Impact of quantum computer on Impagliazzo's five worlds

Samuel Bouaziz--Ermann
Based on joint work with Minki Hhan, Quoc-Huy Vu
and Garazi Muguruza

Supervised by Alex Bredariol Grilo and Damien Vergnaud
Work In Progress

April 24, 2025

SORBONNE UNIVERSITÉ

The plan

1. Classical Assumptions
2. Quantum Assumptions
3. Our result
4. High level idea of the proof
5. Conclusion

Minimal assumption for classical cryptography

One-Way Functions

A function $F : \{0,1\}^n \to \{0,1\}^n$ is a One-Way Function (OWF) if:

1. $F(x)$ can be computed efficiently.
2. Given $y = F(x)$, it is hard to compute x.

Minimal assumption for classical cryptography

One-Way Functions

A function $F : \{0,1\}^n \to \{0,1\}^n$ is a One-Way Function (OWF) if:

1. $F(x)$ can be computed efficiently.
2. Given $y = F(x)$, it is hard to compute x.

One-Way Functions are minimal for cryptography

- Most advanced cryptographic schemes require one-way functions.
- For example, a hash function has to be a one-way function.
- There is nothing (interesting) weaker.

Some results about classical cryptography

Theorem

$$\exists OWF \Rightarrow \mathrm{P} \neq \mathrm{NP}$$

Some results about classical cryptography

Theorem

$$\exists OWF \Rightarrow \mathrm{P} \neq \mathrm{NP}$$

Theorem (Goldreich-Levin)

$$\exists OWF \Leftrightarrow \exists PRNG$$

Some results about classical cryptography

Theorem

$$\exists OWF \Rightarrow \mathrm{P} \neq \mathrm{NP}$$

Theorem (Goldreich-Levin)

$$\exists OWF \Leftrightarrow \exists PRNG$$

Theorem

$$\exists PKE \Rightarrow \exists OWF$$

Some results about classical cryptography

Theorem

$$\exists OWF \Rightarrow \mathsf{P} \neq \mathsf{NP}$$

Theorem (Goldreich-Levin)

$$\exists OWF \Leftrightarrow \exists PRNG$$

Theorem

$$\exists PKE \Rightarrow \exists OWF$$

Theorem ([IR89])

$$\exists OWF \not\Rightarrow \exists PKE$$

Black-box proof

A word on achieving possibility and impossibility results.

Black-box proof

A word on achieving possibility and impossibility results.

Black-box constructions

They are the most natural class of constructions.

Black-box proof

A word on achieving possibility and impossibility results.

Black-box constructions

They are the most natural class of constructions.

A black-box construction of A from B means that:

- The construction of A from B does not use the “code” of B.

Black-box proof

A word on achieving possibility and impossibility results.

Black-box constructions

They are the most natural class of constructions.
A black-box construction of A from B means that:

- The construction of A from B does not use the “code” of B.
- If an adversary breaks A, then an adversary breaks B, without using the “code” of A.

Black-box proof

A word on achieving possibility and impossibility results.

Black-box constructions

They are the most natural class of constructions.
A black-box construction of A from B means that:

- The construction of A from B does not use the "code" of B.
- If an adversary breaks A, then an adversary breaks B, without using the "code" of A.

Black-box constructions *relativizes*, meaning that for any oracle $\mathcal{O}$ such that B exists (relative to $\mathcal{O}$), then A exists (relative to $\mathcal{O}$).

Black-box proof

A word on achieving possibility and impossibility results.

Black-box constructions

They are the most natural class of constructions.
A black-box construction of A from B means that:

- The construction of A from B does not use the "code" of B.
- If an adversary breaks A, then an adversary breaks B, without using the "code" of A.

Black-box constructions *relativizes*, meaning that for any oracle $\mathcal{O}$ such that B exists (relative to $\mathcal{O}$), then A exists (relative to $\mathcal{O}$).

Black-box impossibility results

A black-box impossibility result of A from B consists of exhibiting an oracle $\mathcal{O}$ such that, relative to $\mathcal{O}$, B exists but not A.

But. . .why? 🤔

Motivation

But. . .why? 🤔

No practical use

But. . . why? 🤔
No practical use
The goal is to understand the strength of assumptions and primitives

Worlds of cryptography

Impagliazzo's five worlds [Imp95]

- **Algorithmica** $\mathsf{P} = \mathsf{NP}$.
- **Heuristica** $\mathsf{P} \neq \mathsf{NP}$ but NP problems are easy on average.
- **Pessiland** $\mathsf{P} \neq \mathsf{NP}$ but one-way functions do not exist.
- **Minicrypt** One-way functions exist, but public key cryptography is impossible.
- **Cryptomania** Public key cryptography is possible.

Quantum Computation

A n-qubit state $|\psi\rangle$ is a unitary vector of a Hilbert space ($\mathbb{C}^{2^n}$).

Quantum Computation

A n-qubit state $|\psi\rangle$ is a unitary vector of a Hilbert space ($\mathbb{C}^{2^n}$).

Operations are unitary matrices or measurements.

Quantum Computation

A n-qubit state $|\psi\rangle$ is a unitary vector of a Hilbert space ($\mathbb{C}^{2^n}$).

Operations are unitary matrices or measurements.

An algorithm can be written:

$$c_1 \quad c_2 \quad = \quad M \quad U_s \quad \cdots \quad U_0 \quad |\psi\rangle \quad |0\rangle^{\otimes m}$$

- c_1: Output
- c_2: Discarded bits
- M: Measurement
- U_s: Unitary
- U_0: Unitary
- $|\psi\rangle$: Input
- $|0\rangle^{\otimes m}$: Ancillas

Quantum Pseudorandomness

Let's dive into the quantum paradigm now and define quantum pseudorandomness.

Quantum Pseudorandomness

Let's dive into the quantum paradigm now and define quantum pseudorandomness.
But first, classical pseudorandomness.

Quantum Pseudorandomness

Let's dive into the quantum paradigm now and define quantum pseudorandomness.
But first, classical pseudorandomness.

Pseudorandom Number Generator

A function $F : \{0, 1\}^n \to \{0, 1\}^\ell$ is a Pseudorandom Number Generator (PRNG) if:

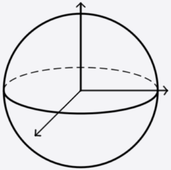
1. $F(x)$ can be computed efficiently.
2. $F(x) \approx \mathcal{U}_\ell$, when $x \leftarrow \mathcal{U}_n$.
3. $\ell > n$.

Quantum Pseudorandomness

Quantum Randomness

We can also consider quantum randomness.

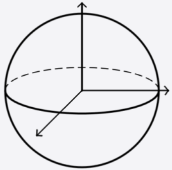
The equivalent to the uniform distribution is the *Haar measure* μ_{2^n}.



Quantum Pseudorandomness

Quantum Randomness

We can also consider quantum randomness.
The equivalent to the uniform distribution is the *Haar measure* μ_{2^n}.



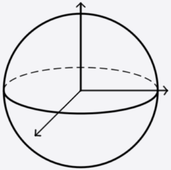
Pseudorandom Quantum States Generators

A function $F : \{0,1\}^\lambda \to \left(\mathbb{C}^2\right)^{\otimes n}$ is a Pseudorandom Quantum State generator (PRS) if:

Quantum Pseudorandomness

Quantum Randomness

We can also consider quantum randomness.
The equivalent to the uniform distribution is the *Haar measure* μ_{2^n}.



Pseudorandom Quantum States Generators

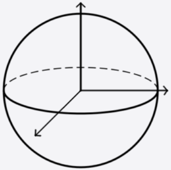
A function $F : \{0,1\}^\lambda \rightarrow \left(\mathbb{C}^2\right)^{\otimes n}$ is a Pseudorandom Quantum State generator (PRS) if:

1. $F(k)$ can be computed efficiently.

Quantum Pseudorandomness

Quantum Randomness

We can also consider quantum randomness.
The equivalent to the uniform distribution is the *Haar measure* μ_{2^n}.



Pseudorandom Quantum States Generators

A function $F : \{0,1\}^\lambda \to \left(\mathbb{C}^2\right)^{\otimes n}$ is a Pseudorandom Quantum State generator (PRS) if:

1. $F(k)$ can be computed efficiently.
2. $F(k) \approx \mu_{2^n}$, when $k \leftarrow \mathcal{U}_\lambda$.

Formal definition of PRSs

Definition (Pseudorandom quantum states [JLS18])

A keyed family of n-qubit quantum states $\{|\varphi_k\rangle\}_{k\in\{0,1\}^\lambda}$ is *pseudorandom* if the following two conditions hold:

Formal definition of PRSs

Definition (Pseudorandom quantum states [JLS18])

A keyed family of n-qubit quantum states $\{|\varphi_k\rangle\}_{k\in\{0,1\}^\lambda}$ is *pseudorandom* if the following two conditions hold:

1. **Efficient generation**. There is a QPT algorithm G such that:

$$G_\lambda(k) = |\varphi_k\rangle \, .$$

Formal definition of PRSs

Definition (Pseudorandom quantum states [JLS18])

A keyed family of n-qubit quantum states $\{|\varphi_k\rangle\}_{k\in\{0,1\}^\lambda}$ is *pseudorandom* if the following two conditions hold:

1. **Efficient generation**. There is a QPT algorithm G such that:

$$G_\lambda(k) = |\varphi_k\rangle \,.$$

2. **Pseudorandomness**. For any QPT adversary $\mathcal{A}$ and all polynomials $t(\cdot)$, we have:

$$\left| \Pr_{k\leftarrow\{0,1\}^\lambda}\left[\mathcal{A}\left(|\varphi_k\rangle^{\otimes t(\lambda)}\right)=1\right] - \Pr_{|\nu\rangle\leftarrow\mu_{2^n}}\left[\mathcal{A}\left(|\nu\rangle^{\otimes t(\lambda)}\right)=1\right]\right| \leq \mathrm{negl}(\lambda).$$

Worlds of quantum cryptography

Worlds relative to which quantum computation is possible.

- Quantum Cryptomania: Public Key Cryptography exists! (resistant to quantum attacks)

Worlds of quantum cryptography

Worlds relative to which quantum computation is possible.

- Quantum Cryptomania: Public Key Cryptography exists! (resistant to quantum attacks)
- MiniQcrypt: Quantum resistant One-Way Functions exist!

Worlds of quantum cryptography

Worlds relative to which quantum computation is possible.

- Quantum Cryptomania: Public Key Cryptography exists! (resistant to quantum attacks)
- MiniQcrypt: Quantum resistant One-Way Functions exist!
- MicroCrypt: PRSs exist!

  oblivious transfer, multi party computation, public key encryption with quantum keys, quantum one-time digital signatures, pseudo one-time pad encryption schemes, statistically binding and computationally hiding commitments and quantum computational zero knowledge proofs, bit commitments...

Relation between quantum primitives

Theorem ([JLS18])

Classical 🎲 $\Rightarrow$ *Quantum* 🎲

Relation between quantum primitives

Theorem ([JLS18])

Classical 🎲 $\Rightarrow$ *Quantum* 🎲

Theorem ([Kre21])

Quantum 🎲 $\not\Rightarrow$ *Classical* 🎲

Relation between quantum primitives

Theorem ([JLS18])

Classical 🎲 $\Rightarrow$ *Quantum* 🎲

Theorem ([Kre21])

Quantum 🎲 $\not\Rightarrow$ *Classical* 🎲

There can be quantum cryptography even if "P $=$ NP"

🤯

Different type of Quantum Pseudorandomness

PRU, PRFS, PRS, 1PRS, EFI pairs, OWSG...

Different type of Quantum Pseudorandomness

PRU, PRFS, PRS, 1PRS, EFI pairs, OWSG...

Claim

Classically, all these primitives are equivalent.

Different type of Quantum Pseudorandomness

PRU, PRFS, PRS, 1PRS, EFI pairs, OWSG...

Claim

Classically, all these primitives are equivalent.

In the quantum setting however...

The Landscape of Quantum Assumptions

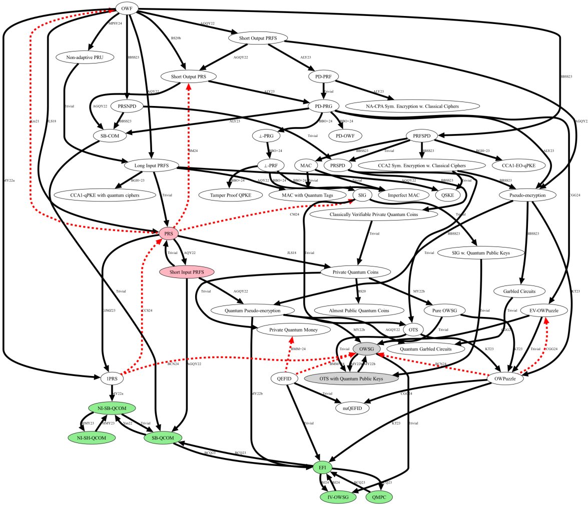
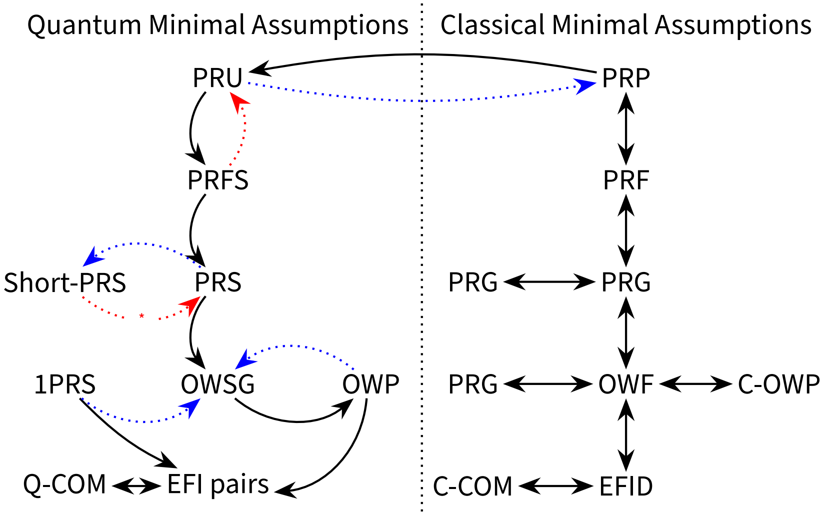


Figure: https://sattath.github.io/microcrypt-zoo/

The Landscape of Quantum Assumptions



Main result

Theorem

There exists an oracle $\mathcal{O}$ relative to which PRFSs exist, but PRUs do not.

Main result

Theorem

There exists an oracle $\mathcal{O}$ relative to which PRFSs exist, but PRUs do not.

- PRFSs are a natural generalization of PRSs.
- PRUs are *unitaries* that are indistinguishable from Haar-random *unitaries*.

Main result

Theorem

There exists an oracle $\mathcal{O}$ relative to which PRFSs exist, but PRUs do not.

- PRFSs are a natural generalization of PRSs.
- PRUs are *unitaries* that are indistinguishable from Haar-random *unitaries*.

$$\mathcal{O} = (\quad \mathcal{O}_1 \quad , \quad \mathcal{O}_2 \quad)$$

$\exists$ PRFS (for $\mathcal{O}_1$) $\quad\quad \nexists$ PRU (for $\mathcal{O}_2$)

Common Haar Function-like State Oracle

The Common Haar Function-like State Oracle (CHFS oracles) with length ℓ is a family of unitaries $\{S_x\}_{x\in\{0,1\}^*}$ such that:

Common Haar Function-like State Oracle

The Common Haar Function-like State Oracle (CHFS oracles) with length ℓ is a family of unitaries $\{S_x\}_{x\in\{0,1\}^*}$ such that:

$$S_x : \begin{cases} |0\rangle \mapsto |\phi_x\rangle\,, \\ |\phi_x\rangle \mapsto |0\rangle\,, \\ |\psi\rangle \mapsto |\psi\rangle\,, & \text{if } |\psi\rangle \notin \mathrm{span}(|0\rangle\,, |\phi_x\rangle), \end{cases}$$

where $|\phi_x\rangle$ is a predetermined Haar-random state of length $\ell(|x|)$.

Common Haar Function-like State Oracle

The Common Haar Function-like State Oracle (CHFS oracles) with length ℓ is a family of unitaries $\{S_x\}_{x\in\{0,1\}^*}$ such that:

$$S_x : \begin{cases} |0\rangle \mapsto |\phi_x\rangle\,, \\ |\phi_x\rangle \mapsto |0\rangle\,, \\ |\psi\rangle \mapsto |\psi\rangle\,, \quad \text{if } |\psi\rangle \notin \text{span}(|0\rangle\,, |\phi_x\rangle), \end{cases}$$

where $|\phi_x\rangle$ is a predetermined Haar-random state of length $\ell(|x|)$.

Claim

PRFSs exist relative to $\mathcal{O}_1$ = the CHFS oracles.

Common Haar Function-like State Oracle

The Common Haar Function-like State Oracle (CHFS oracles) with length ℓ is a family of unitaries $\{S_x\}_{x\in\{0,1\}^*}$ such that:

$$S_x : \begin{cases} |0\rangle \mapsto |\phi_x\rangle\,, \\ |\phi_x\rangle \mapsto |0\rangle\,, \\ |\psi\rangle \mapsto |\psi\rangle\,, \quad \text{if } |\psi\rangle \notin \text{span}(|0\rangle\,, |\phi_x\rangle), \end{cases}$$

where $|\phi_x\rangle$ is a predetermined Haar-random state of length $\ell(|x|)$.

Claim

PRFSs exist relative to $\mathcal{O}_1$ = the CHFS oracles.

Now let's rule out PRUs!

Definition of PRUs

Definition (Pseudorandom unitaries [JLS18])

A keyed family of n-qubit unitaries $\{U_k\}_{k\in\{0,1\}^\lambda}$ is *pseudorandom* if the following two conditions hold:

Definition of PRUs

Definition (Pseudorandom unitaries [JLS18])

A keyed family of n-qubit unitaries $\{U_k\}_{k\in\{0,1\}^\lambda}$ is *pseudorandom* if the following two conditions hold:

1. **Efficient generation.** There is a QPT algorithm G such that, for any state $|\psi\rangle$:

$$G_\lambda(k, |\psi\rangle) = U_k |\psi\rangle .$$

Definition of PRUs

Definition (Pseudorandom unitaries [JLS18])

A keyed family of n-qubit unitaries $\{U_k\}_{k\in\{0,1\}^\lambda}$ is *pseudorandom* if the following two conditions hold:

1. **Efficient generation.** There is a QPT algorithm G such that, for any state $|\psi\rangle$:

$$G_\lambda(k, |\psi\rangle) = U_k |\psi\rangle .$$

2. **Pseudorandomness.** For any QPT adversary $\mathcal{A}$, we have:

$$\left| \Pr_{k\leftarrow\{0,1\}^\lambda}\left[\mathcal{A}^{U_k}\left(1^\lambda\right) = 1\right] - \Pr_{V\leftarrow\mu_{2^n}}\left[\mathcal{A}^{V}\left(1^\lambda\right) = 1\right]\right| \leq \mathrm{negl}(\lambda).$$

By contradiction, consider the PRU algorithm $\{G_k\}_{k \in \{0,1\}^*}$:

$$G_k : |\psi\rangle \mapsto |\psi'\rangle = U_T^{(k)} \; S_{x_T^{(k)}} \; \cdots \; U_1^{(k)} \; S_{x_1^{(k)}} \; U_0^{(k)} \; |\psi\rangle$$

Unitary — Query — Unitary — Query — Unitary

Breaking PRUs

By contradiction, consider the PRU algorithm $\{G_k\}_{k \in \{0,1\}^*}$:

$$G_k : |\psi\rangle \mapsto |\psi'\rangle = U_T^{(k)} \quad S_{x_T^{(k)}} \quad \dots \quad U_1^{(k)} \quad S_{x_1^{(k)}} \quad U_0^{(k)} \quad |\psi\rangle$$

Unitary Query Unitary Query Unitary

We assume there is no ancilla. (general case is WIP) 😬

The tools

Lemma (Swap test)

The swap test on input $(|\sigma\rangle, |\rho\rangle)$ outputs 1 with probability

$$\frac{1 + |\langle\rho|\sigma\rangle|^2}{2},$$

in which case we say that it passes the swap test.

Attack idea

The algorithm

Input V: either one of $\{G_k\}$ or a truly Haar random unitary.

Attack idea

The algorithm

Input V: either one of $\{G_k\}$ or a truly Haar random unitary.
For all k:

- We compare V with G_k, using swap tests.
- If they are close, output 1.

Output 0.

Attack idea

The algorithm

Input V: either one of $\{G_k\}$ or a truly Haar random unitary.
For all k:

- We compare V with G_k, using swap tests.
- If they are close, output 1.

Output 0.

- There are $O(2^n)$ operations, but $\mathcal{O}_2$ can make it possible

Attack idea

The algorithm

Input V: either one of $\{G_k\}$ or a truly Haar random unitary.
For all k:

- We compare V with G_k, using swap tests.
- If they are close, output 1.

Output 0.

- There are $O(2^n)$ operations, but $\mathcal{O}_2$ can make it possible
- But here, $\mathcal{O}_2$ will be dependant of $\mathcal{O}_1$, which is bad for the existence of PRFS! 😟

Attack idea

The algorithm

Input V: either one of $\{G_k\}$ or a truly Haar random unitary.
For all k:

- We compare V with G_k, using swap tests.
- If they are close, output 1.

Output 0.

- There are $O(2^n)$ operations, but $\mathcal{O}_2$ can make it possible
- But here, $\mathcal{O}_2$ will be dependant of $\mathcal{O}_1$, which is bad for the existence of PRFS! 😟
- We will approximate G_k without querying $\mathcal{O}_1$, and $\mathcal{O}_2$ will be independent of $\mathcal{O}_1$ 😌

Breaking PRUs

Claim

For any state $|\psi\rangle$ independent from the oracle,

$$S_x |\psi\rangle \approx |\psi\rangle .$$

Breaking PRUs

Claim

For any state $|\psi\rangle$ independent from the oracle,

$$S_x |\psi\rangle \approx |\psi\rangle .$$

Therefore, one may argue that

$$\begin{aligned} G_k |\psi\rangle &= U_T^{(k)} \cdot S_{x_T^{(k)}} \cdot U_{T-1}^{(k)} \cdot \ldots \cdot U_1^{(k)} \cdot S_{x_1^{(k)}} \cdot U_0^{(k)} |\psi\rangle \\ &\approx U_T^{(k)} \cdot U_{T-1}^{(k)} \cdot \ldots \cdot U_1^{(k)} \cdot U_0^{(k)} |\psi\rangle . \end{aligned}$$

Breaking PRUs

Claim

For any state $|\psi\rangle$ independent from the oracle,

$$S_x |\psi\rangle \approx |\psi\rangle .$$

Therefore, one may argue that

$$G_k |\psi\rangle = U_T^{(k)} \cdot S_{x_T^{(k)}} \cdot U_{T-1}^{(k)} \cdot \ldots \cdot U_1^{(k)} \cdot S_{x_1^{(k)}} \cdot U_0^{(k)} |\psi\rangle$$
$$\approx U_T^{(k)} \cdot U_{T-1}^{(k)} \cdot \ldots \cdot U_1^{(k)} \cdot U_0^{(k)} |\psi\rangle .$$

However, the loss is proportional to $1/2^{|x|}$ 🤓👆

Breaking PRUs

Lemma (Informal Tomography Lemma)

Let $|\psi\rangle$ be a quantum state of dimension n. Given $O(2^n)$ copies of $|\psi\rangle$, there exists an algorithm that can approximate $|\psi\rangle$ with negligible error.

Breaking PRUs

Lemma (Informal Tomography Lemma)

Let $|\psi\rangle$ be a quantum state of dimension n. Given $O(2^n)$ copies of $|\psi\rangle$, there exists an algorithm that can approximate $|\psi\rangle$ with negligible error.

We define:

$$\tilde{S}_x = \begin{cases} S'_x, & \text{for small } |x|, \\ I, & \text{for large } |x|. \end{cases}$$

$$F_k : |\psi\rangle \mapsto U_T^{(k)} \cdot \tilde{S}_{x_T^{(k)}} \cdot U_{T-1}^{(k)} \cdot \ldots \cdot U_1^{(k)} \cdot \tilde{S}_{x_1^{(k)}} \cdot U_0^{(k)} |\psi\rangle ,$$

Breaking PRUs

Lemma (Informal Tomography Lemma)

Let $|\psi\rangle$ be a quantum state of dimension n. Given $O(2^n)$ copies of $|\psi\rangle$, there exists an algorithm that can approximate $|\psi\rangle$ with negligible error.

We define:

$$\tilde{S}_x = \begin{cases} S'_x, & \text{for small } |x|, \\ I, & \text{for large } |x|. \end{cases}$$

$$F_k : |\psi\rangle \mapsto U_T^{(k)} \cdot \tilde{S}_{x_T^{(k)}} \cdot U_{T-1}^{(k)} \cdot \ldots \cdot U_1^{(k)} \cdot \tilde{S}_{x_1^{(k)}} \cdot U_0^{(k)} |\psi\rangle ,$$

$$\boxed{F_k |\psi\rangle \approx G_k |\psi\rangle}.$$

Breaking PRUs

Input V: either one of $\{G_k\}$ or a truly Haar random unitary.

Breaking PRUs

Input V: either one of $\{G_k\}$ or a truly Haar random unitary.
Informally: we compare V with all our simulations F_k of the G_k.

Breaking PRUs

Input V: either one of $\{G_k\}$ or a truly Haar random unitary.
Informally: we compare V with all our simulations F_k of the G_k.

The attack

Prepares $\Phi = (|\rho\rangle \otimes V|\rho\rangle)^{\otimes M}$ for some large M and defines:

P_k: on input $\Phi = (|\rho\rangle \otimes V|\rho\rangle)^{\otimes M}$, it applies $(F_k \otimes \mathrm{Id})^{\otimes M}$, applies M swap tests on each copy; if sufficiently many copies pass the swap test, it returns 1. Otherwise it returns 0.

Breaking PRUs

Input V: either one of $\{G_k\}$ or a truly Haar random unitary.
Informally: we compare V with all our simulations F_k of the G_k.

The attack

Prepares $\Phi = (|\rho\rangle \otimes V|\rho\rangle)^{\otimes M}$ for some large M and defines:

P_k: on input $\Phi = (|\rho\rangle \otimes V|\rho\rangle)^{\otimes M}$, it applies $(F_k \otimes \mathrm{Id})^{\otimes M}$, applies M swap tests on each copy; if sufficiently many copies pass the swap test, it returns 1. Otherwise it returns 0.

It works

We can show that

- if $V = G_k$, P_k returns 1 with high probability,
- if V is a Haar random unitary, P_k returns almost always 0.

Breaking PRUs

Input V: either one of $\{G_k\}$ or a truly Haar random unitary.
Informally: we compare V with all our simulations F_k of the G_k.

The attack

Prepares $\Phi = (|\rho\rangle \otimes V|\rho\rangle)^{\otimes M}$ for some large M and defines:

P_k: on input $\Phi = (|\rho\rangle \otimes V|\rho\rangle)^{\otimes M}$, it applies $(F_k \otimes \mathrm{Id})^{\otimes M}$, applies M swap tests on each copy; if sufficiently many copies pass the swap test, it returns 1. Otherwise it returns 0.

It works

We can show that

- if $V = G_k$, P_k returns 1 with high probability,
- if V is a Haar random unitary, P_k returns almost always 0.

This can be done with a QPSPACE oracle! (Quantum OR Lemma) 🔥

Breaking PRUs

Input V: either one of $\{G_k\}$ or a truly Haar random unitary.
Informally: we compare V with all our simulations F_k of the G_k.

The attack

Prepares $\Phi = (|\rho\rangle \otimes V|\rho\rangle)^{\otimes M}$ for some large M and defines:

P_k: on input $\Phi = (|\rho\rangle \otimes V|\rho\rangle)^{\otimes M}$, it applies $(F_k \otimes \mathrm{Id})^{\otimes M}$, applies M swap tests on each copy; if sufficiently many copies pass the swap test, it returns 1. Otherwise it returns 0.

It works

We can show that

- if $V = G_k$, P_k returns 1 with high probability,
- if V is a Haar random unitary, P_k returns almost always 0.

This can be done with a QPSPACE oracle! (Quantum OR Lemma) 🔥
Relative to $\mathcal{O} = (\mathcal{O}_1, \mathcal{O}_2)$ =(CHFS,QPSPACE), we have PRUs but not PRFSs!

Other results

Theorem

Assuming a conjecture is true,

$$\exists \text{short-PRFS} \not\Rightarrow \exists\ PRG \quad \textit{(with negligible correctness)}$$

unless BQP $\neq$ QMA.

Other results

Theorem

Assuming a conjecture is true,

$$\exists \textit{short-PRFS} \not\Rightarrow \exists \textit{ PRG}$$ *(with negligible correctness)*

unless BQP $\neq$ QMA.

This complements a previous result that shows that PRFSs can be used to construct PRGs with $1/\mathrm{poly}(\cdot)$ correctness error.

Other results

Theorem

Assuming a conjecture is true,

$$\exists \textit{short-PRFS} \not\Rightarrow \exists \textit{ PRG}$$ *(with negligible correctness)*

unless BQP $\neq$ QMA.

This complements a previous result that shows that PRFSs can be used to construct PRGs with $1/\text{poly}(\cdot)$ correctness error.

Theorem

Assuming the same conjecture is true,

$$\exists \textit{short-PRS} \not\Rightarrow \exists \textit{ long-PRS}$$ *(with pure generation)*

Other results

Theorem

Assuming a conjecture is true,

$$\exists \textit{short-PRFS} \nRightarrow \exists \textit{ PRG}$$ *(with negligible correctness)*

unless BQP $\neq$ QMA.

This complements a previous result that shows that PRFSs can be used to construct PRGs with $1/\text{poly}(\cdot)$ correctness error.

Theorem

Assuming the same conjecture is true,

$$\exists \textit{short-PRS} \nRightarrow \exists \textit{ long-PRS}$$ *(with pure generation)*

This complements a previous result that shows that there exits an oracle relative which PRSs exist but short PRSs do not.

Conclusion

- Oracle separation of PRUs and PRFSs (There is still some work left to finish our proof!)
- Conditionned oracle separation of short-PRSs and PRSs.
- Also, there is still a lot left to do to fully grasp the strength of quantum assumptions.

Conclusion

- Oracle separation of PRUs and PRFSs (There is still some work left to finish our proof!)
- Conditionned oracle separation of short-PRSs and PRSs.
- Also, there is still a lot left to do to fully grasp the strength of quantum assumptions.

Thank you for your attention!

Lemma (Quantum OR lemma)

Let $\{\Pi_i\}_{i\in[N]}$ be POVMs. Let $0 < \varepsilon < 1/2$ and $\delta > 0$. Let Ψ be a quantum state such that either

1. *there exists $i \in [N]$ such that $\mathrm{Tr}[\Pi_i \Psi] \geq 1 - \varepsilon$, or*
2. *for all $i \in [N]$, $\mathrm{Tr}[\Pi_i \Psi] \leq \delta$.*

Then, there is a quantum circuit C, such that in case i)

$$\Pr(1 \leftarrow C(\Psi)) \geq \frac{(1-\varepsilon)^2}{7},$$

and in case ii),

$$\Pr(1 \leftarrow C(\Psi)) \leq 4N\delta.$$

The circuit C can be implemented in QPSPACE.

Bibliography

R. Impagliazzo.
A personal view of average-case complexity.
In *Proceedings of Structure in Complexity Theory. Tenth Annual IEEE Conference*, pages 134–147, 1995.

Russell Impagliazzo and Steven Rudich.
Limits on the provable consequences of one-way permutations.
In *21st ACM STOC*, pages 44–61. ACM Press, May 1989.

Zhengfeng Ji, Yi-Kai Liu, and Fang Song.
Pseudorandom quantum states.
In Hovav Shacham and Alexandra Boldyreva, editors, *CRYPTO 2018, Part III*, volume 10993 of *LNCS*, pages 126–152. Springer, Cham, August 2018.