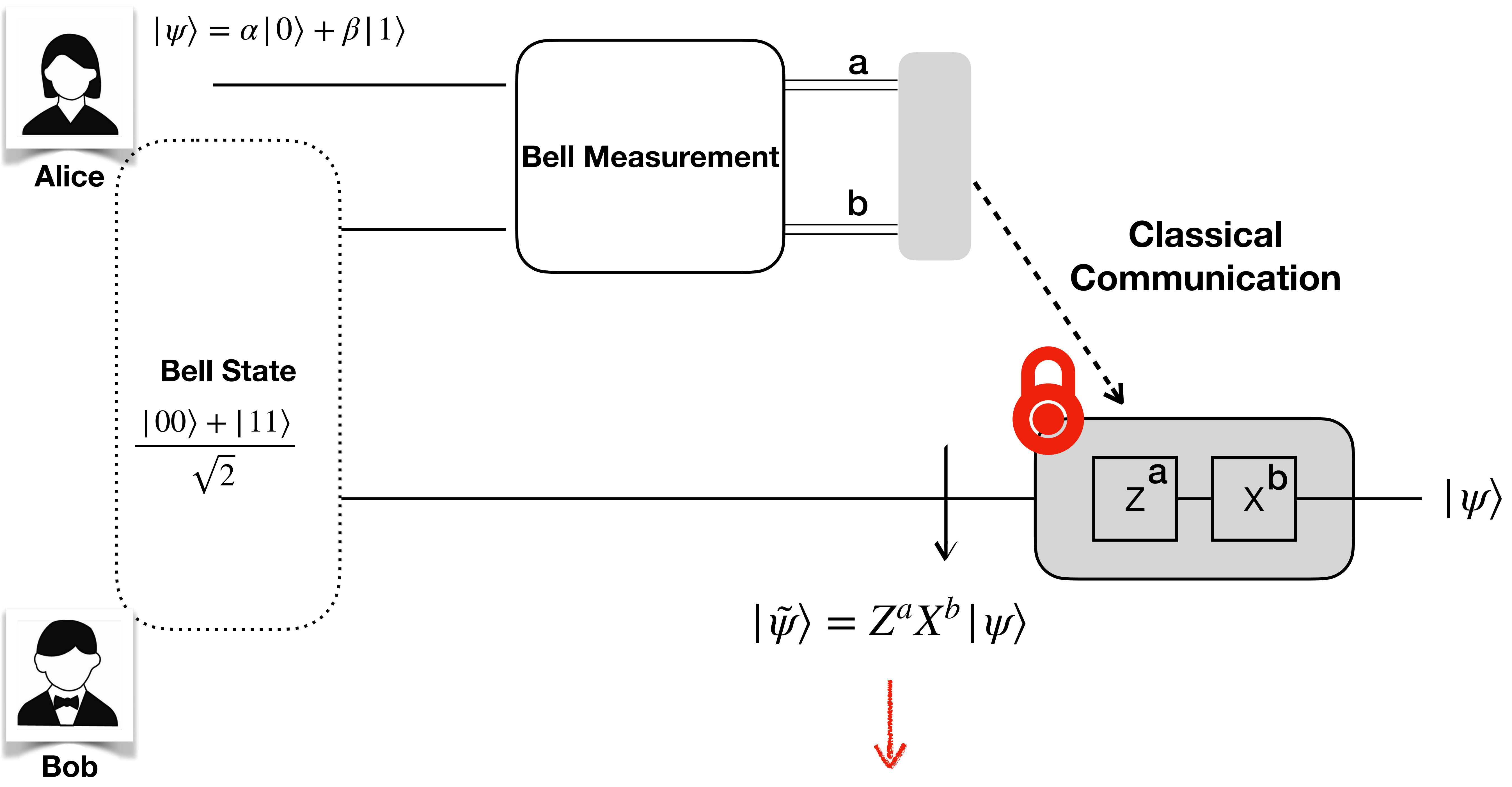
Useful in Quantum Key Distribution, Quantum Money, etc..

We will see security limitation of two-party quantum cryptographic primitives based on no-cloning theorem

Quantum Teleportation



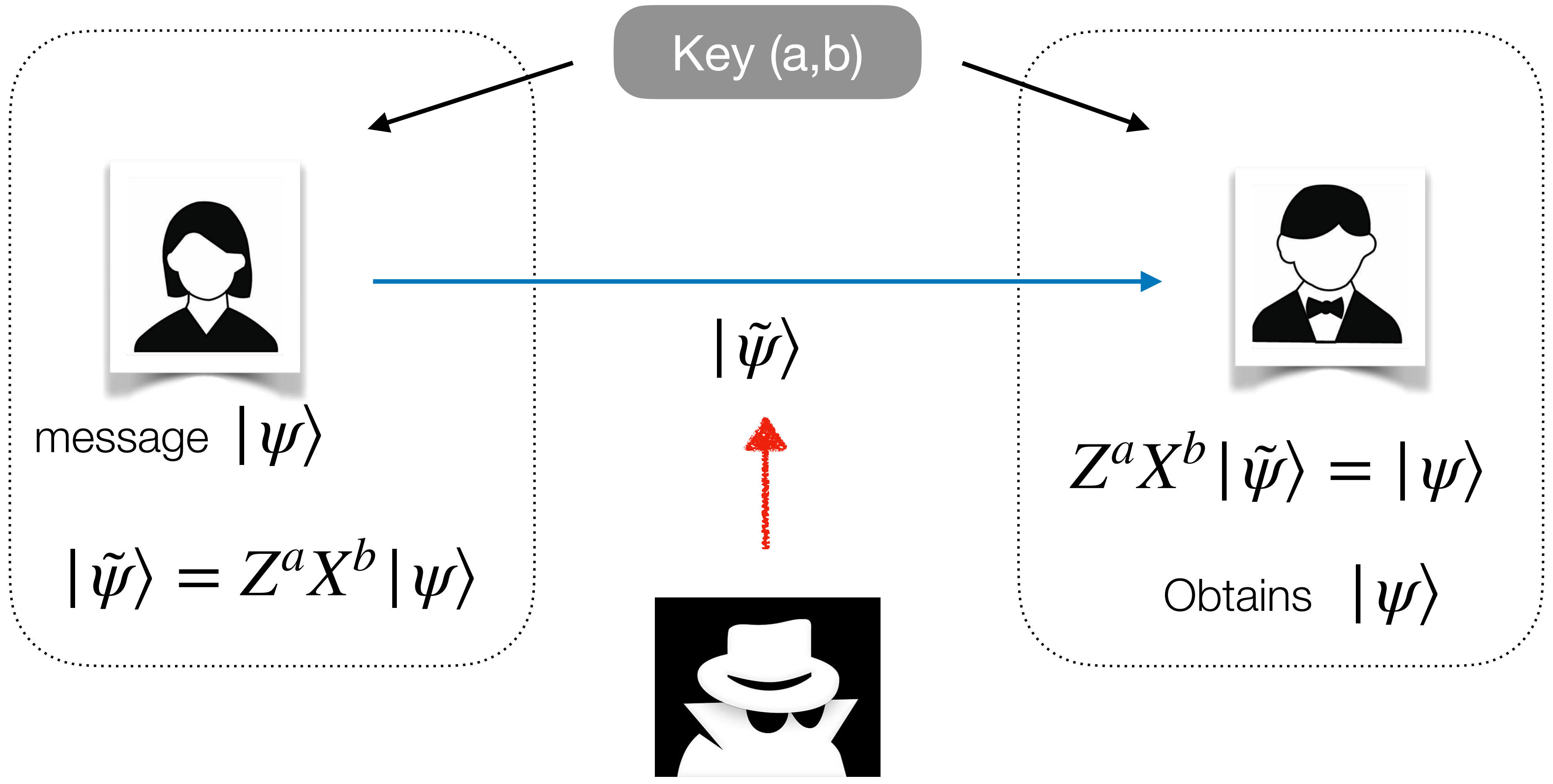
Quantum Teleportation || Quantum One-Time Pad



$$|\tilde{\psi}\rangle = Z^a X^b |\psi\rangle$$

$$\rho = Z^a X^b |\psi\rangle\langle\psi| Z^a X^b$$

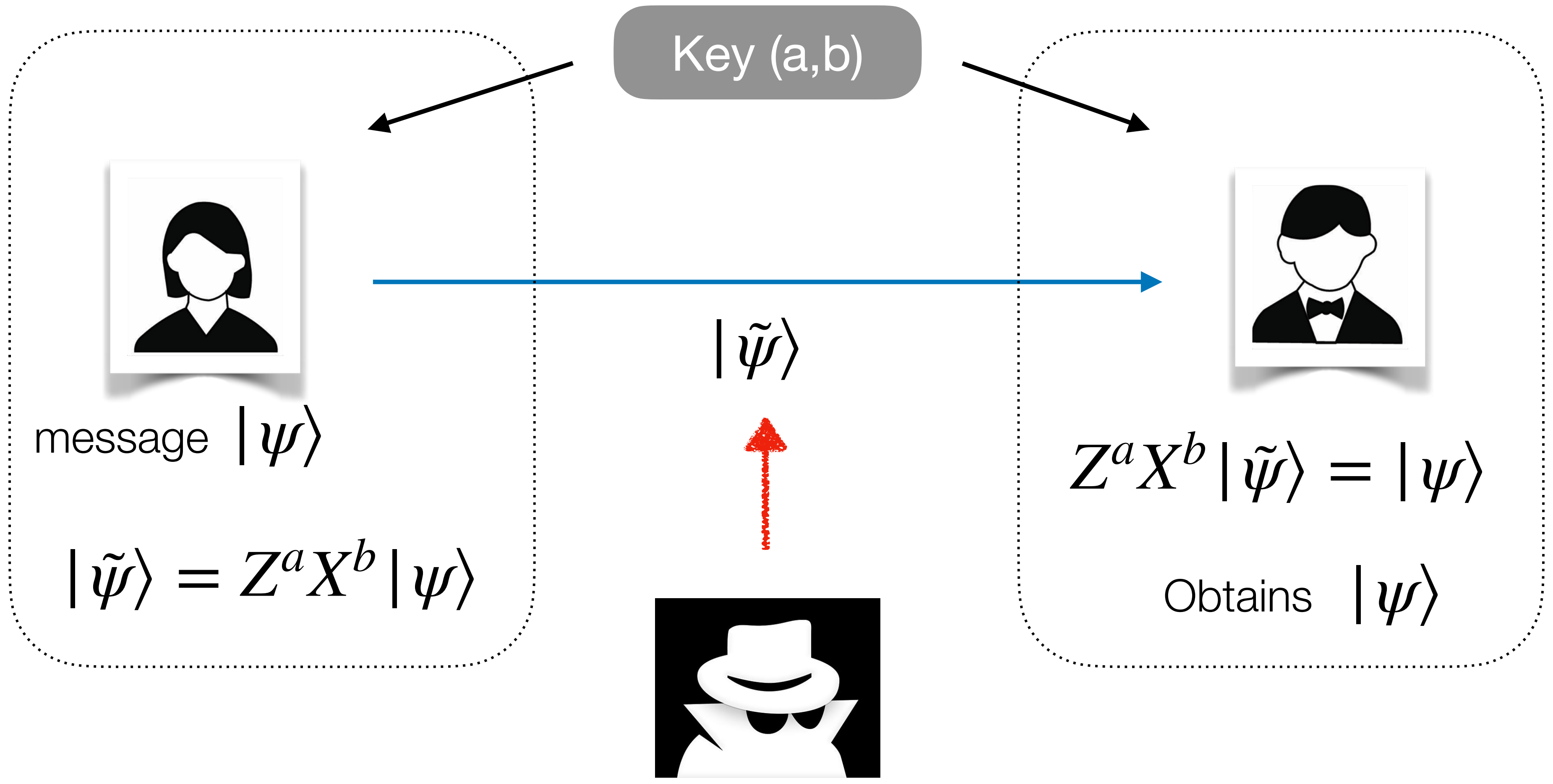
$$\rho = \frac{1}{4}\sum_{a,b} Z^a X^b |\psi\rangle\langle\psi| Z^a X^b = \frac{\mathbb{I}}{2}$$



Correctness: Bob can read the message
Security: Eve gains no information i.e. state is completely mixed and hence independent of message

Information-theoretically secure

Classical vs Quantum One-time Pad



Correctness: Bob can read the message
Security: Eve gains no information i.e. state is completely mixed and hence independent of message

Information-theoretically secure

Encrypt

$$\tilde{m} = m \oplus b$$

$$|\tilde{m}\rangle = X^b |m\rangle$$

X is quantum operation that does the bit flip

Decrypt

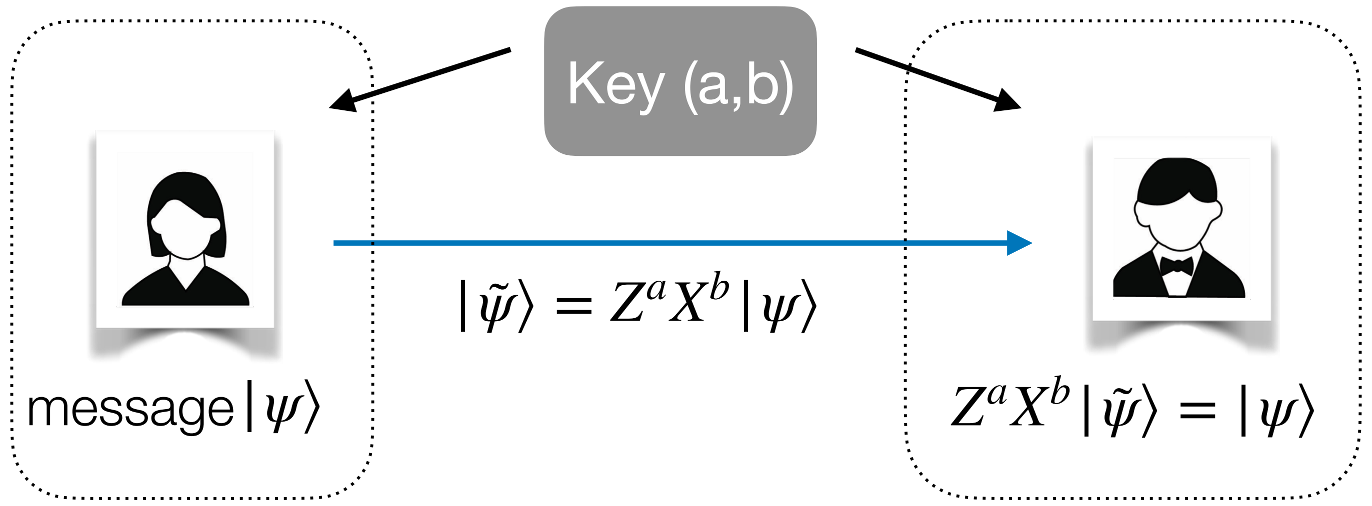
$$m = \tilde{m} \oplus b = (m \oplus b) \oplus b$$

$$|m\rangle = X^b |\tilde{m}\rangle = X^b(X^b |m\rangle)$$

$$X|m\rangle = |m \oplus 1\rangle$$
$$Z|m\rangle = (-1)^m |m\rangle$$

Quantum One-time pad: Bit flips in both basis

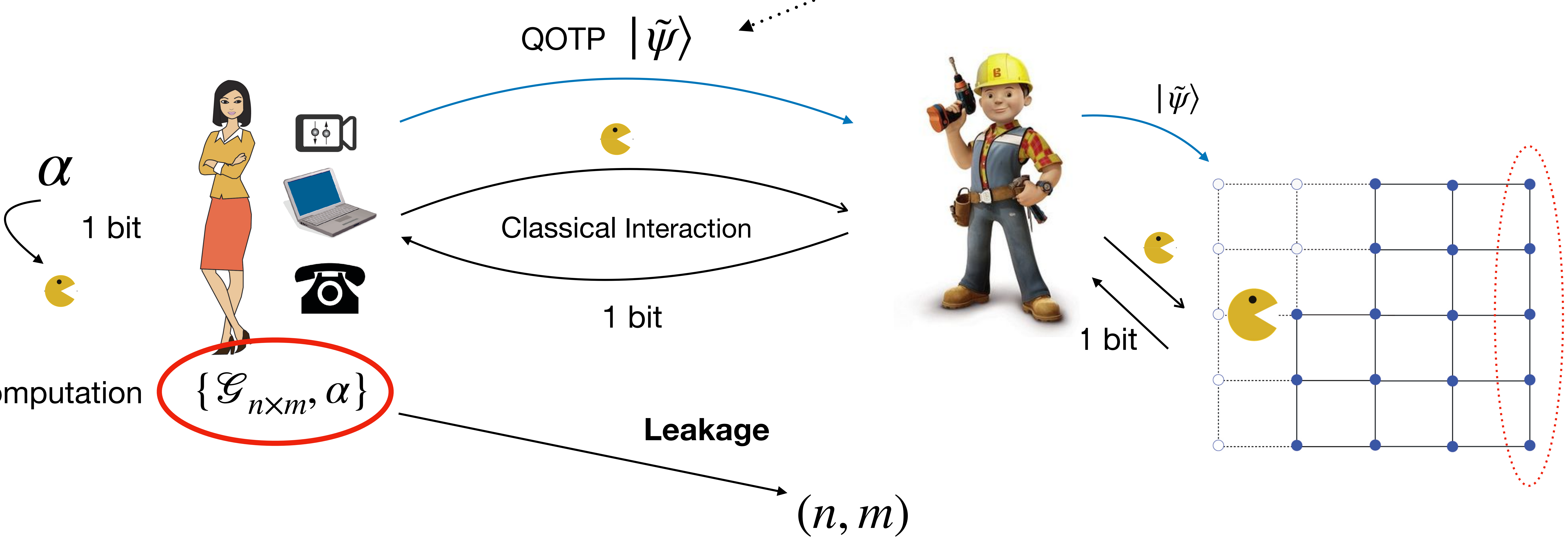
Delegated Quantum Computation



Quantum One-Time Pad (QOTP)

Broadbent-Fitzsimons-Kashefi (BFK) scheme

Single-qubit quantum states $|\tilde{\psi}\rangle := \frac{|0\rangle + e^{i\theta}|1\rangle}{\sqrt{2}}$



One-time Pad
the computation angle
Key (a,b)

Alice's Computation $\{\mathcal{G}_{n\times m}, \alpha\}$

BFK Scheme consists of **Quantum** + Classical Interaction

Private Quantum Computation

Information-theoretic Schemes
(all powerful server)

2001

Powerful Quantum Client

Childs' Scheme (QIC)

2009

Weak Quantum Client

Broadbent-Fitzsimons-Kashefi (FOCS)
Aharonov-Ben-or-Eban (ICS)

2012

Classical Client
2 entangled servers

Reichardt-Unger-Vazirani
(Nature)

2013

Optimal Scheme for Cloud QC

MDPF(PRL)
GMMR(PRL)

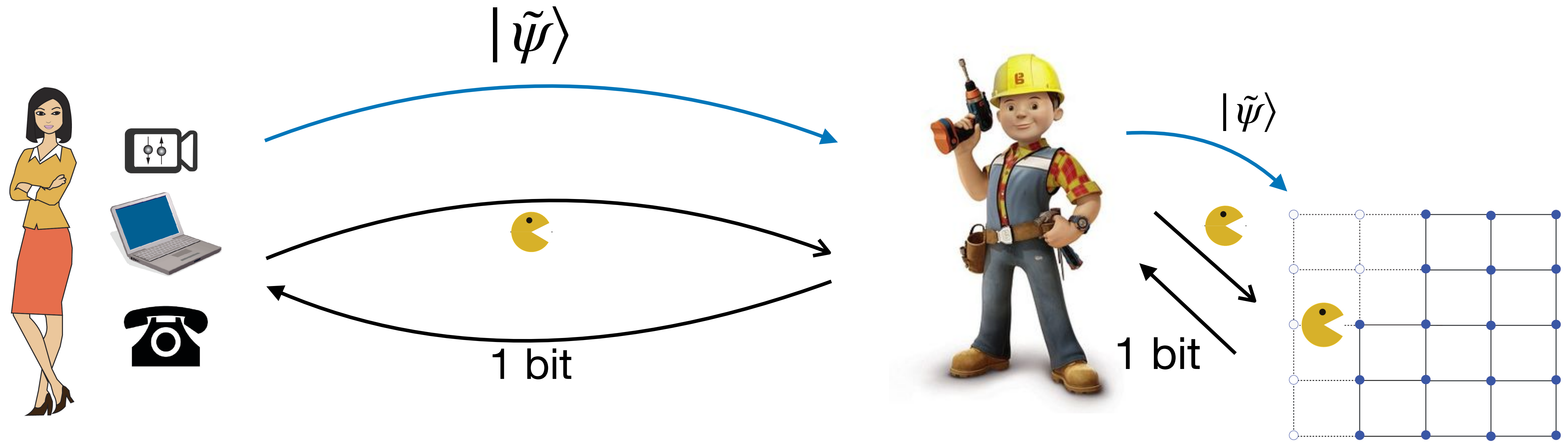
2016

First Scheme
Classical Client - Single server

MDMF (PRX)

Any questions so far?

Can we “dequantize” the quantum interaction from the BFK scheme?



Remote State Preparation (RSP)

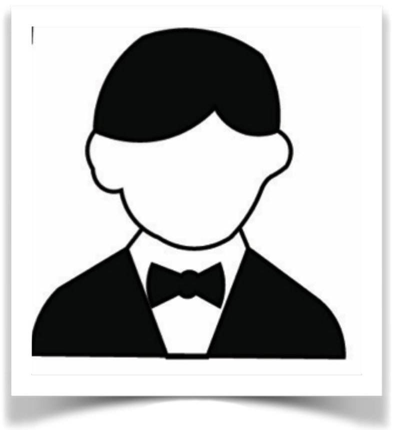
Classical Bits

RSP

Quantum State

a, b ← RSP → $H^a X^b |0\rangle$

Alice



Bob

a	b	$H^a X^b \|0\rangle$
0	0	$\|0\rangle$
0	1	$\|1\rangle$
1	0	$\|+\rangle$
1	1	$\|-\rangle$

Easy and secure if Alice and Bob share quantum resources

1. Alice could perform Quantum Teleportation

2. Alice could prepare and send the state via Quantum Channel

Quantum Satellite

Maybe not so easy and secure only if Quantum Satellite doesn't collude with Bob

What if Alice and Bob share a classical channel and they don't trust Quantum Satellite?

Classical User - Quantum Server

Computational Security

2017

Complexity-theoretic limitations

Aaronson et al. (ICALP)

2018

FHE for Quantum Circuits
Verification of Quantum Comp.

Mahadev (FOCS)

2019

Secure RSP

Gheorghiu and Vidick (FOCS)
Cojocaru et al. (ASIACRYPT)

2020

Modular approach, simpler cryptographic assumption and security limitations

BCCKMW ASIACRYPT

2020

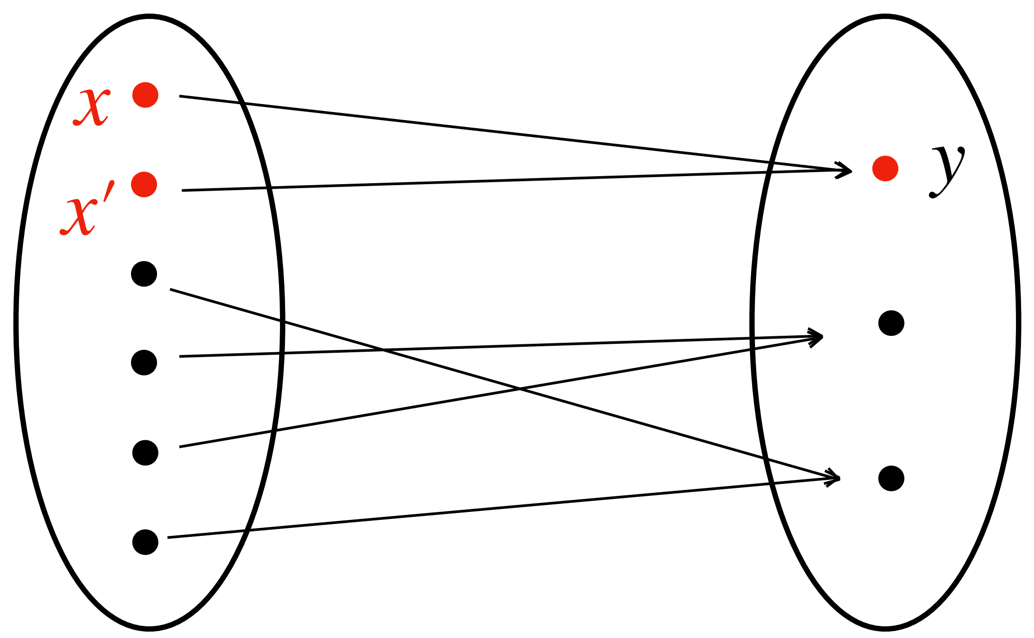
First Secure Q2PC based on Classical Channel

CCKM (arXiv: 2010.07925)

RSP Constructions

Type I: Using trapdoor claw-free functions (TCFF)

Brakerski et al., Mahadev (FOCS 2018), Gheorghiu-Vidick (FOCS 2019)



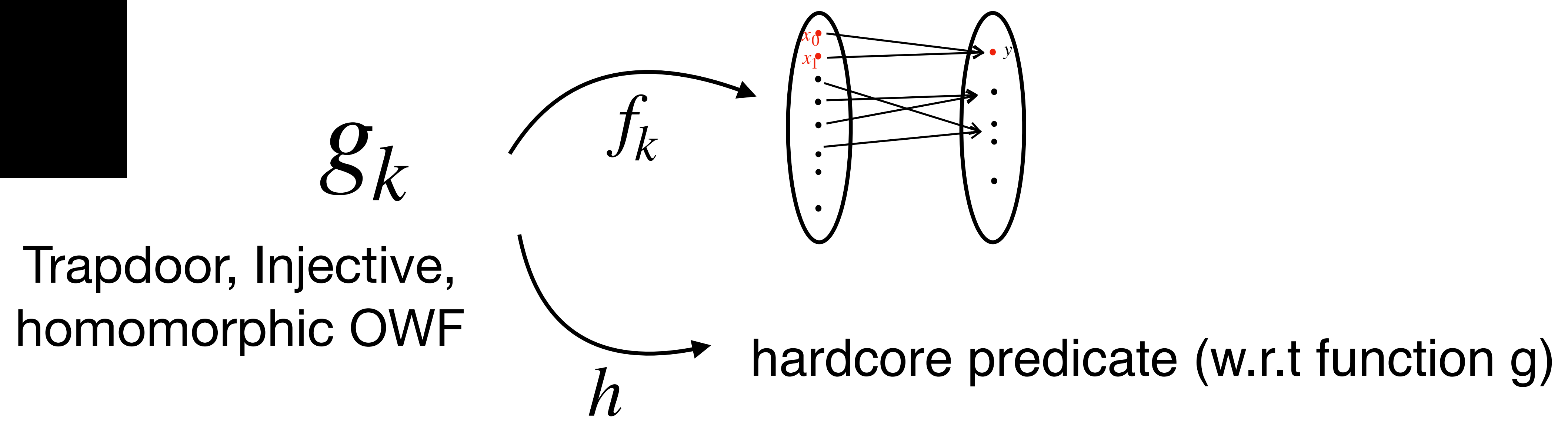
- f is one-way, hard to invert
- 2-to-1 function
- Collision resistant i.e. hard to find claws: pairs (x, x') such that f(x) = f(x') = y without trapdoor
- With trapdoor it is easy to invert y and find (x, x')

Type II: Using homomorphic trapdoor injective OWF

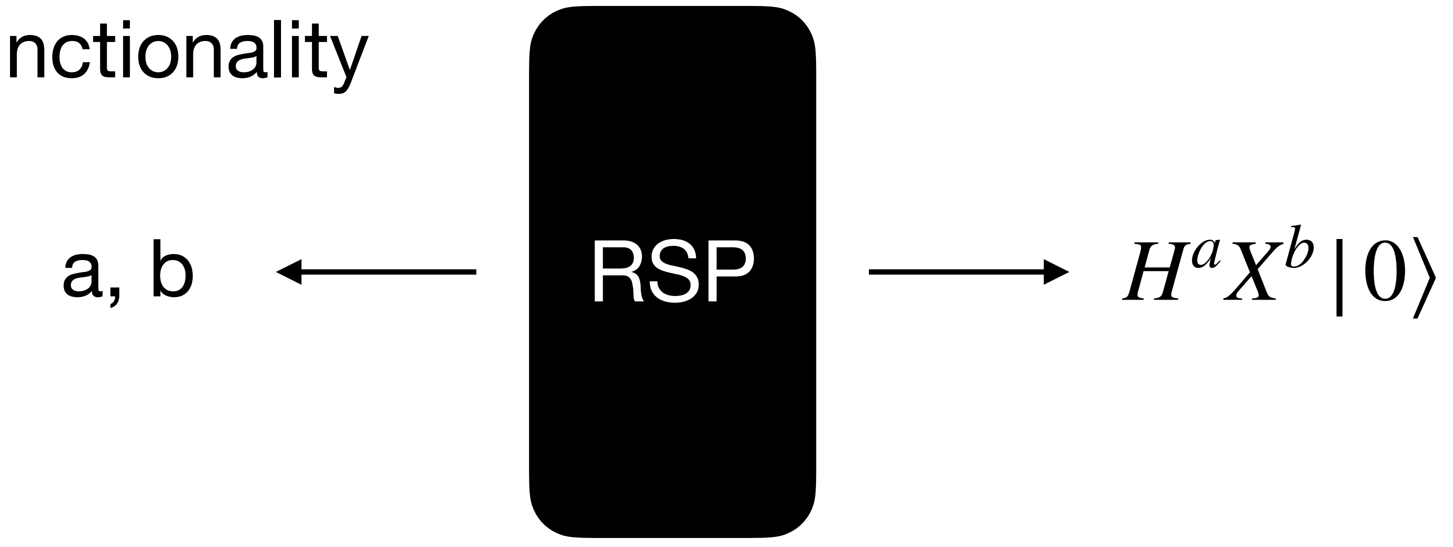
Cojocaru et al. (Asiacrypt 2019)

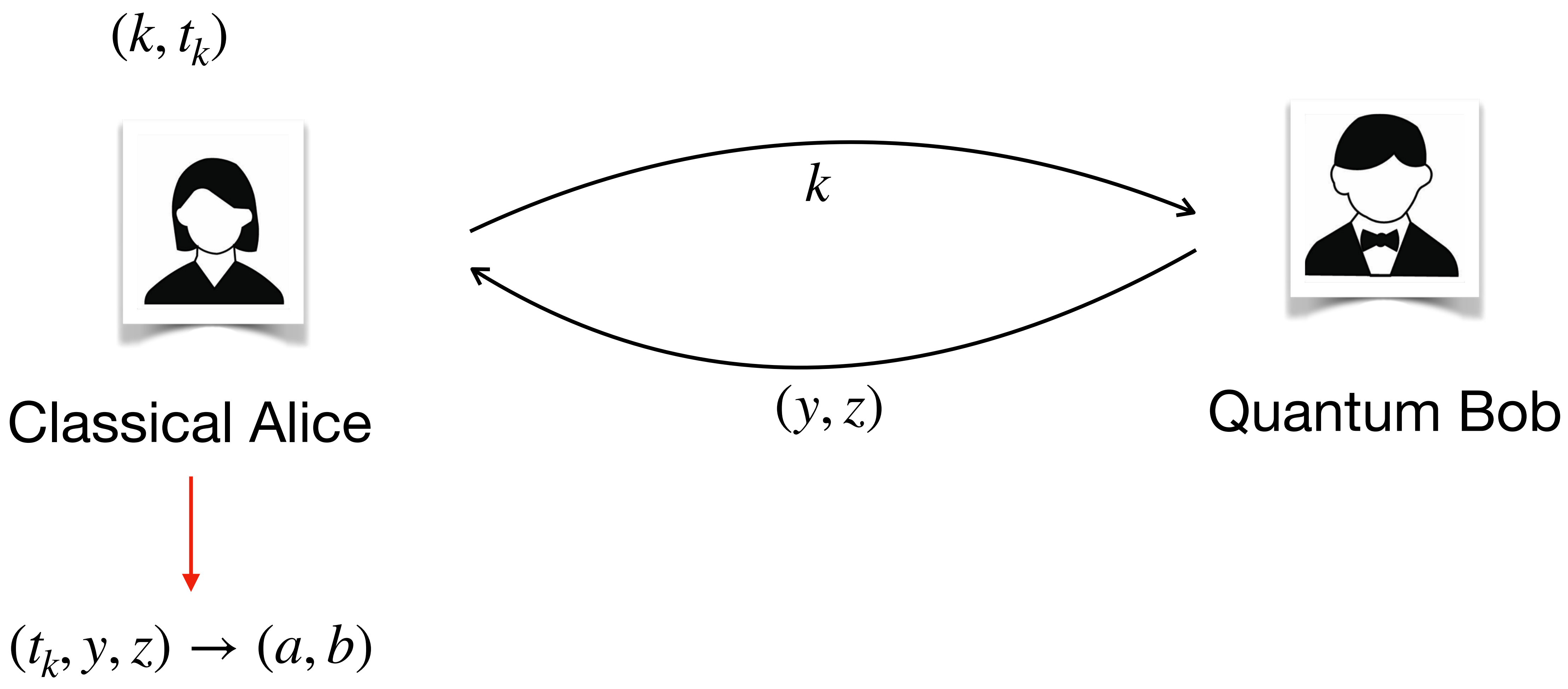
RSP Construction in this talk are based on Type II

High-Level Idea

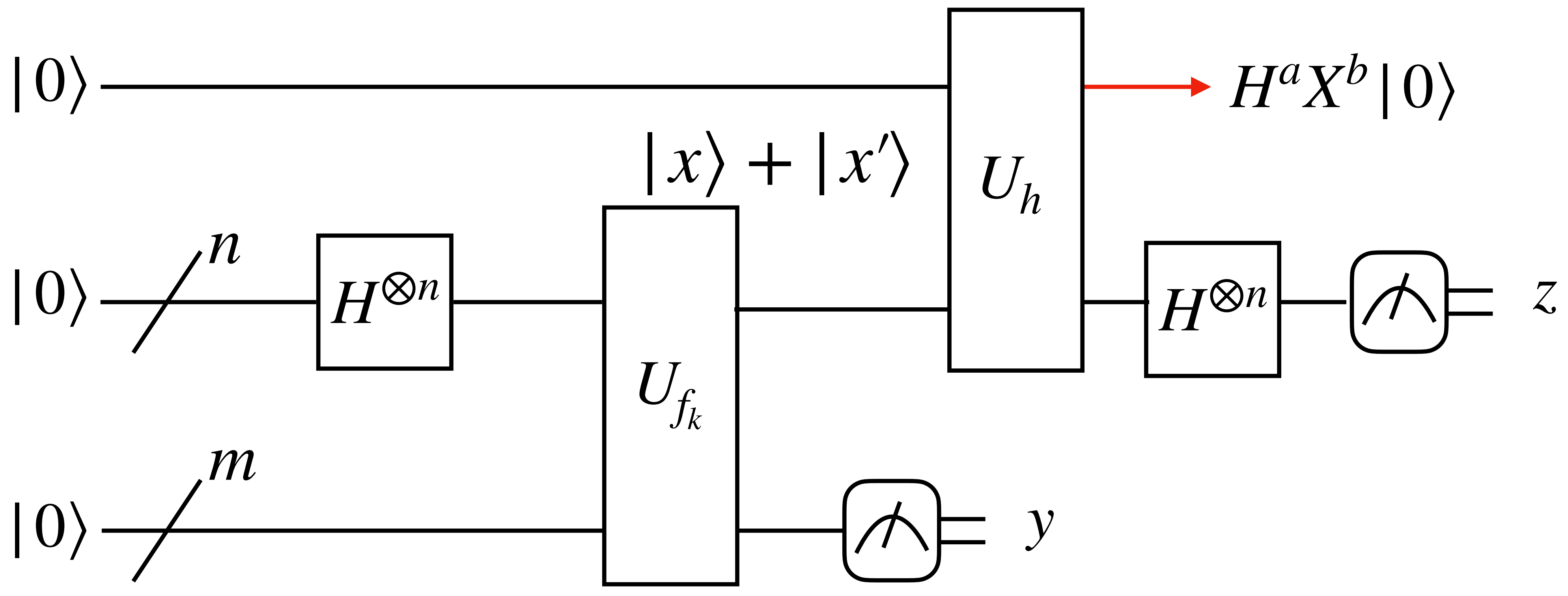


Ideal Functionality





Concrete Protocol



Prepare superposition over all possible inputs x

Evaluate the function f in another register

Measure the second register (image) to obtain the outcome y

Evaluate the function h

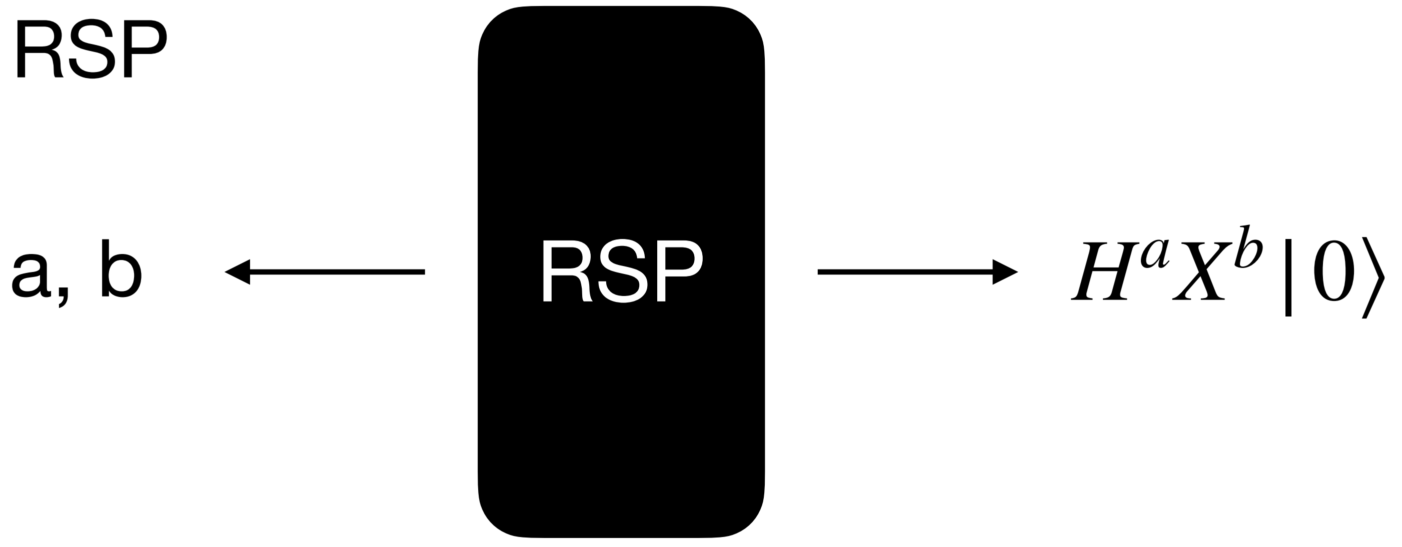
Measure all but one qubit and obtain z

Security: The bit "a" is a hard-core predicate => Bob cannot guess the bit "a" any better than 1/2

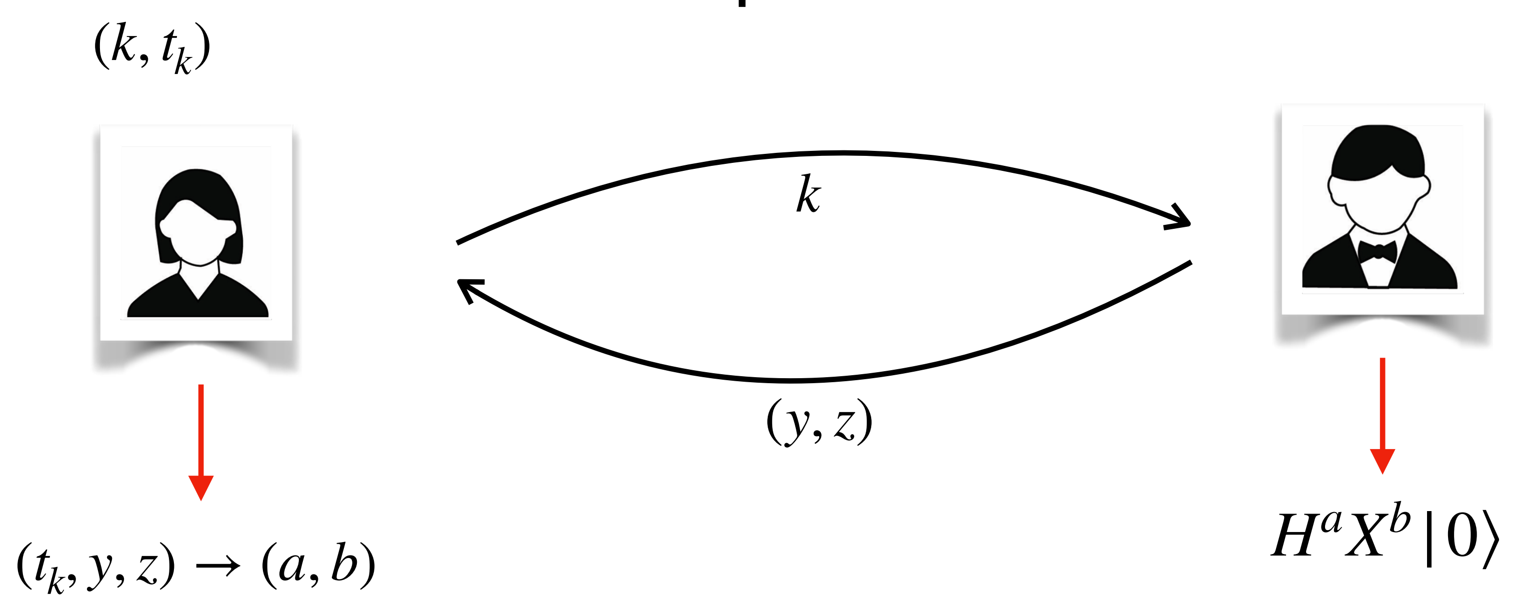
Alexandru Cojocaru, Léo Colisson, Elham Kashefi, Petros Wallden (Asiacrypt 2019)

Abstract Cryptography
A framework for Composable security

Ideal RSP



Concrete protocol RSP

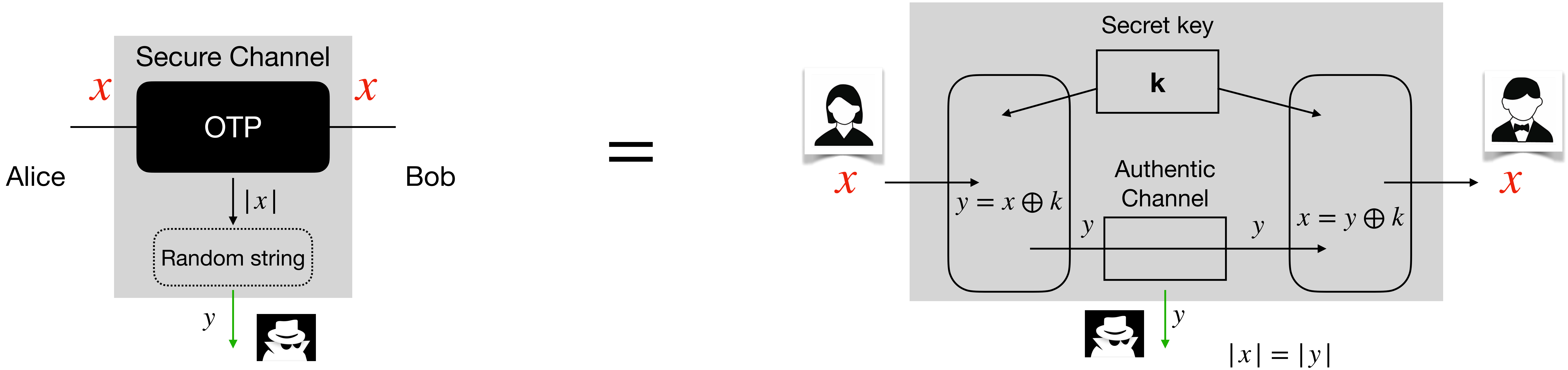


Secure by definition

Cryptography can be regarded as a resource theory!

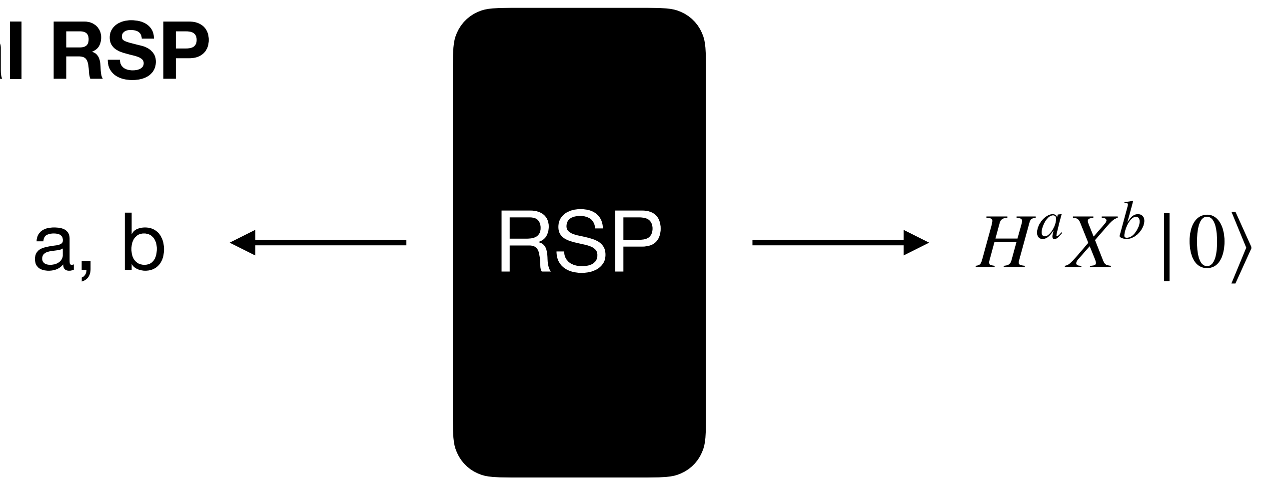
Aim is to construct desired resources from a set of given resources

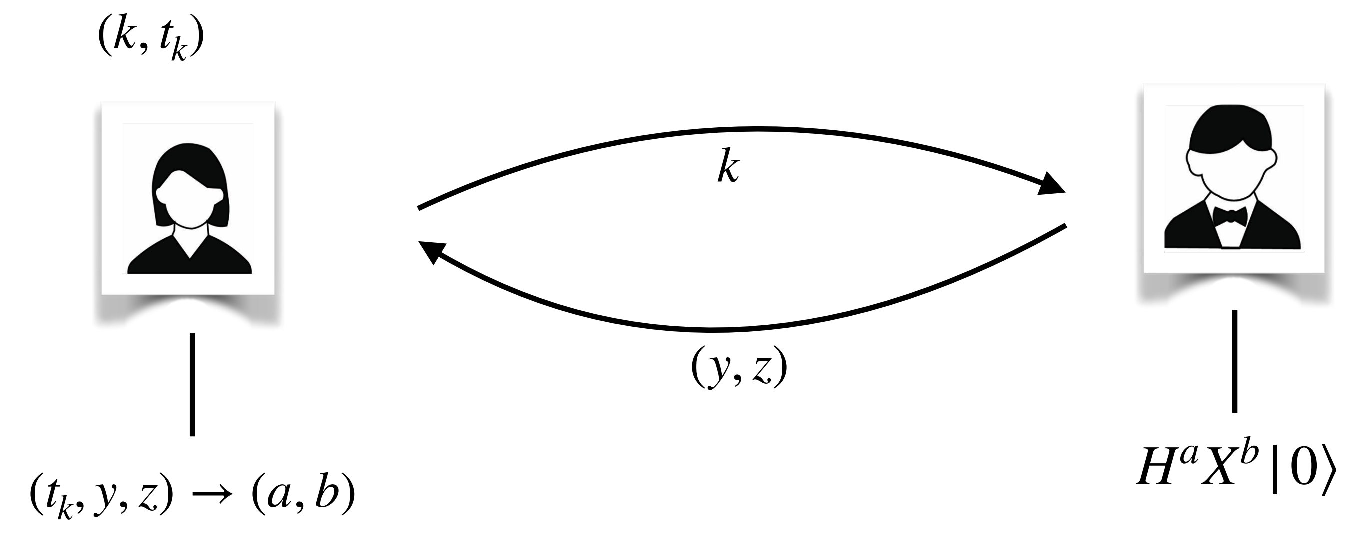
Example: One-time Pad

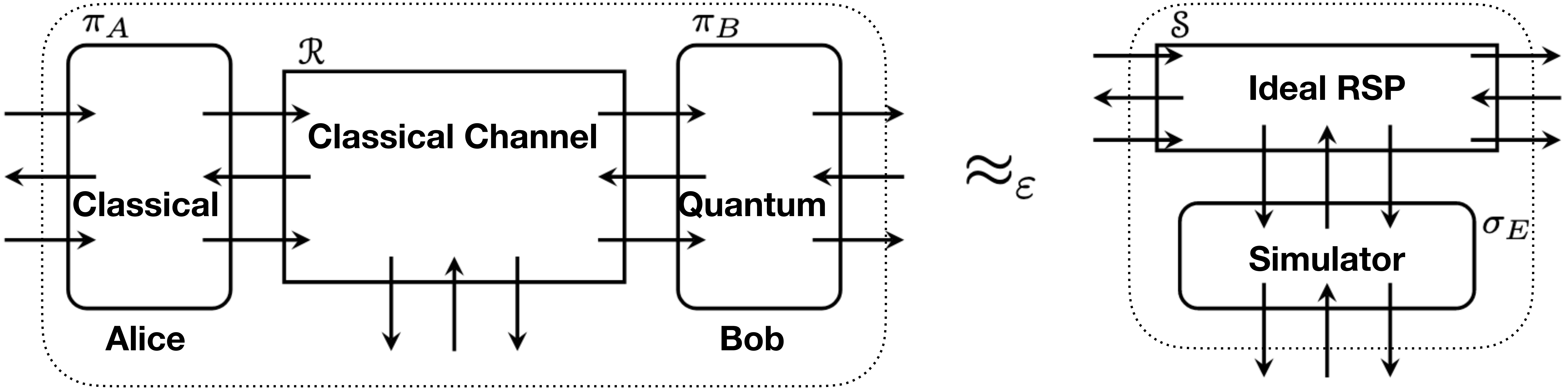


Security of RSP

Ideal RSP



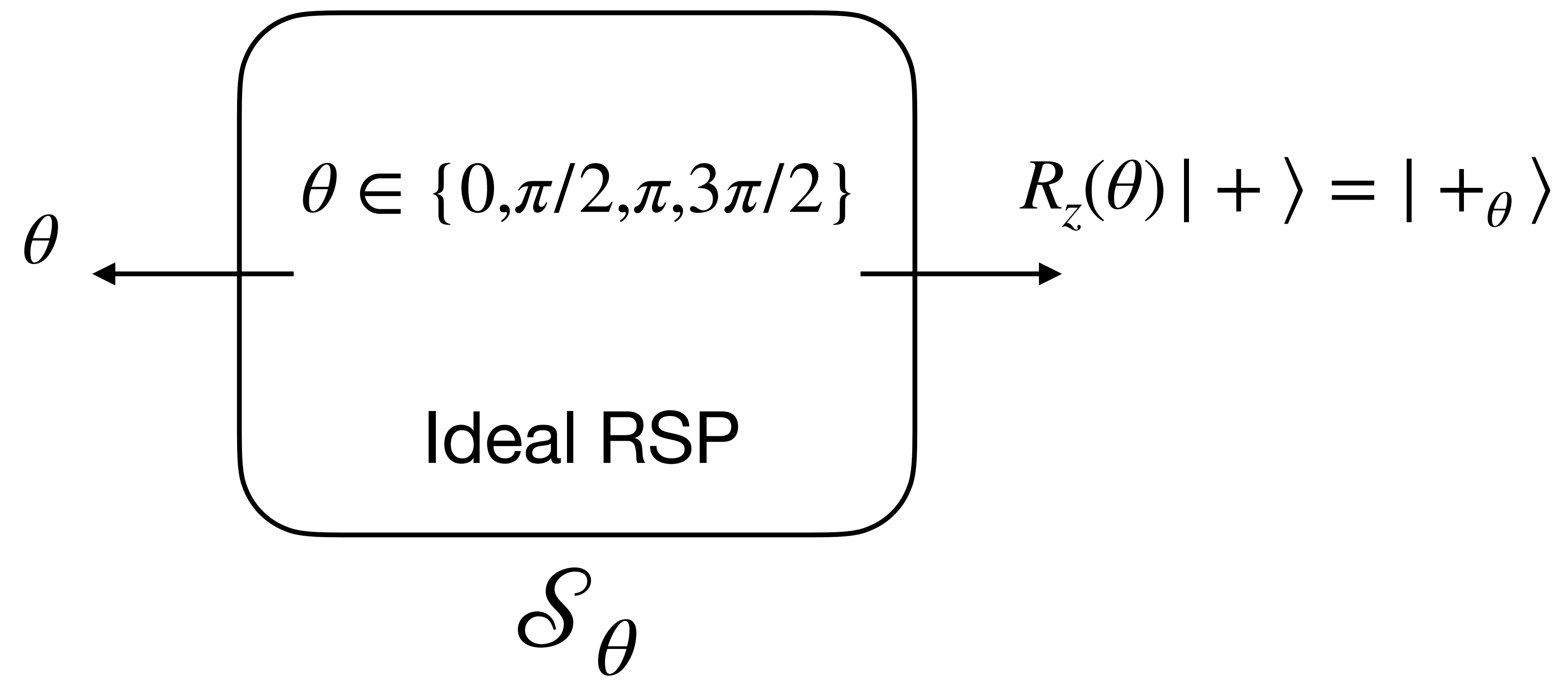


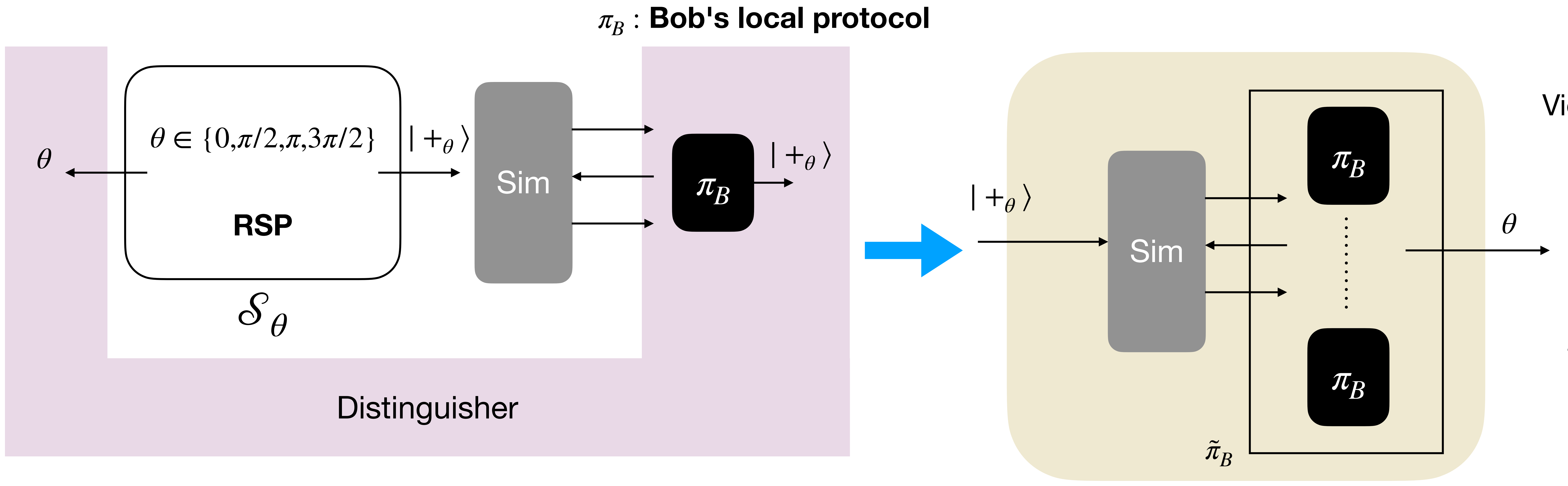


Result: Classical-client RSP protocols **cannot be secure in composable setting**.

Badertscher, Cojocaru, Colisson, Kashefi, Leichtle, Mantri, Wallden (ASIACRYPT 2020)

Proof Sketch



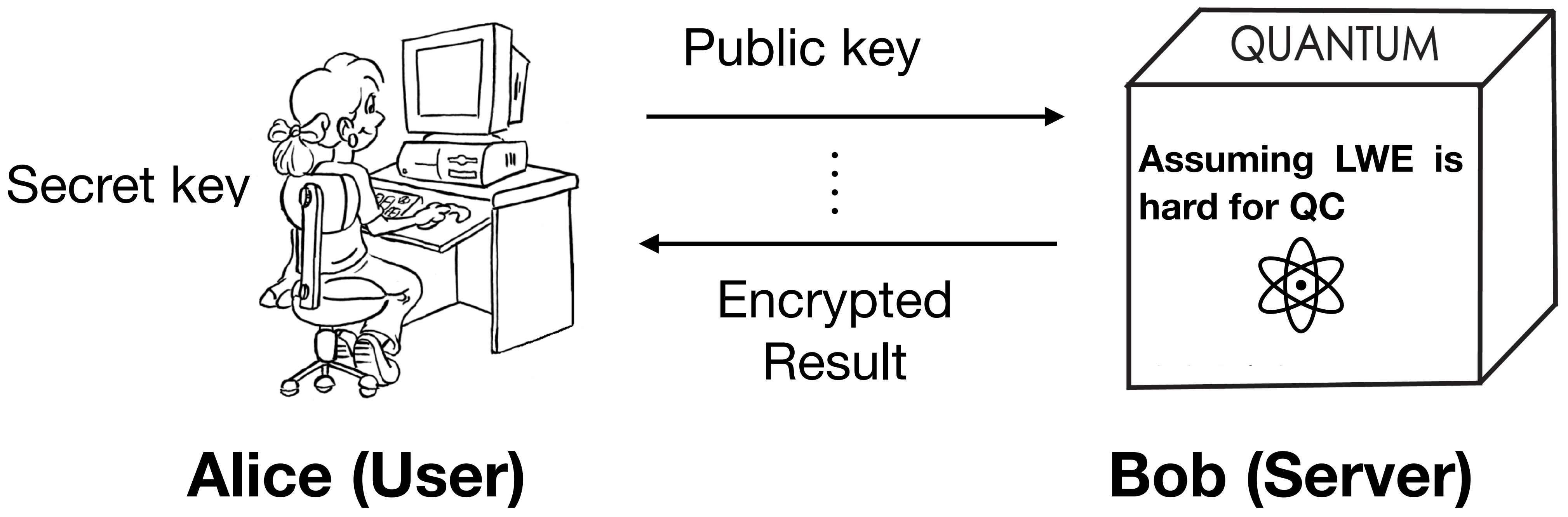


Violates No-Cloning

Takes as input a single copy of the unknown state and outputs classical description

Does that mean RSP is not useful at all?

Applications



Modular classical client delegation scheme (based on computational assumptions)

Using <u>remote state preparation</u> to replace quantum channel in BFK scheme

Assumptions: Trapdoor homomorphic Injective OWFs

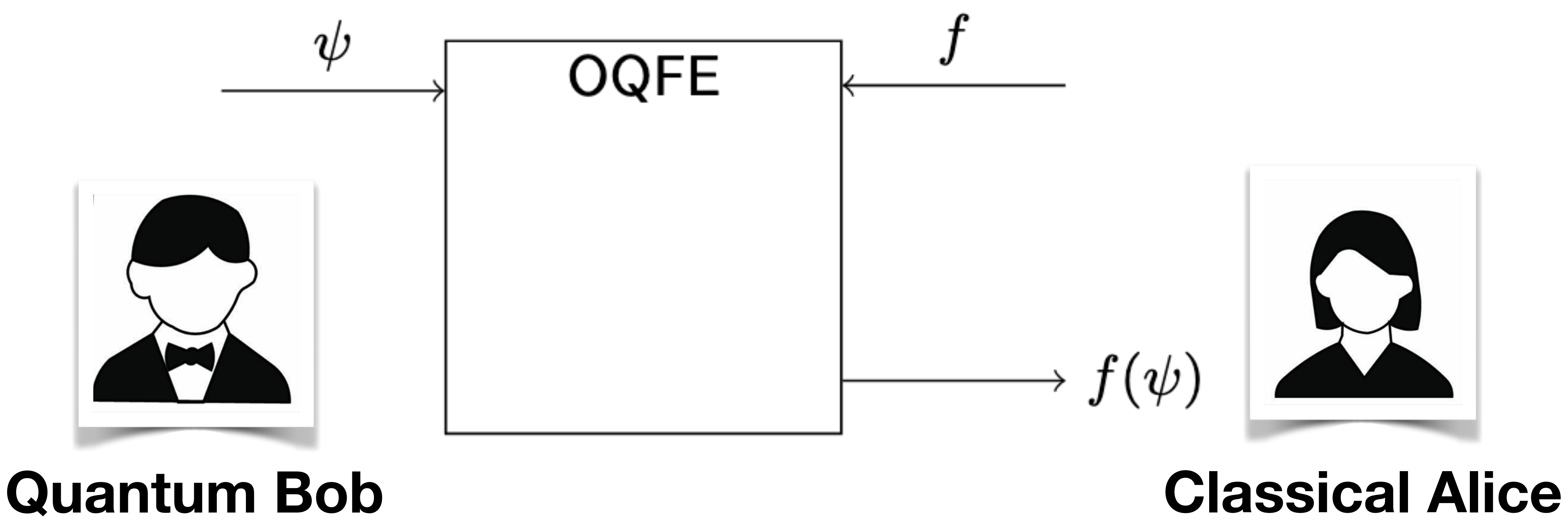
Security: Game-based vs composable

Open Questions: Composable Verifiable Delegated Quantum Computation? Other relaxations?

BCCKLMW (ASIACRYPT 2020)

<u>Quantum two-party Computation over Classical Channel</u>

Oblivious Quantum Function Evaluation

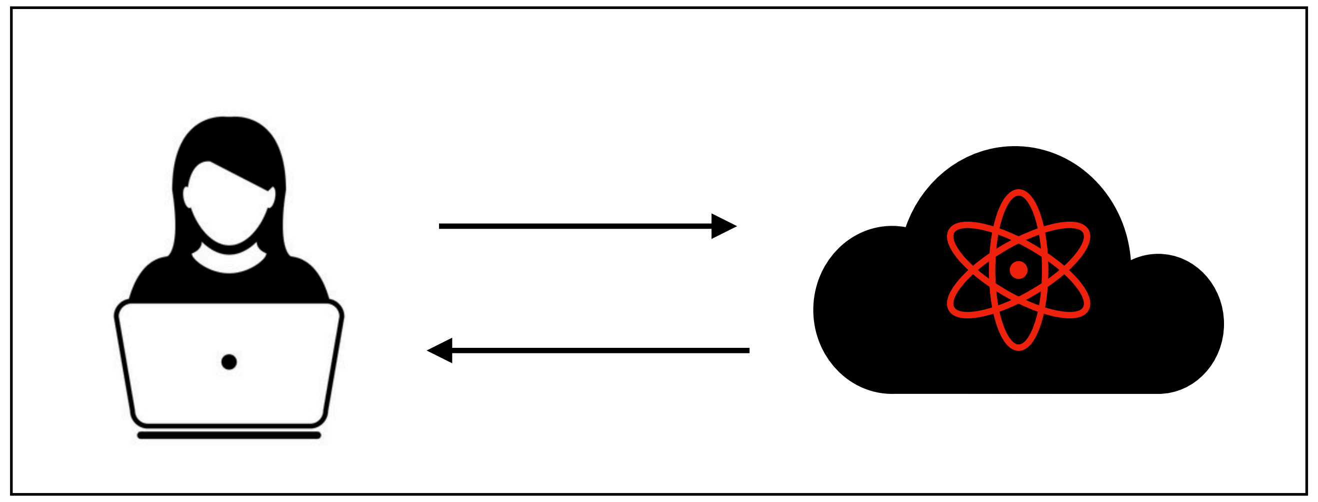


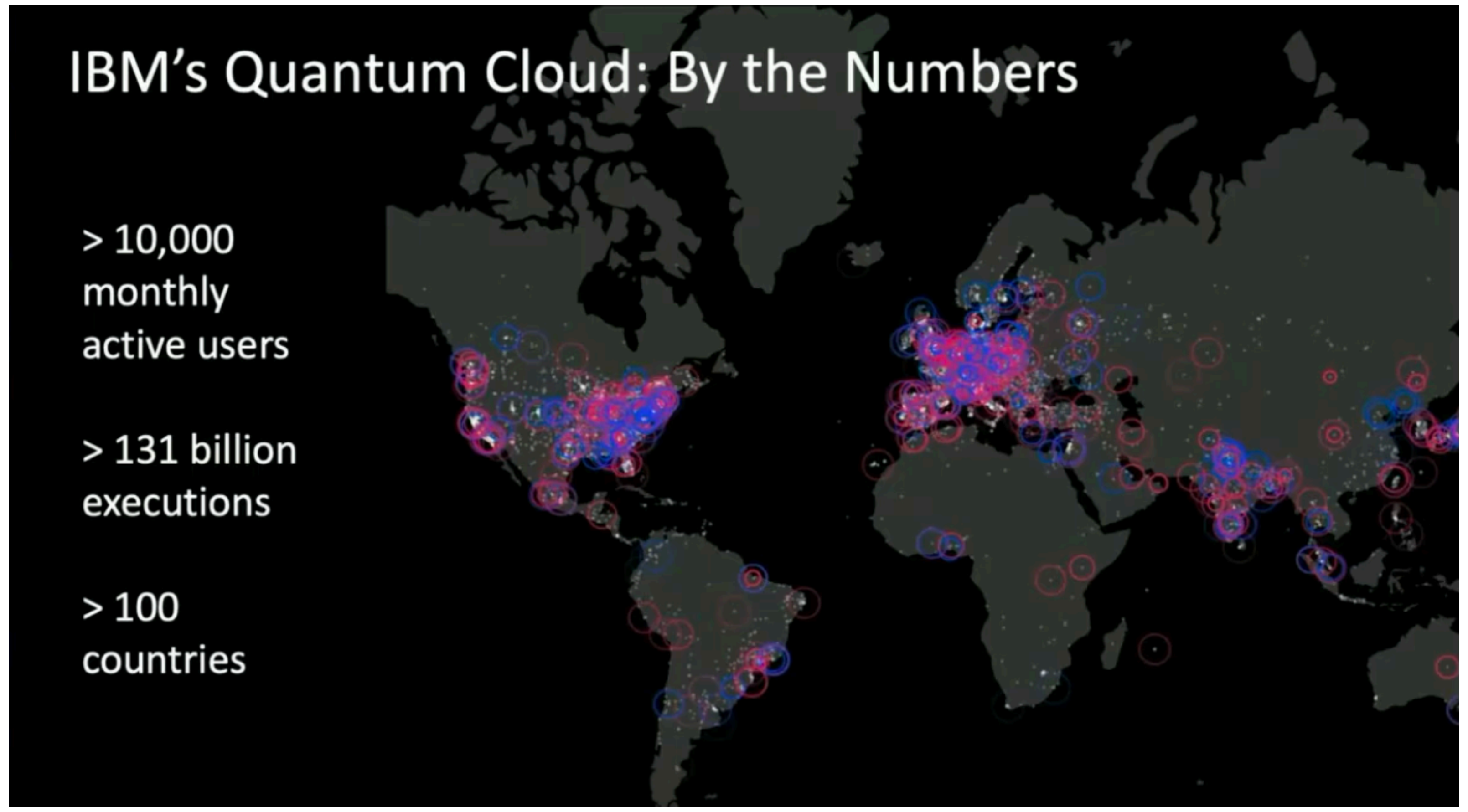
- Construction: Using RSP and ideas from BFK scheme!
- Security: Simulation-based security against Malicious Alice and Privacy against Quantum Bob
- Limitation with fully Black-Box simulation ~ Classical Proofs of Quantum Knowledge
- Open Questions: MPC over hybrid classical-quantum networks? Non Black-Box simulation?

Ciampi, Cojocaru, Kashefi, Mantri (arXiv:2010.07925)

Summary

- Securely delegating quantum functions is indeed possible.
- Tradeoff: Information-theoretic security and Computational Security
  - Perfect Security is possible but requires quantum channel.
  - Protocols based on Classical Networks are possible at the cost of (weaker) security i.e. against Quantum Servers.
  - Open Problems: Other applications of secure remote state preparation? Can they be based on weaker cryptographic assumptions?





Data from early 2020

Quantum Computers are getting distributed around the world and applications/algorithms would require privacy.

Thank you for listening!