Quantum Cryptography 103:

Understanding the Limitations of Quantum Information & Going Beyond Key Distribution

Mina Doosti

Okinawa School in Physics: From quantum key distribution to the quantum internet (OSP2025)

OIST, Okinawa

September 2025

Outline:

- Recap of some limitations/no-gos
- Quantum cryptography beyond QKD: What else it there?
- Quantum Money
- Bit Commitment
- Quantum Coin Flipping

What were the things we couldn’t do in quantum again?

No-cloning: We can’t perfectly copy completely unknown quantum states. We can’t even do it imperfectly with any precision (fidelity) that we like, there are fundamental limits for that.
There are also other no-go theorems in quantum (no broadcasting, no deleting, no superposition)

Classical information extraction limit : We can only extract one classical information from one qubit

Distinguishability: We can’t perfectly tell apart any two arbitrary quantum states and how well we can distinguish them depends on their “distance”.

Entanglement distillation: We can’t get entanglement for free or by just local operation (and classical communication). Entanglement is a resource, and it can be distilled using states that contain “less resource”, but we will need many of them.

But that’s not all… sometimes more is less!

The quantum adversary being more powerful also means that there are some security levels/functionalities that we can’t achieve against them.

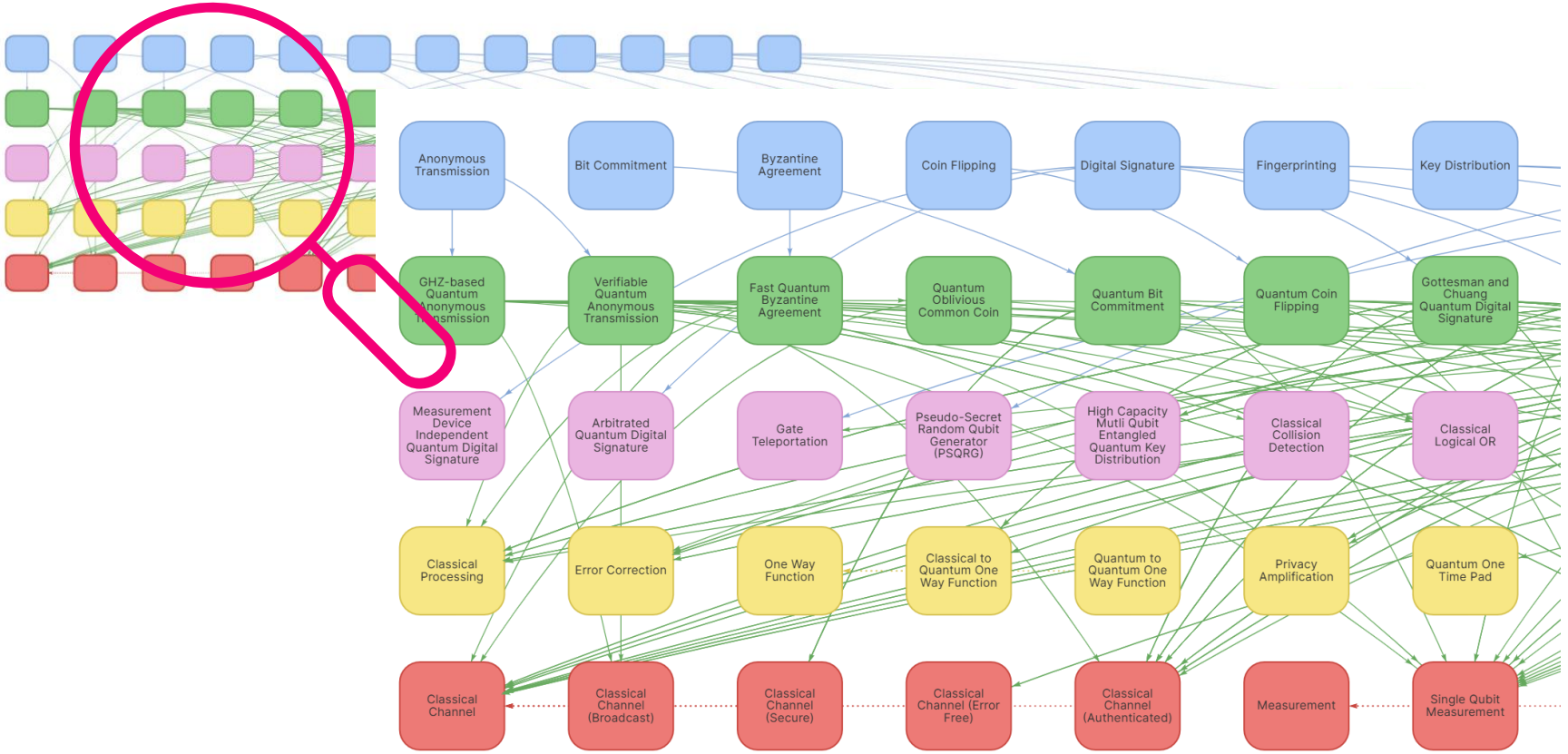
Quantum Cryptography Beyond QKD

or: what else we can do on a quantum internet?

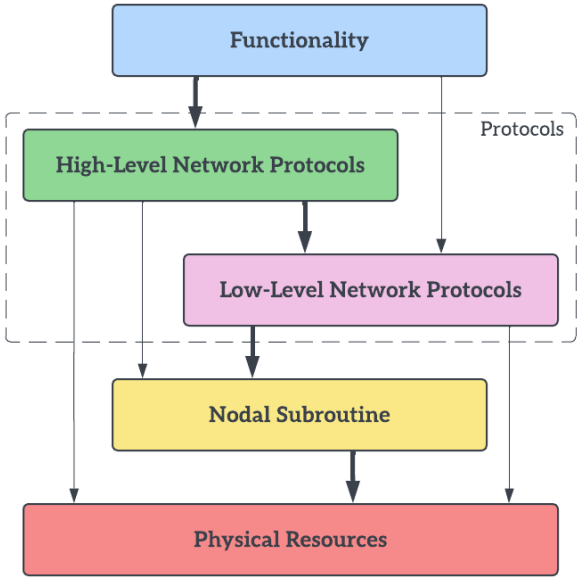
What else can you do on quantum networks?

There is a zoo of quantum protocols

https://wiki.veriqloud.fr/index.php?title=Main_Page



Quantum protocols have certain structures and hierarchy



Singh, Shraddha, Mina Doosti, Natansh Mathur, Mahshid Delavar, Atul Mantri, Harold Ollivier, and Elham Kashefi. "Towards a unified quantum protocol framework: Classification, implementation, and use cases." *arXiv preprint arXiv:2310.12780* (2023).

Quantum Protocol Zoo and QAgora

Agora

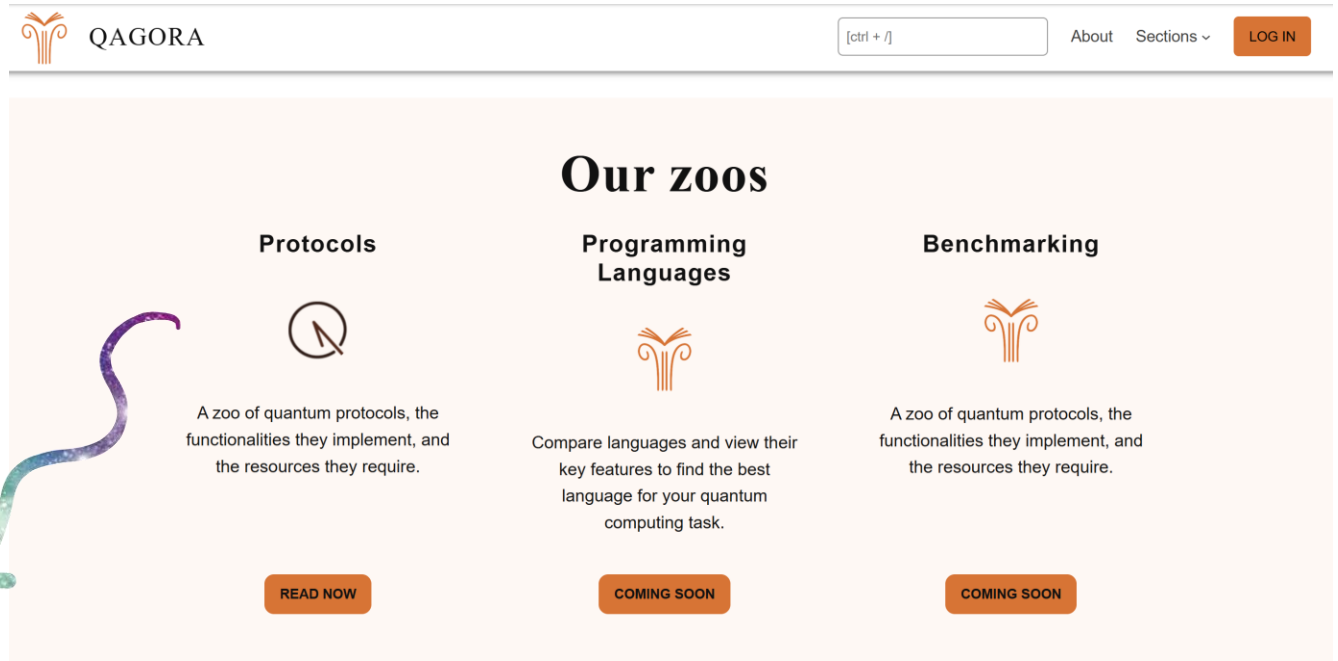
/əˈgɔː.rə/ noun

A gathering place

A community for sharing quantum computing knowledge

Read about quantum protocols, programming languages, and benchmarking.
Explore the page structures and visualisation tools.
Share what you already know.

Version 2.0 out now on QAgora!



Quantum Protocol Zoo and QAgora

Welcome to the Quantum Protocol Zoo!

Explore, Understand, and Code Quantum Protocols.

We invite you to join us and contribute! ☺

Agora

/əˈgɔː.rə/ noun

A gathering place

A community for sharing quantum computing knowledge

Read about quantum protocols, programming languages, and benchmarking.
Explore the page structures and visualisation tools.
Share what you already know.

Gottesman and Chuang Quantum Digital Signature

implements Quantum Digital Signature

Introduction

This protocol achieves the functionality of (Quantum) Digital Signatures (QDS) allowing the exchange of classical messages from sender to multiple recipients, with a guarantee that the signature has come from a genuine sender. This protocol achieves all the properties of QDS. Further it requires the parties to store quantum states for comparison at a later stage thus necessitating the requirement of quantum memory. This protocol is based quantum public key cryptography.

Related Paper(s)

Quantum Digital Signatures

Outline

The signature scheme proposed by Gottesman and Chuang is based on quantum one way functions, which takes classical bit string as input and outputs quantum states. Quantum Digital Signature (QDS) protocols can be divided into two phases: the distribution phase, where quantum signals (public keys) are sent to all recipients, and the messaging phase, where classical messages are signed, sent and verified. Here, we take the case of three parties, one sender (referred to as seller) and two receivers (buyer and verifier) sharing a one bit message. Distribution phase can be divided into the following two steps:

Table of Contents

Some important quantum cryptographic protocols

Quantum Oblivious Transfer
Quantum Bit Commitment
Quantum Coin Flipping

} Primitives (fundamental protocols)

Quantum Secret Sharing
Quantum Digital Signature
Authentication (of quantum and classical messages)
Quantum Leader Election
Quantum Money
Anonymous Transmission

} Quantum-enhanced and quantum functionalities

Secure Multiparty Delegated Quantum Computation
Blind Quantum Computation (next week)
Verification of Quantum Computation
Quantum Electronic Voting

} High-level functionalities and QC-related protocols

Quantum Teleportation (you coded it!)
Copy Protection
Certified Deletion

} Only-quantum functionalities, doesn't exist classically!

Quantum Money

Quantum Money

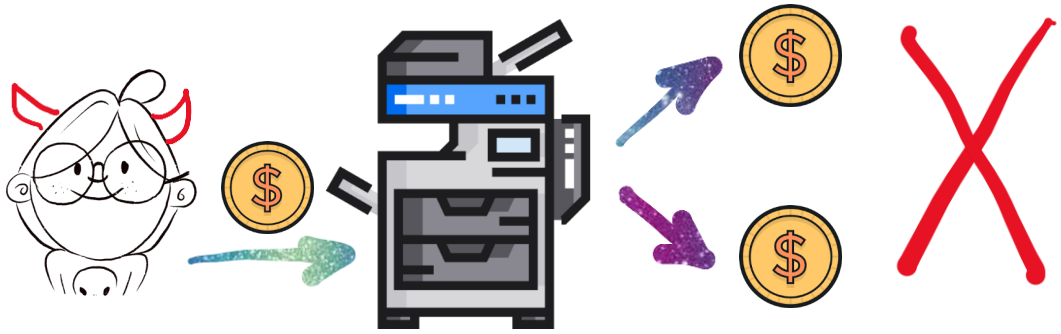
What is money?

Just a number that you spend?

Serial number

Special paper, ink, etc.

Should be verifiable



This should not happen!

In general, any money scheme needs to have unclonability (also called anti-counterfeiting or unforgeability) and verifiability.

What if we use unclonable states instead of special papers to get unclonable money?

Wiesner's Quantum Money

Proposed by: Stephen Wiesner in 1969 (but published in 1983)

Conjugate Coding *

Stephen Wiesner

Columbia University, New York, N.Y.
Department of Physics

The uncertainty principle imposes restrictions on the capacity of certain types of communication channels. This paper will show that in compensation for this "quantum noise", quantum mechanics allows us novel forms of coding without analogue in communication channels adequately described by classical physics.

Wiesner realized that the quantum No-Cloning of quantum states can be used to make a notion of "money" with quantum properties. So Wiesner proposed using qubits to make money that would be physically impossible to duplicate (counterfeit).

But to have a money scheme, we don't only need unclonability but we also verifiability!

How did Wiesner solve this problem?

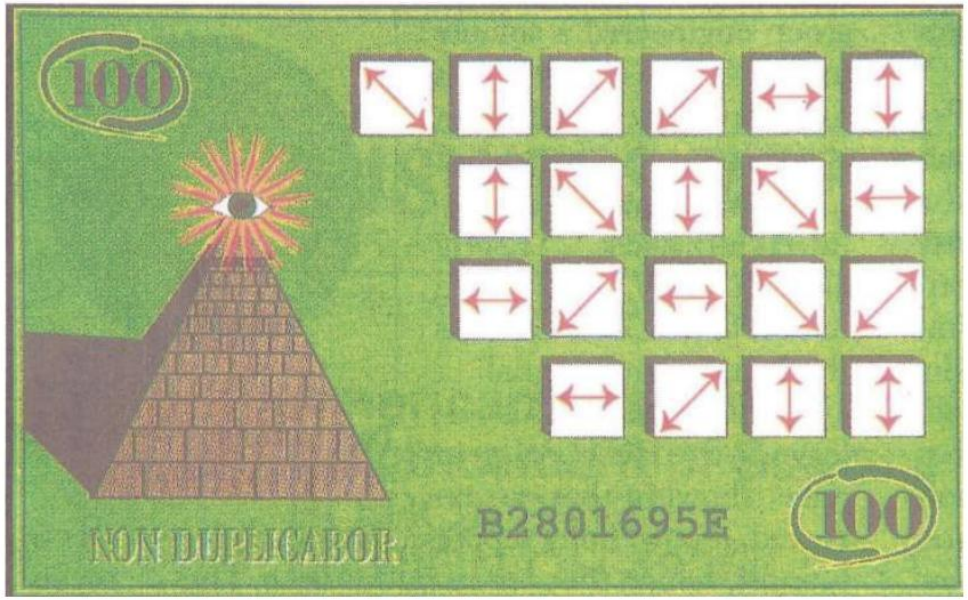
Wiesner's Quantum Money

- Each serial number $\$$ is made of two strings $x_{\$}, \theta_{\$} \in \{0,1\}^n$
- For each pair, a quantum state $|\psi_{x_i,\theta_i}\rangle$ is created which is one of the following states. (should remind you of BB84!)

$$|\psi_{00}\rangle = |0\rangle \quad |\psi_{01}\rangle = |1\rangle \quad |\psi_{10}\rangle = |+\rangle \quad |\psi_{11}\rangle = |-\rangle$$

- The total state is then:

$$|\Psi_S\rangle = |\psi_{x_1,\theta_1}\rangle \otimes |\psi_{x_2,\theta_2}\rangle \otimes \cdots \otimes |\psi_{x_n,\theta_n}\rangle$$



How to verify?

To verify a bill, you bring it back to the bank.

The bank verifies the bill by looking at the serial number, and then measuring each qubit in the bill in the basis in which it was supposed to be prepared.

A bit more formal: The verifier takes a pair $(|\Psi_S\rangle, \$)$ and outputs accept or reject.

Security of Wiesner's Quantum Money

So… is Wiesner's quantum money secure? Does simply no-cloning theorem ensure the security?

Trivial attack: Let's say the adversary tries to guess the serial number by measuring the state.
What's the probability of success?

Other attacks: Ideas?

The best attack we know has probability ¾ per qubit, so $\left(\frac{3}{4}\right)^n$ overall. (still good)

Drawbacks:

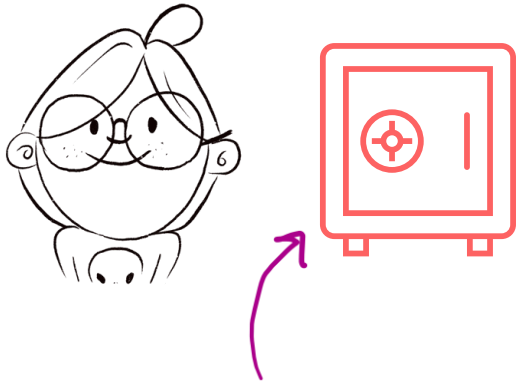
- The scheme requires private verification i.e. only bank can verify the bills (not any merchant).
  This type of quantum money has an important practical problem: We need to ensure that the qubits in a bill don't lose their state (decoherence).

  Side note: Having a fully secure public quantum money scheme is still one of the main open questions in quantum cryptography!

Bit Commitment

Bit Commitment Functionality

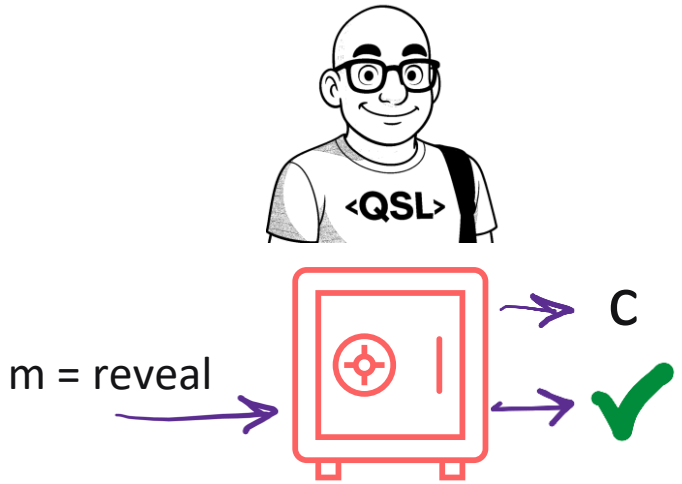
Commit Phase



Alice: Input a bit c into the safe

Bit Commitment

Reveal Phase



Alice: sends the message/request “reveal”

Bob: Receives c
& confirmation that matches commitment

Security:

Alice: Cannot open the commitment to another value than the one she inputs in the commit phase (Binding)

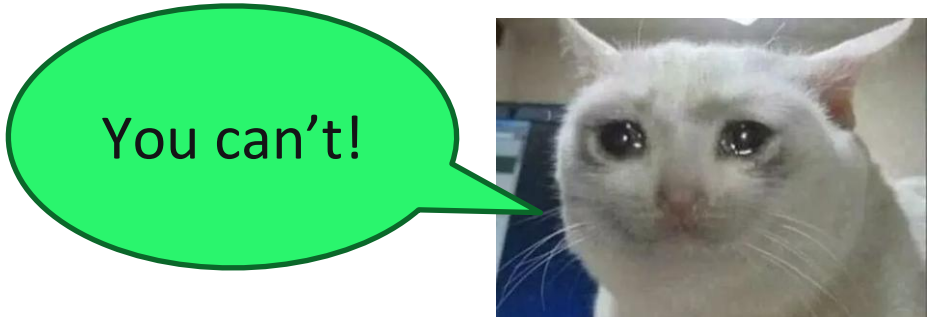
Bob: Learns nothing about c before reveal (Concealing)

Classical and Quantum (Perfect) Bit Commitment

Bit Commitment is one of the most important building blocks (primitives) of cryptography

Why? Because given a perfect BC you can construct many (not all) two-party functionalities (like Zero-knowledge proofs)

So, how do we do it?



It is impossible to achieve Bit-Commitment classically, with information-theoretic security (ITS)

There is easy bruit-force attack that works!
Hiding implies binding is impossible!

How about in Quantum?

IT classical Bit Commitment is impossible.

But Quantum can help, right?

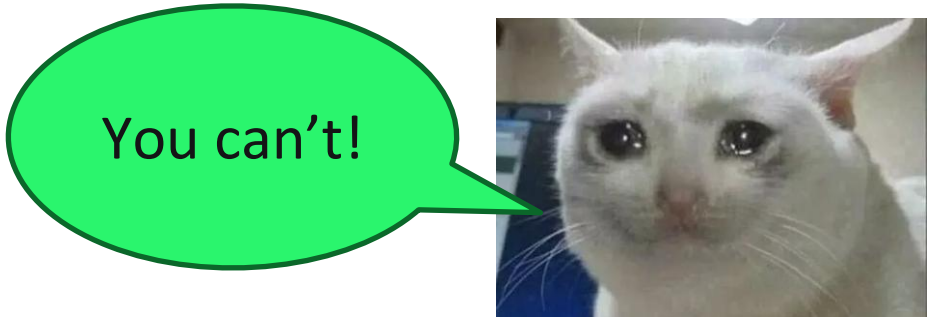
Right??!!

Classical and Quantum (Perfect) Bit Commitment

Bit Commitment is one of the most important building blocks (primitives) of cryptography

Why? Because given a perfect BC you can construct many (not all) two-party functionalities (like Zero-knowledge proofs)

So, how do we do it?



It is impossible to achieve Bit-Commitment classically, with information-theoretic security (ITS)

Hiding implies binding is impossible!

It is impossible (quantumly) to achieve Bit Commitment that is Information Theoretically both Binding and Concealing (by Lo-Chau & Mayers)

Intuition: There are two-qubit states that are different, but Bob's reduced density matrix is the same, and so Alice can change one to another by a local unitary.

Quantum Coin Flipping

Coin flipping

They need a protocol to agree on a random bit But they don’t trust each other!

This is the task of a coin flipping protocol!
Coin flipping was introduced by Blum in 1983

Manuel Blum. “Coin flipping by telephone a protocol for solving impossible problems”. In: ACM SIGACT News 15.1 (1983), pages 23–27

Definition of (Strong) Coin flipping

Definition (Strong) coin flipping**:**

The task of coin flipping consists of two mutually distrustful players, Alice and Bob, and the goal is for both players to output the same random bit $c \in \{0, 1\}$ such that the following properties hold:

1. **Correctness**: if both Alice and Bob are honest then b is uniformly distributed: $p(c = 0) = p(c = 1) = 1/2$.
2. **ε-secure:** neither player can force $p(c = 0) \geq 1/2 + \varepsilon$ or $p(c = 1) \geq 1/2 + \varepsilon$, where p(c) is the probability that the honest player outputs a value c.

The smallest ε for which a protocol is ε-secure is called the **bias.**

Impossibility of classical unconditionally secure coin flipping (Also by Blum 83):
No classical coin flipping protocol is secure, i.e. no value of $\varepsilon < 1/2$ can be achieved for security!

If Alice cannot completely bias the output of the protocol, Bob can (and vice versa)

Intuitively can you see why?

But you can do it with computational assumption (OWF)

Manuel Blum. "Coin flipping by telephone a protocol for solving impossible problems". In: ACM SIGACT News 15.1 (1983), pages 23–27

Quantum Coin Flipping

The first quantum coin flipping protocol was introduced by Mayers et al [1] in 1999. But the security proof was not complete

Progress toward practical quantum cryptanalysis by variational quantum cloning

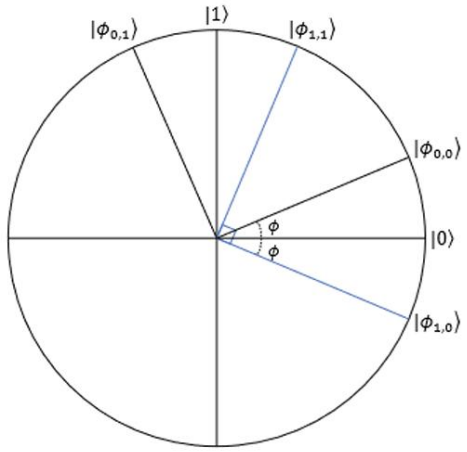
Brian Coyle[1], Mina Doosti[1], Elham Kashefi[1,2], and Niraj Kumar[1]

Show more

Phys. Rev. A **105**, 042604 – **Published 11 April, 2022**

DOI: https://doi.org/10.1103/PhysRevA.105.042604

The next one was introduced in 2000 by Aharonov[2] (with a formal security proof)
It uses pairs of non-orthogonal qubits
It's not perfect but showed possibility: Bob's bias: 0.36, Alice's bias 0.42



Another protocol was introduced by Ambainis [3] (2004) with a better bias
This one uses qutrits (d = 3)
Has a symmetric bias of 0.25

[1] D. Mayers, L. Salvail, and Y. Chiba-Kohno, "Unconditionally secure quantum coin tossing," tech. rep., -, 1999.
[2] Dorit Aharonov et al. "Quantum bit escrow". In: Proceedings of the thirty-second annual ACM symposium on Theory of computing. ACM. 2000, pages 705–714
[3] Andris Ambainis. "A new protocol and lower bounds for quantum coin flipping". In: Proceedings of the thirty-third annual ACM symposium on Theory of computing. ACM. 2001, pages 134–142.

Ambainis Quantum Coin Flipping

$|\phi_{x,a}\rangle$

b

$$|\phi_{a,x}\rangle = \begin{cases} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) & a = 0, x = 0 \\ \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) & a = 0, x = 1 \\ \frac{1}{\sqrt{2}}(|0\rangle + |2\rangle) & a = 1, x = 0 \\ \frac{1}{\sqrt{2}}(|0\rangle - |2\rangle) & a = 1, x = 1 \end{cases}$$

$c = a \oplus b$

Ambainis's coin flipping protocol:

1. Alice selects x ∈ {0, 1} and a ∈ {0, 1} uniformly at random and sends $|\phi_{a,x}\rangle$ to Bob.
2. Bob selects b ∈ {0, 1} uniformly at random and sends b to Alice.
3. Alice sends a and x to Bob.
4. Bob verifies the state he received from Alice in step 1. is $|\phi_{a,x}\rangle$, if it is not the case then he declares that Alice has been cheating and aborts the protocol.
5. Both players return the outcome c = a ⊕ b

Quantum Coin Flipping Security

How can Bob bias the protocol?

Bob needs to learn Alice's bit from the state, so he can bias the final bit

What's the best possible quantum strategy to do that?

The state corresponding to Alice's choice of a = 0: $\rho_0 = \frac{1}{2}(|\psi_{0,0}\rangle\langle\psi_{0,0}| + |\psi_{1,0}\rangle\langle\psi_{1,0}|)$

The state corresponding to Alice's choice of a = 1: $\rho_1 = \frac{1}{2}(|\psi_{1,1}\rangle\langle\psi_{1,1}| + |\psi_{0,1}\rangle\langle\psi_{0,1}|)$

If Bob distinguishes between these two, he can win. How well we can distinguish between two states?

Remember we saw this problem in the first lecture?

Holevo-Helstrom bound: The optimal probability of distinguishing between two density matrices which have been picked with equal probability, is given by this bound:

$$P_{disc}^{opt} = \frac{1}{2} + \frac{1}{4}\|\rho_1 - \rho_2\|_{tr}$$

Calculate it as an exercise!

Quantum Coin Flipping…

How about Alice?

Bounding success probability of Alice is harder because she can prepare arbitrary states (for instance entangled with other information), which she can use later to cheat, after Bob reveals.

But again, you can show that for the best symmetric density matrix Alice can at most cheat with probability ¾

Can we do much better? Can we design a quantum protocol that achieves arbitrary small bias using quantum information?

No! perfectly secure strong coin-flipping is also impossible for quantum protocols.

Kitaev's bound for strong coin flipping:

The smallest bias any strong coin flipping protocol can achieve is

$$\varepsilon = \frac{\sqrt{2}-1}{2} \approx 0.207.$$

The proof is not easy… It relies on Linear Programming (LP) and Semidefinite Programming (SDP).

André Chailloux and Iordanis Kerenidis. "Optimal quantum strong coin flipping". In: Foundations of Computer Science, 2009. FOCS'09. 50th Annual IEEE Symposium on. IEEE. 2009, pages 527–533.

Weak Quantum Coin Flipping

If the choice of Alice and Bob are predetermined (Let's say Alice always prefers 0), then we have a weaker (easier to achieve) version of the protocol called "weak coin flipping"

It's still impossible classically!

It has been shown that weak quantum coin flipping, with arbitrarily small (but non-zero) bias ε, is possible (by Mochon[1] in 2007)

But the protocol that achieves this arbitrary small bias is complicated and requires multiple rounds that scales exponentially with $1/\varepsilon$

Designing concrete protocols with arbitrary small bias is still open research problem (Solved by Arora et al. [2] (2019) for protocols with bias around 1/10)

Interesting research in quantum coin flipping continues…

Quantum coin-flipping has also implemented in the lab [3,4]

[1] Carlos Mochon. "Quantum weak coin flipping with arbitrarily small bias". In: arXiv preprint arXiv:0711.4114 (2007)
[2] Arora AS, Roland J, Weis S. Quantum weak coin flipping. InProceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing 2019 (pp. 205-216)
[3] Pappa, A., Jouguet, P., Lawson, T., Chailloux, A., Legré, M., Trinkler & Diamanti, E. (2014). Experimental plug and play quantum coin flipping. Nature communications
[4] Bozzio, M., Chabaud, U., Kerenidis, I., & Diamanti, E. (2020). Quantum weak coin flipping with a single photon. PRA

Quantum Software Lab

THE UNIVERSITY of EDINBURGH
informatics

Quantum Cryptography (Special Topics):

New assumptions for Quantum Cryptography

Mina Doosti

Okinawa School in Physics: From quantum key distribution to the quantum internet (OSP2025)

OIST, Okinawa

September 2025

Outline:

- Cryptography from different set of assumptions
- Crypro Imaginarium
- Quantum Cryptography with minimal quantum assumptions
- Quantum Cryptography with hardware/physical assumptions
- Quantum Cryptography from hardness of learning assumptions

Quantum Cryptography with minimal quantum assumptions

Minimal assumptions in cryptography

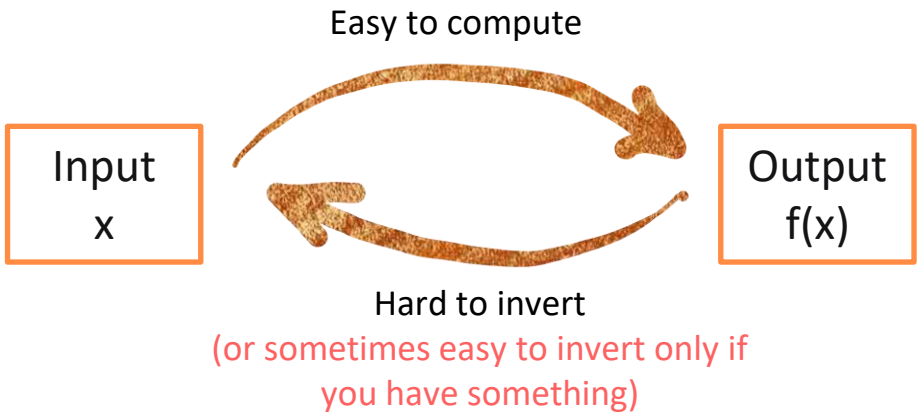
Cryptography is always about assumptions!

Cryptographers tend to be as paranoid as possible, and use as less assumption as possible

Cryptography holy grail: Is there one assumption based on which we can construct cryptography?

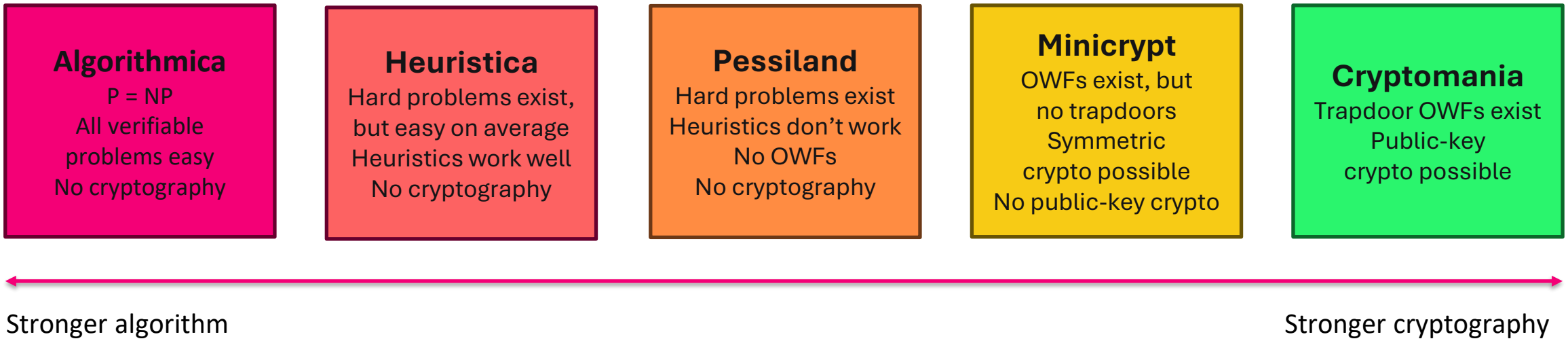
Yes! This assumption is One-Way Function (OWF)

One-way functions (OWFs) are functions that are easy to compute one-way, and hard to invert.



Impagliazzo's 5 worlds

Complexity worlds and cryptographic consequences



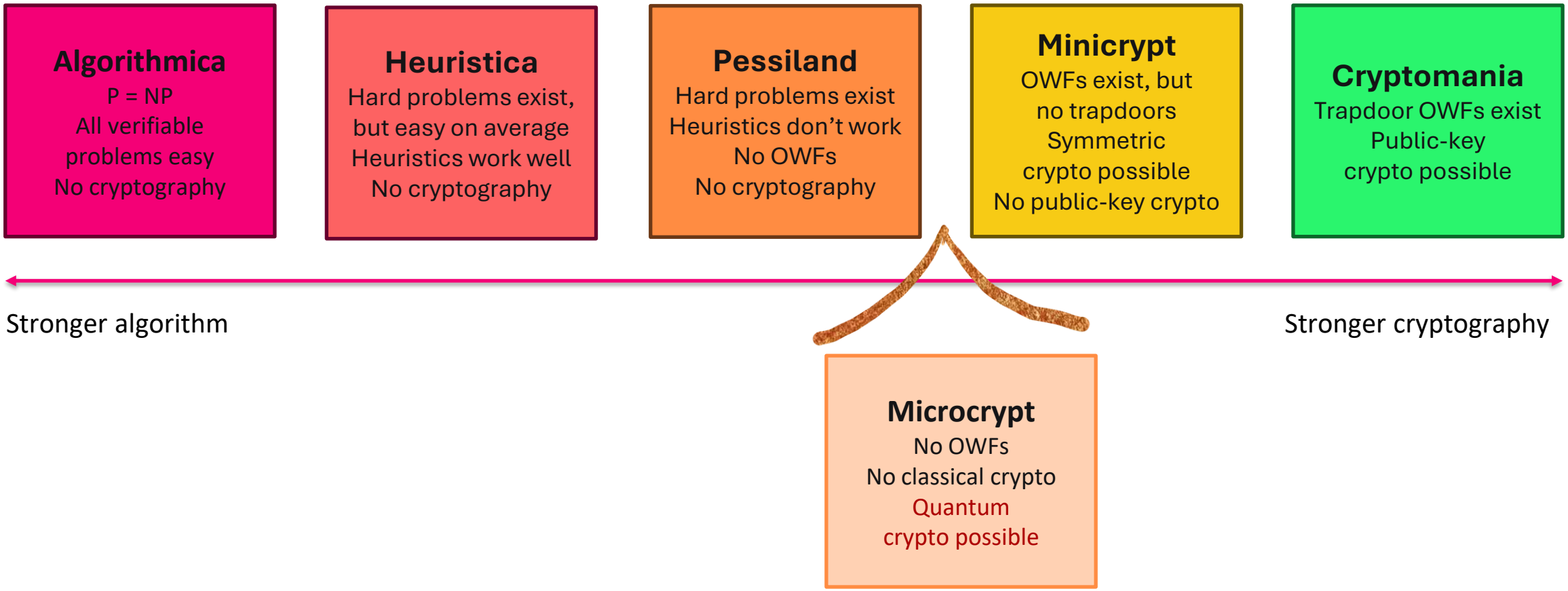
We believed No OWF, NO Cryptography!

This turned out not to be the case in the quantum world!

There can exist a world where P=NP, but we can still have a quantum minimal assumptions that are sufficient for cryptography [Kretchmer 19]!

Kretschmer, W., 2021. Quantum pseudorandomness and classical complexity. *arXiv preprint arXiv:2103.09320*.

Quantum Imaginarium!



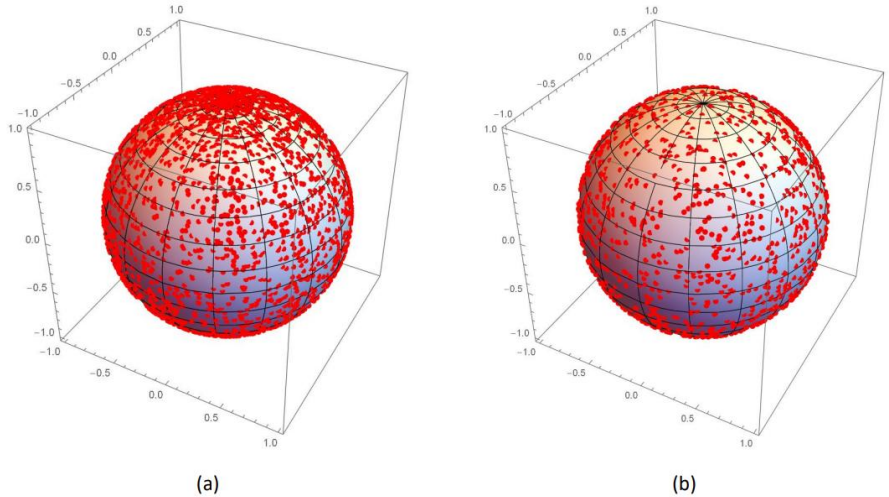
Kretschmer, W., 2021. Quantum pseudorandomness and classical complexity. *arXiv preprint arXiv:2103.09320*.

Quantum Pseudorandomness

True randomness is almost impossible to build classically!
You can sample things at random, but good randomness needs exponential cost.
But… if you have OWF, you can build Pseudorandom Number Generator (PRG), and Pseudorandom Function (PRF)
These are objects that looks random to computationally bounded adversaries, but are efficient to build

In quantum, the true randomness over the set of states is given by "Haar measure"

But generating Haar-random states are is also exponential.



Approximation of Haar randomness

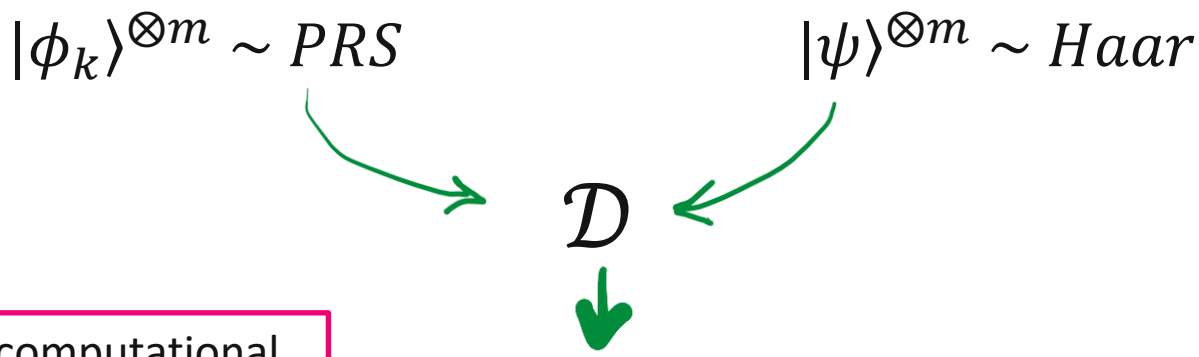
Statistical: t-design

Computational: PRS/PRU

Ji Z, Liu YK, Song F. Pseudorandom quantum states. In Advances in Cryptology–CRYPTO 2018: August 19–23, 2018.

Quantum Pseudorandomness

Pseudorandom quantum states/unitaries [Ji, Liu, Song 2018]: Set of keyed states/unitaries that can be generated efficiently and are computationally indistinguishable to Haar-random states/unitaries



This indistinguishability is a computational version of no-cloning theorem

Created very interesting body of research in cryptography, complexity theory, and physics (quantum gravity) over the past 6-7 years

Ji Z, Liu YK, Song F. Pseudorandom quantum states. In Advances in Cryptology–CRYPTO 2018: August 19–23, 2018.

PRS definition (more formal)

Definition 2 (Pseudorandom Quantum States (PRS's)). *Let $\mathcal{H}$ be a Hilbert space and $\mathcal{K}$ the key space. $\mathcal{H}$ and $\mathcal{K}$ depend on the security parameter κ. A keyed family of quantum states $\{|\phi_k\rangle \in \mathrm{S}(\mathcal{H})\}_{k\in\mathcal{K}}$ is* ***pseudorandom****, if the following two conditions hold:*

1. (***Efficient generation***). *There is a polynomial-time quantum algorithm G that generates state $|\phi_k\rangle$ on input k. That is, for all $k \in \mathcal{K}$, $G(k) = |\phi_k\rangle$.*

2. (***Pseudorandomness***). *Any polynomially many copies of $|\phi_k\rangle$ with the same random $k \in \mathcal{K}$ is* ***computationally indistinguishable*** *from the same number of copies of a Haar random state. More precisely, for any efficient quantum algorithm $\mathcal{A}$ and any $m \in \mathrm{poly}(\kappa)$,*

$$\left| \Pr_{k\leftarrow\mathcal{K}}\left[\mathcal{A}(|\phi_k\rangle^{\otimes m}) = 1\right] - \Pr_{|\psi\rangle\leftarrow\mu}\left[\mathcal{A}(|\psi\rangle^{\otimes m}) = 1\right] \right| = \mathrm{negl}(\kappa),$$

where μ is the Haar measure on $\mathrm{S}(\mathcal{H})$.

Note: There are also other "Pseudo-" stuff! Pseudo-entanglement , Pseudo-magic
It's interesting to look at quantum resources from a "computational" perspective

Ji Z, Liu YK, Song F. Pseudorandom quantum states. In Advances in Cryptology–CRYPTO 2018: August 19–23, 2018.

Crypto from Quantum Pseudorandomness

Based on PRS we can construct:

- Private-key Quantum Money (JLS paper)
- Quantum bit commitment, MAC, SMPC
- Digital Signature,
- …

Cryptography from Pseudorandom Quantum States

Prabhanjan Ananth, Luowen Qian, Henry Yuen

Pseudorandom states, introduced by Ji, Liu and Song (Crypto'18), are efficiently-computable quantum states that are computationally indistinguishable from Haar-random states. One-way functions imply the existence of pseudorandom states, but Kretschmer (TQC'20) recently constructed an oracle relative to which there are no one-way functions but pseudorandom states still exist. Motivated by this, we study the intriguing possibility of basing interesting cryptographic tasks on pseudorandom states.

We construct, assuming the existence of pseudorandom state generators that map a \lambda-bit seed to a \omega(\log\lambda)-qubit state, (a) statistically binding and computationally hiding commitments and (b) pseudo one-time encryption schemes. A consequence of (a) is that pseudorandom states are sufficient to construct maliciously secure multiparty computation protocols in the dishonest majority setting.

Our constructions are derived via a new notion called pseudorandom function-like states (PRFS), a generalization of pseudorandom states that parallels the classical notion of pseudorandom functions. Beyond the above two applications, we believe our notion can effectively replace pseudorandom functions in many other cryptographic applications.

On black-box separations of quantum digital signatures from pseudorandom states

Andrea Coladangelo, Saachi Mutreja

It is well-known that digital signatures can be constructed from one-way functions in a black-box way. While one-way functions are essentially the minimal assumption in classical cryptography, this is not the case in the quantum setting. A variety of qualitatively weaker and inherently quantum assumptions (e.g. EFI pairs, one-way state generators, and pseudorandom states) are known to be sufficient for non-trivial quantum cryptography.

While it is known that commitments, zero-knowledge proofs, and even multiparty computation can be constructed from these assumptions, it has remained an open question whether the same is true for quantum digital signatures schemes (QDS). In this work, we show that there *does not* exist a black-box construction of a QDS scheme with classical signatures from pseudorandom states with linear, or greater, output length. Our result complements that of Morimae and Yamakawa (2022), who described a *one-time* secure QDS scheme with classical signatures, but left open the question of constructing a standard *multi-time* secure one.

But so far, almost all constructions we have for PRS are based on quantum-secure PRF (or OWF)

Also, constructions for PRU was an open problem till last year!

How to Construct Random Unitaries

Authors: Fermi Ma, Hsin-Yuan Huang | Authors Info & Claims

STOC '25: Proceedings of the 57th Annual ACM Symposium on Theory of Computing • Pages 806 - 809
https://doi.org/10.1145/3717823.3718254

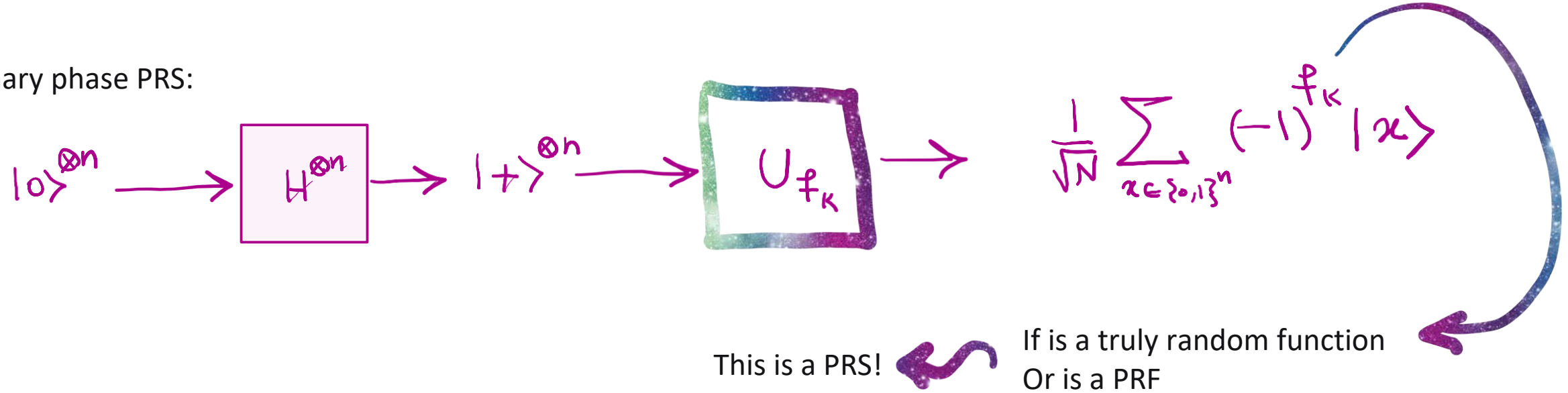
Simple Constructions of Linear-Depth t-Designs and Pseudorandom Unitaries

Publisher: IEEE | Cite This | PDF

Tony Metger ; Alexander Poremba ; Makrand Sinha ; Henry Yuen **All Authors**

Let's see one construction of PRS

Binary phase PRS:



This is a PRS!

If is a truly random function
Or is a PRF

How?

$$\rho_\mu = \mathop{\mathbb{E}}_{\mu} [(|\psi\rangle\langle\psi|)^{\otimes m}] = \int (|\psi\rangle\langle\psi|)^{\otimes m} d\mu$$

$$\rho_f = \mathop{\mathbb{E}}_{f} [|\psi_f\rangle\langle\psi_f|]$$

$$\rho_{PRF} = \mathop{\mathbb{E}}_{K} [|\psi_{f_K}\rangle\langle\psi_{f_K}|]$$

These are all close (wrt security parameter) in trace distance

EFI Pairs

It's a pair of states

E F I

Efficiently generatable

Statistically Far

Computationally Indistinguishable

Why are they important?

Quantum bit commitment
(computationally hiding, statistically binding)

Multi-party computation

[Submitted on 9 Sep 2022 (v1), last revised 24 Nov 2022 (this version, v2)]

On the computational hardness needed for quantum cryptography

Zvika Brakerski, Ran Canetti, Luowen Qian

In the classical model of computation, it is well established that one-way functions (OWF) are minimal for computational cryptogra
cryptographic application that cannot be realized with respect to computationally unbounded adversaries. In the quantum setting,
(Kretschmer 2021; Ananth et al., Morimae and Yamakawa 2022), and the question of whether such a minimal primitive exists rem
We consider EFI pairs -- efficiently samplable, statistically far but computationally indistinguishable pairs of (mixed) quantum state
equivalence between EFI pairs and statistical commitment schemes, we show that EFI pairs are necessary for a large class of qu
construct EFI pairs from minimalistic versions of commitments schemes, oblivious transfer, and general secure multiparty comput
essentially any non-trivial language. We also construct quantum computational zero knowledge (QCZK) proofs for all of QIP fro
This suggests that, for much of quantum cryptography, EFI pairs play a similar role to that played by OWFs in the classical setting
serve as a linchpin for demonstrating equivalence between primitives.

Brakerski, Zvika, Ran Canetti, and Luowen Qian. "On the computational hardness needed for quantum cryptography." *arXiv preprint arXiv:2209.04101* (2022).

EFI and pseudo-stuff!

Pseudo-entangled states

EFI pairs

[Submitted on 11 Jun 2024 (v1), last revised 10 Oct 2024 (this version, v2)]

Pseudo-Entanglement is Necessary for EFI Pairs

Manuel Goulão, David Elkouss

Regarding minimal assumptions, most of classical cryptography is known to depend on the existence of One-Way Functions (OWFs). However, recent evidence has shown that this is not the case when considering quantum resources. Besides the well known unconditional security of Quantum Key Distribution, it is now known that computational cryptography may be built on weaker primitives than OWFs, e.g., pseudo-random states [JLS18], one-way state generators [MY23], or EFI pairs of states [BCQ23]. We consider a new quantum resource, pseudo-entanglement, and show that the existence of EFI pairs, one of the current main candidates for the weakest computational assumption for cryptography (necessary for commitments, oblivious transfer, secure multi-party computation, computational zero-knowledge proofs), implies the existence of pseudo-entanglement, as defined by [ABF+24, ABV23] under some reasonable adaptations. We prove this by constructing a new family of pseudo-entangled quantum states given only EFI pairs. Our result has important implications for the field of computational cryptography. It shows that if pseudo-entanglement does not exist, then most of cryptography cannot exist either. Moreover, it establishes pseudo-entanglement as a new minimal assumption for most of computational cryptography, which may pave the way for the unification of other assumptions into a single primitive. Finally, pseudo-entanglement connects physical phenomena and efficient computation, thus, our result strengthens the connection between cryptography and the physical world.

Any quantum pseudo-resource

EPFI pairs

Q commitment

[Submitted on 21 Apr 2025]

Quantum pseudoresources imply cryptography

Alex B. Grilo, Álvaro Yángüez

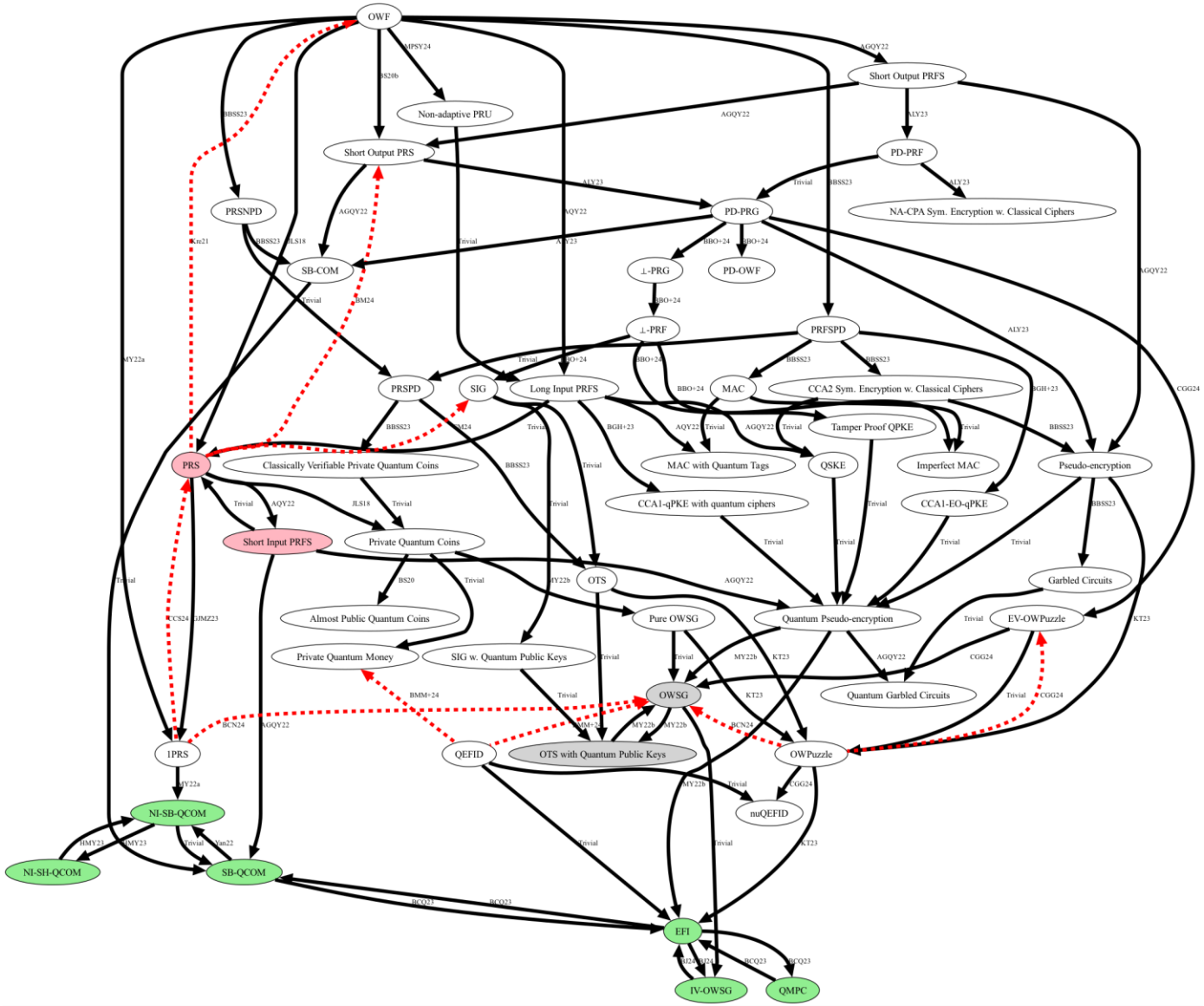
While one-way functions (OWFs) serve as the minimal assumption for computational cryptography in the classical setting, in quantum cryptography, we have even weaker cryptographic assumptions such as pseudo-random states, and EFI pairs, among others. Moreover, the minimal assumption for computational quantum cryptography remains an open question. Recently, it has been shown that pseudoentanglement is necessary for the existence of quantum cryptography (Goulão and Elkouss 2024), but no cryptographic construction has been built from it.

In this work, we study the cryptographic usefulness of quantum pseudoresources -- a pair of families of quantum states that exhibit a gap in their resource content yet remain computationally indistinguishable. We show that quantum pseudoresources imply a variant of EFI pairs, which we call EPFI pairs, and that these are equivalent to quantum commitments and thus EFI pairs. Our results suggest that, just as randomness is fundamental to classical cryptography, quantum resources may play a similarly crucial role in the quantum setting.

Finally, we focus on the specific case of entanglement, analyzing different definitions of pseudoentanglement and their implications for constructing EPFI pairs. Moreover, we propose a new cryptographic functionality that is intrinsically dependent on entanglement as a resource.

Goulão, Manuel, and David Elkouss. "Pseudo-entanglement is necessary for EFI pairs." *arXiv preprint arXiv:2406.06881* (2024).
Grilo, Alex B., and Álvaro Yángüez. "Quantum pseudoresources imply cryptography." *arXiv preprint arXiv:2504.15025* (2025).

The landscape of quantum minimal assumptions

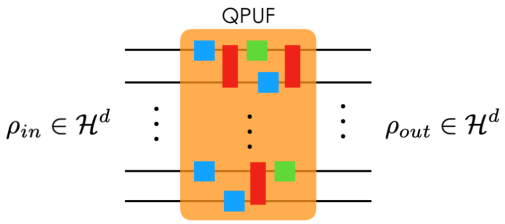


It's called "Microcrypt Zoo"
You can find it here:
https://sattath.github.io/microcrypt-zoo/

Quantum Cryptography based on hardware assumptions

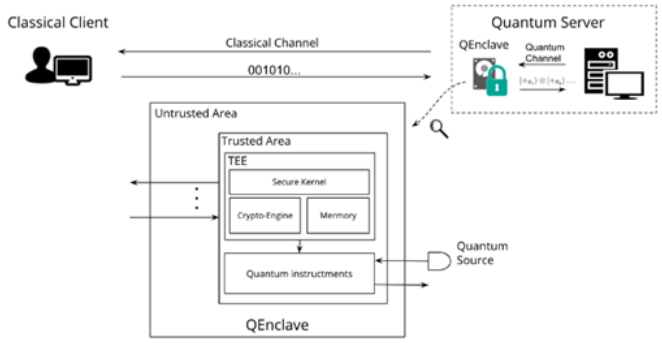
What sets of hardware assumptions do we have?

Quantum Hardware Assumptions



Quantum PUFs

Arapinis, M., Delavar, M., Doosti, M., & Kashefi, E. (2021). Quantum physical unclonable functions: Possibilities and impossibilities. *Quantum*, *5*, 475.



Quantum Enclave (QTEE)

Ma, Y., Kashefi, E., Arapinis, M., Chakraborty, K., & Kaplan, M. (2022). QEnclave-A practical solution for secure quantum cloud computing. npj Quantum Information, 8(1), 128

Quantum One-Time Memory

Broadbent, A., Gharibian, S., & Zhou, H. S. (2021). Towards quantum one-time memories from stateless hardware. Quantum, 5, 429.

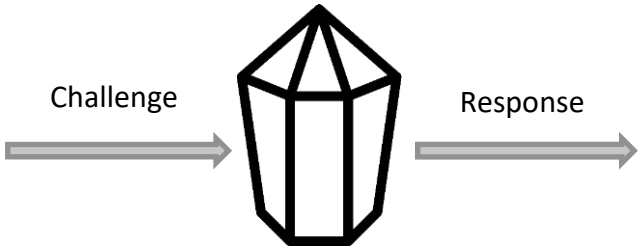
Noisy Quantum Storage Model (NQSM)

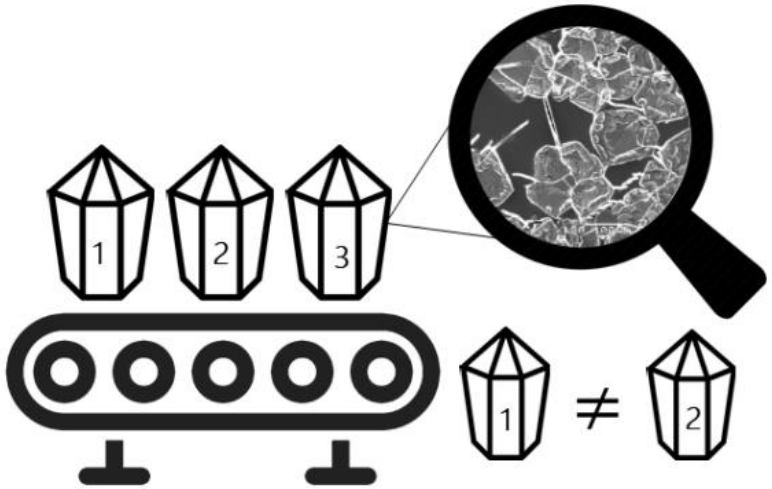
Wehner, Stephanie, Christian Schaffner, and Barbara M. Terhal. "Cryptography from noisy storage." *Physical Review Letters* 100, no. 22 (2008): 220502.

Physical Unclonability

No-cloning of quantum states is not the only type of unclonability we know!

Physical Unclonable Functions (PUF)

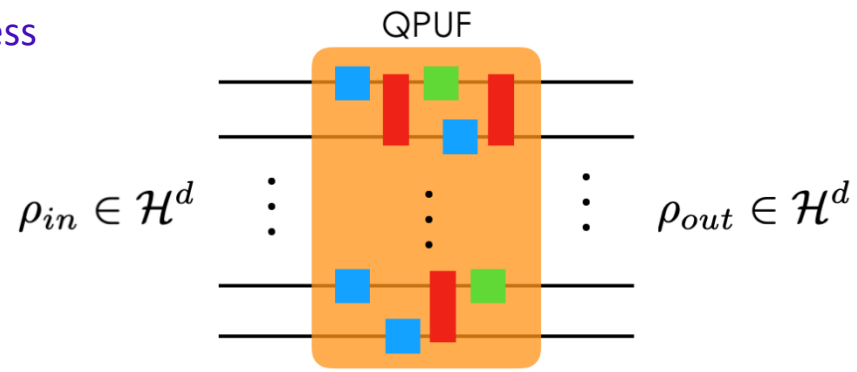


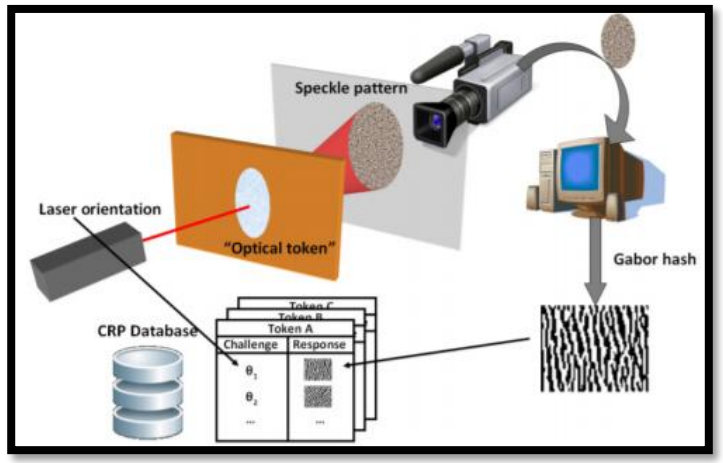


Unique physical behavior

Quantum Physical Unclonable Functions (QPUF)

Unclonable (hard to clone) quantum process with quantum inputs and outputs



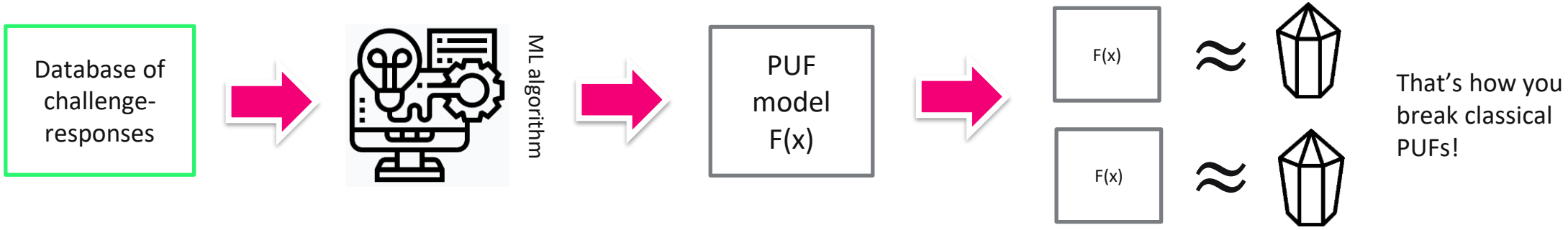


[4] Arapinis, M., Delavar, **M., Doosti**, M., & Kashefi, E. (2021). Quantum physical unclonable functions: Possibilities and impossibilities. *Quantum*, *5*, 475.

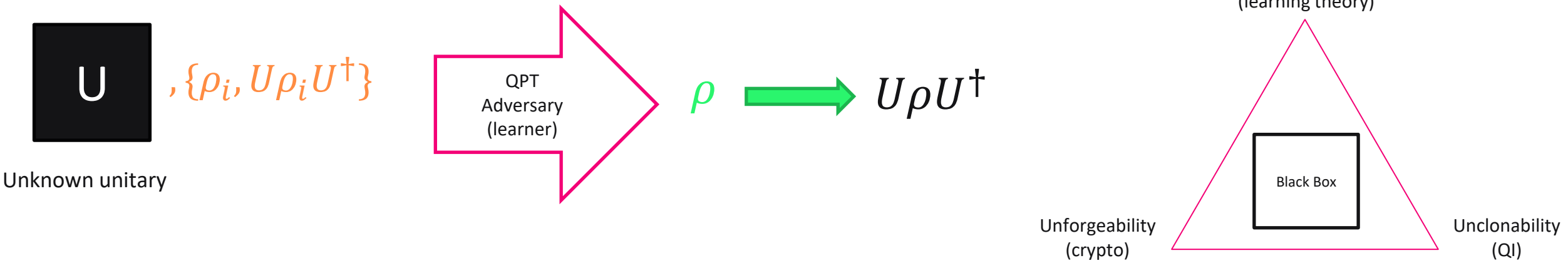
Great! So, what's the problem?

Breaking Physical Unclonability

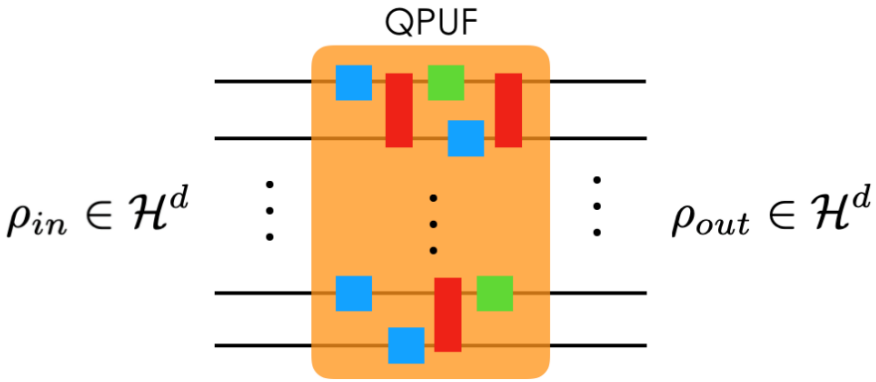
How an unclonable hardware becomes clonable?!

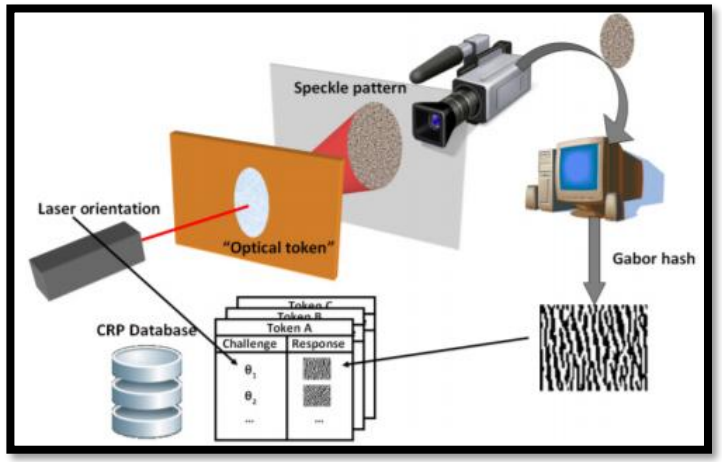


How to formalize the quantum hardware assumption of unclonability?



Quantum PUF





Unlike classical PUFs, general QPUFs can be proven to be unforgeable/unclonable against quantum adversaries, under minimal hardware assumptions.

PRU and Quantum PUFs are interestingly related!

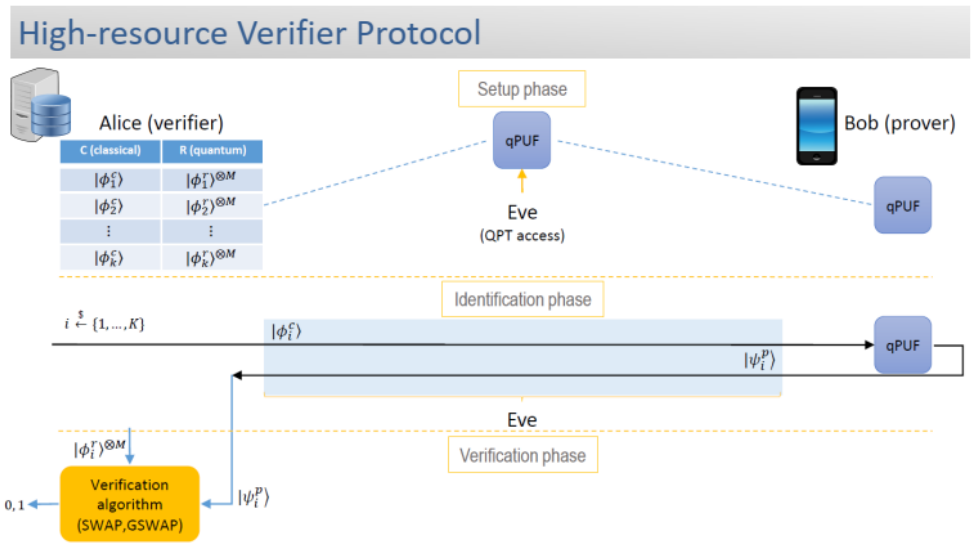
On the Connection Between Quantum Pseudorandomness and Quantum Hardware Assumptions

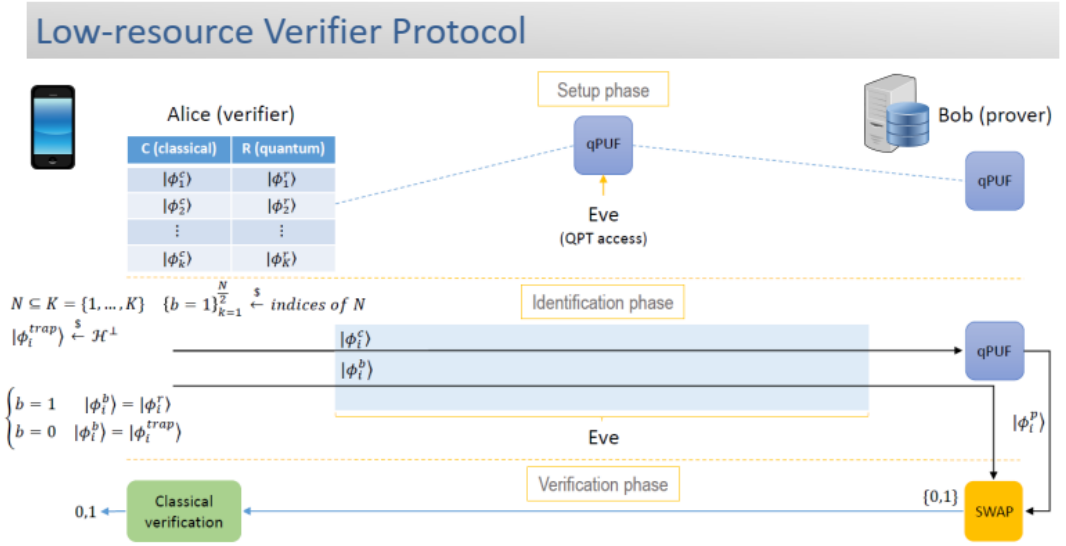
Mina Doosti, Niraj Kumar, Elham Kashefi, Kaushik Chakraborty

This paper, for the first time, addresses the questions related to the connections between the quantum pseudorandomness and quantum hardware assumptions, specifically quantum physical unclonable functions (qPUFs). Our results show that the efficient pseudorandom quantum states (PRS) are sufficient to construct the challenge set for the universally unforgeable qPUF, improving the previous existing constructions that are based on the Haar-random states. We also show that both the qPUFs and the quantum pseudorandom unitaries (PRUs) can be constructed from each other, providing new ways to obtain PRS from the hardware assumptions. Moreover, we provide a sufficient condition (in terms of the diamond norm) that a set of unitaries should have to be a PRU in order to construct a universally unforgeable qPUF, giving yet another novel insight into the properties of the PRUs. Later, as an application of our results, we show that the efficiency of an existing qPUF-based client-server identification protocol can be improved without losing the security requirements of the protocol.

Arapinis, M., Delavar, **M., Doosti**, M., & Kashefi, E. (2021). Quantum physical unclonable functions: Possibilities and impossibilities. *Quantum*, *5*, 475.

QPUF-based Identification Protocols



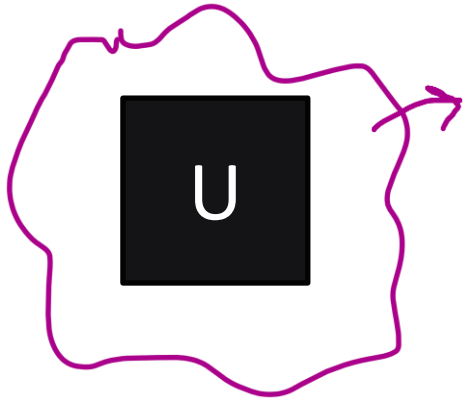


- Both protocols have exponential security with polynomial number of rounds
- Different types of test algorithms can be used
- The second protocol has classical verification and one-way quantum communication

Building a real QPUF is hard!
Protocols require large quantum memory (so… experimentalists won't like it)

Doosti, M., Kumar, N., Delavar, M., & Kashefi, E. (2021). Client-server identification protocols with quantum PUF. ACM Transactions on Quantum Computing, 2(3), 1-40.

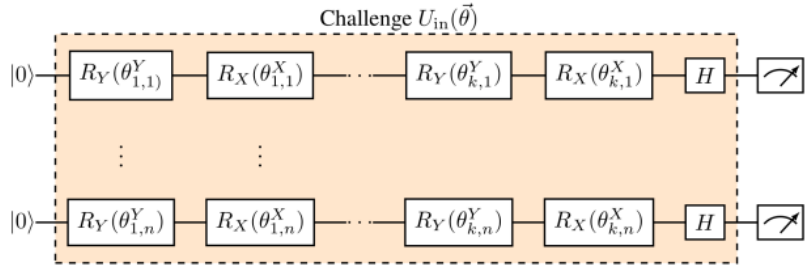
More crypto-learning relations!



Noisy black box

The output is the statistics instead of the quantum states

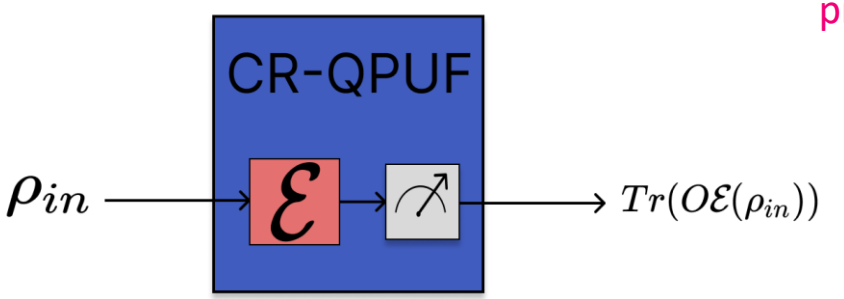
Classical readout of quantum PUFs (CR-QPUFs) [1]:



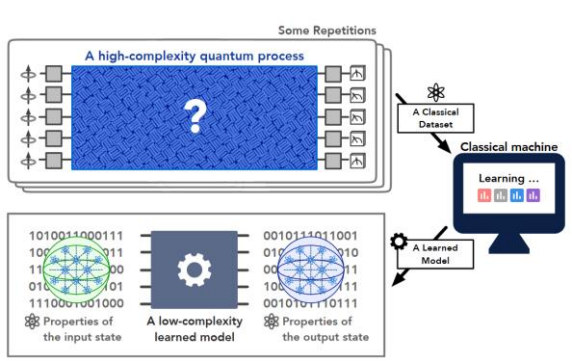
The problem is…
They are broken (using ML) [1]

But this is a very simple circuit… What if we keep this model, but the circuit it more complicated?

CR-QPUF in Statistical Query (SQ) model



We defined and studied the problem of learning quantum processes from statistical queries [2].



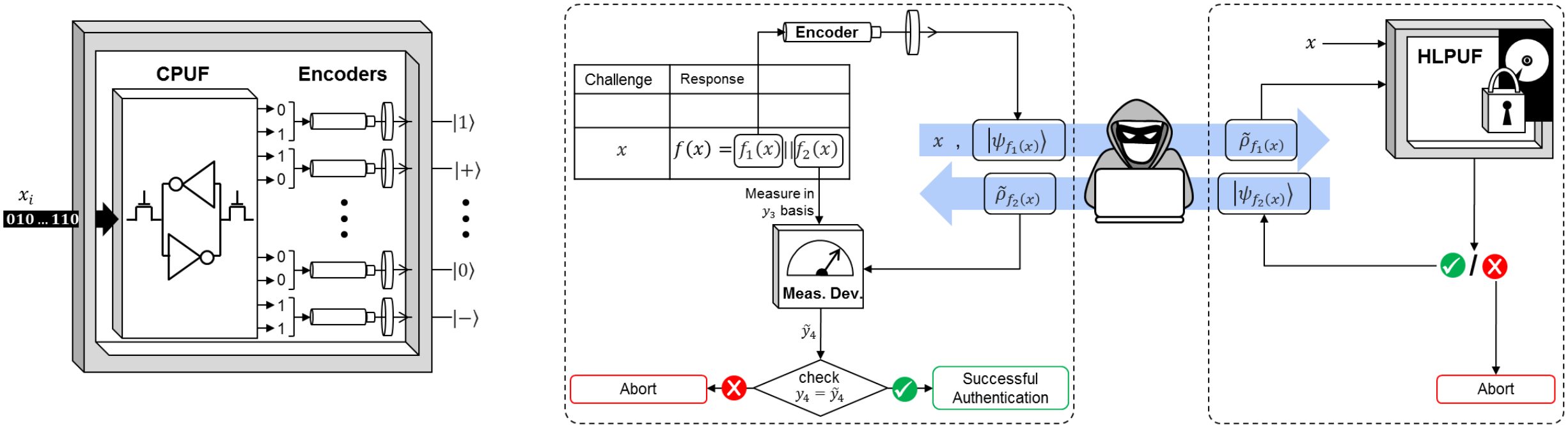
New algorithm to learn quantum processes

This family of QPUFs are learnable (except some restricted cases, which are probably not efficient) and hence, not good candidates for unclonable processes.

[1] Pappa, Anna, Niklas Pirnay, and Jean-Pierre Seifert. arXiv:2112.06661 (2021).
[2] Wadhwa, Chirag, and Mina Doosti. "Learning Quantum Processes with Quantum Statistical Queries." *arXiv preprint arXiv:2310.02075* (2023).

Can we design authentication (with hardware assumptions) in a way that is both practical and provably secure?

Hybrid-Locked-PUF authentication protocol

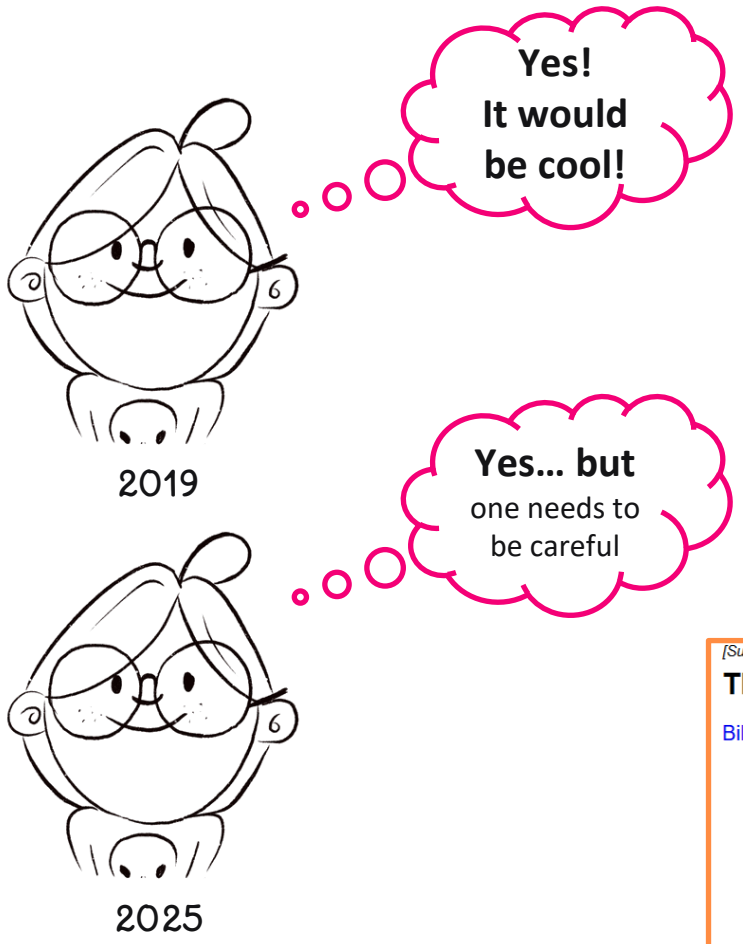


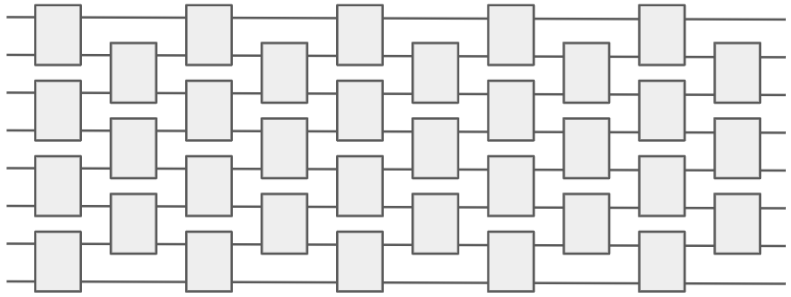
- Provably quantum secure protocol (unbounded adversary during protocol)
- The protocol shows an exponential quantum communication advantage.
- Implementable with only QKD technology.
- Information-theoretic challenge re-usability.

Chakraborty, K., **Doosti, M.**, Ma, Y., Wadhwa, C., Arapinis, M., & Kashefi, E. (2023). Quantum Lock: A Provable Quantum Communication Advantage. Quantum, 7, 1014.

Quantum Cryptography from (hardness of) learning

Cryptography from Learning Theory?





Hard to learn after certain depth,
even for quantum computers!

[Submitted on 21 Apr 2025]

The Hardness of Learning Quantum Circuits and its Cryptographic Applications

Bill Fefferman, Soumik Ghosh, Makrand Sinha, Henry Yuen

We show that concrete hardness assumptions about learning or cloning the output state of a random quantum circuit can be used as the foundation for secure quantum cryptography. In particular, under these assumptions we construct secure one-way state generators (OWSGs), digital signature schemes, quantum bit commitments, and private key encryption schemes. We also discuss evidence for these hardness assumptions by analyzing the best-known quantum learning algorithms, as well as proving black-box lower bounds for cloning and learning given state preparation oracles.

Our random circuit-based constructions provide concrete instantiations of quantum cryptographic primitives whose security do not depend on the existence of one-way functions. The use of random circuits in our constructions also opens the door to NISQ-friendly quantum cryptography. We discuss noise tolerant versions of our OWSG and digital signature constructions which can potentially be implementable on noisy quantum computers connected by a quantum network. On the other hand, they are still secure against noiseless quantum adversaries, raising the intriguing possibility of a useful implementation of an end-to-end cryptographic protocol on near-term quantum computers. Finally, our explorations suggest that the rich interconnections between learning theory and cryptography in classical theoretical computer science also extend to the quantum setting.

I hope you had fun learning quantum cryptography!

Thank you!