Audition CNRS - Concours 06/02

Complexity-Theoretic Foundations of Cryptography

Willy Quach

Area of research: Theory of cryptography

- September 2023 - : Postdoctoral Fellow at the Weizmann Institute of Science. <u>Host:</u> Zvika Brakerski
- September 2017 - August 2023: PhD student at Northeastern University. <u>Advisor:</u> Daniel Wichs
- September 2013 - August 2017: École Normale Supérieure de Lyon

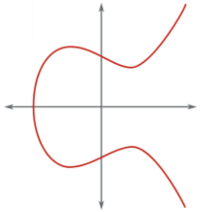
Cryptography is a core backbone for security and privacy

Cryptography is a core backbone for security and privacy

What makes modern cryptography reliable?

VS

$N = pq$



"Ancient" cryptography

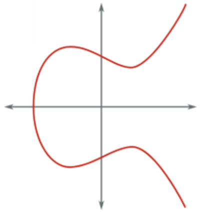
Modern cryptography

Cryptography is a core backbone for security and privacy

What makes modern cryptography reliable?

VS

$N = pq$



"Ancient" cryptography

Modern cryptography

We have **abstractions** to reason about security and **paradigms** to achieve them.

Formalize and quantify security (!)

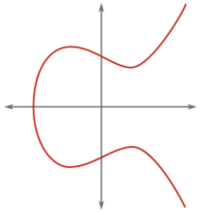
Techniques to tie security to **complexity theory**

Cryptography is a core backbone for security and privacy

What makes modern cryptography reliable?

VS

$N = pq$



"Ancient" cryptography

Modern cryptography

We have **abstractions** to reason about security and **paradigms** to achieve them.

Formalize and quantify security (!)

Techniques to tie security to **complexity theory**

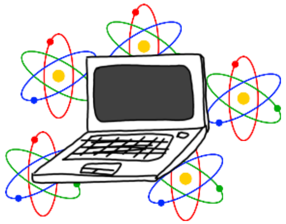
What is there left to do?

My Research in a Nutshell

My Research in a Nutshell

1

Address new threats



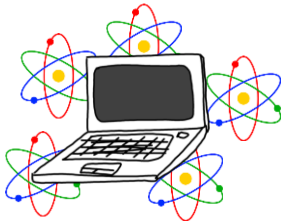
Devastating effects of
quantum attacks, side-channel attacks

My Research in a Nutshell

1

Address new threats

Devastating effects of
quantum attacks, side-channel attacks



- Security against quantum computers

  How to argue security? [TCC ‘22, **Invited to the Journal of Cryptology**]

  Alternate ``quantum-secure’’ constructions [PKC ‘18, CRYPTO ‘19, TCC ‘21]

My Research in a Nutshell

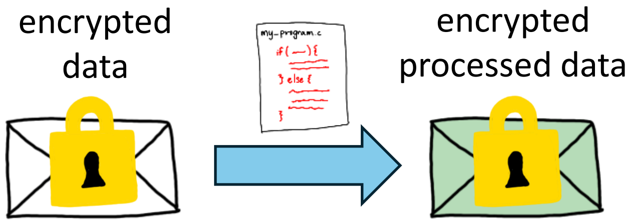
1 Address new threats

Devastating effects of **quantum attacks, side-channel attacks**

- Security against quantum computers
  - How to argue security? [TCC '22, **Invited to the Journal of Cryptology**]
  - Alternate ``quantum-secure'' constructions [PKC '18, CRYPTO '19, TCC '21]

2 Provide stronger functionalities

Private data used in **computation**, not just transit



My Research in a Nutshell

1

Address new threats

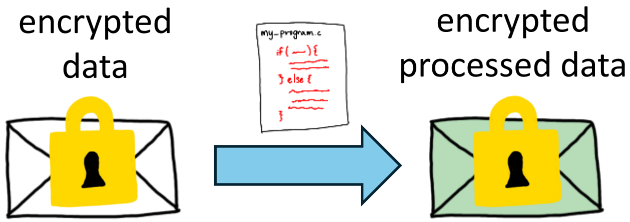
Devastating effects of
quantum attacks, side-channel attacks

- Security against quantum computers
  How to argue security? [TCC '22, **Invited to the Journal of Cryptology**]
  Alternate ``quantum-secure'' constructions [PKC '18, CRYPTO '19, TCC '21]

2

Provide stronger functionalities

Private data used in **computation**, not just transit



- Tools to compute blindly over encrypted data
  Introducing new cryptographic tools [FOCS '18]
  Advanced encryption [CRYPTO '19], program obfuscation [TCC '21]

My Research in a Nutshell

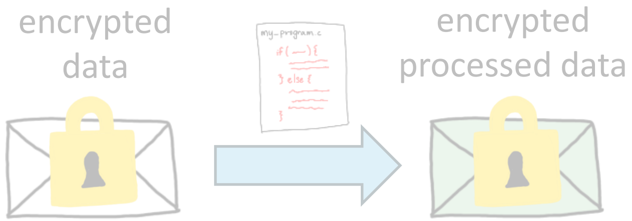
1 Address new threats

Devastating effects of **quantum attacks, side-channel attacks**

- Security against quantum computers
  - How to argue security? [TCC ‘22, **Invited to the Journal of Cryptology**]
  - Alternate ``quantum-secure’’ constructions [PKC ‘18, CRYPTO ‘19, TCC ‘21]

2 Provide stronger functionalities

Private data used in **computation**, not just transit



- Tools to compute blindly over encrypted data
  - Introducing new cryptographic tools [FOCS ‘18]
  - Advanced encryption [CRYPTO ‘19], program obfuscation [TCC ‘21]

3 Firmer foundations of cryptography

Foundations are still poorly understood

My Research in a Nutshell

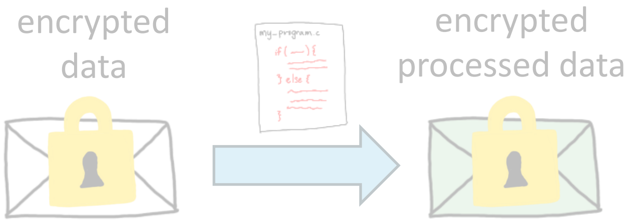
1 Address new threats

Devastating effects of
quantum attacks, side-channel attacks

- Security against quantum computers
  How to argue security? [TCC ‘22, **Invited to the Journal of Cryptology**]
  Alternate ``quantum-secure’’ constructions [PKC ‘18, CRYPTO ‘19, TCC ‘21]

2 Provide stronger functionalities

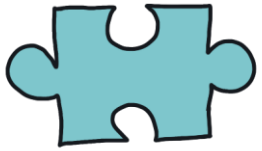
Private data used in **computation**, not just transit



- Tools to compute blindly over encrypted data
  Introducing new cryptographic tools [FOCS ‘18]
  Advanced encryption [CRYPTO ‘19], program obfuscation [TCC ‘21]

3 Firmer foundations of cryptography

Foundations are still poorly understood



- Refine ties with complexity theory
  Cryptographic proof systems [EUROCRYPT ‘19, CRYPTO ‘19, ’21, ’23]
  Alternate models of security [EUROCRYPT ‘22, ‘23, TCC ‘23]

A Global Lens: Computational Hardness

A Global Lens: Computational Hardness

Cryptographic security is proven under **computational assumptions**

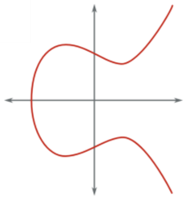
Most cryptography can be broken in $NP \implies$ need to assume algorithmic hardness / that $P \neq NP$

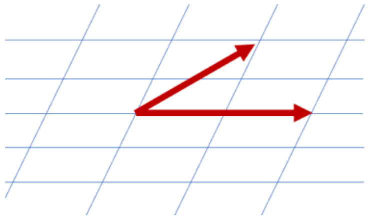
A Global Lens: Computational Hardness

Cryptographic security is proven under **computational assumptions**

Most cryptography can be broken in $NP \implies$ need to assume algorithmic hardness / that $P \neq NP$

$$N = pq$$





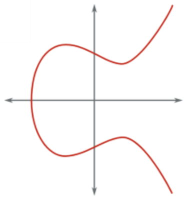
Hard algorithmic problem

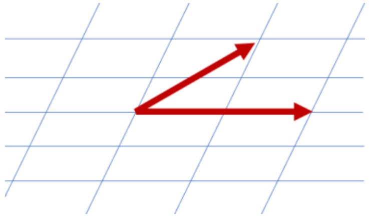
A Global Lens: Computational Hardness

Cryptographic security is proven under **computational assumptions**

Most cryptography can be broken in $NP \implies$ need to assume algorithmic hardness / that $P \neq NP$

$N = pq$





Hard algorithmic problem

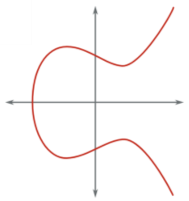
The choice of assumption matters a lot!

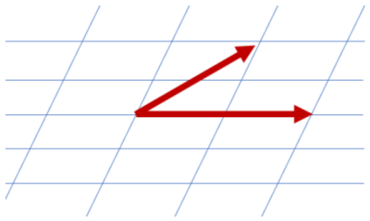
A Global Lens: Computational Hardness

Cryptographic security is proven under **computational assumptions**

Most cryptography can be broken in $NP \implies$ need to assume algorithmic hardness / that $P \neq NP$

$N = pq$





Hard algorithmic problem

The choice of assumption matters a lot!

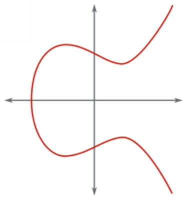
<u>Property about the assumption:</u>

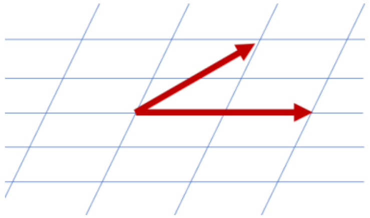
A Global Lens: Computational Hardness

Cryptographic security is proven under computational assumptions

Most cryptography can be broken in $NP \implies$ need to assume algorithmic hardness / that $P \neq NP$

$N = pq$



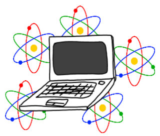


The choice of assumption matters a lot!

Hard algorithmic problem

Property about the assumption:

1 Security against quantum attacks



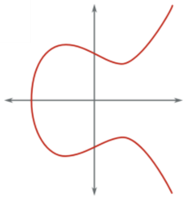
Hardness against quantum computers

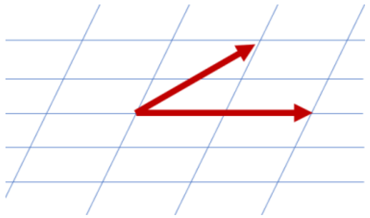
A Global Lens: Computational Hardness

Cryptographic security is proven under computational assumptions

Most cryptography can be broken in $NP \implies$ need to assume algorithmic hardness / that $P \neq NP$

$$N = pq$$



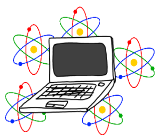


Hard algorithmic problem

The choice of assumption matters a lot!

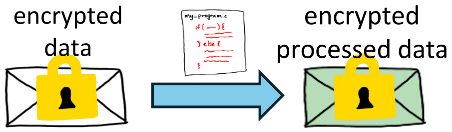
Property about the assumption:

1. Security against quantum attacks



Hardness against quantum computers

2. Strong functionalities



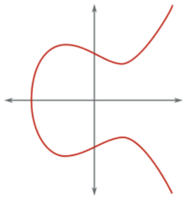
Exploitable algebraic structure

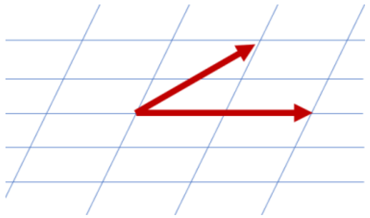
A Global Lens: Computational Hardness

Cryptographic security is proven under **computational assumptions**

Most cryptography can be broken in $NP \implies$ need to assume algorithmic hardness / that $P \neq NP$

$N = pq$



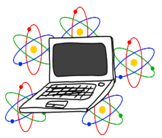


Hard algorithmic problem

The choice of assumption matters a lot!

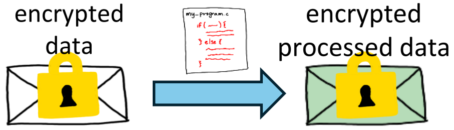
<u>Property about the assumption:</u>

1 Security against quantum attacks



Hardness against quantum computers

2 Strong functionalities



Exploitable algebraic structure

3 Foundations of cryptography

Strength of assumption

A Global Lens: Computational Hardness

Cryptographic security is proven under **computational assumptions**

Mo

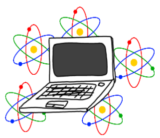
lot!

Focus for today:

How (not) to argue security against quantum attacks

[LMQW, TCC '22, *Invited to the Journal of Cryptology*]

Property about the assumption:

1 Security against quantum attacks  Hardness against quantum computers

2 Strong functionalities

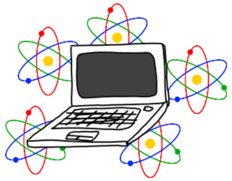
Exploitable algebraic structure

3 Foundations of cryptography Strength of assumption

Post-Quantum Security

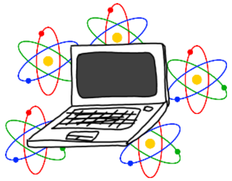
Quantum computers would **break** most public-key cryptography deployed.

via Shor's algorithm [Shor'94]



Post-Quantum Security

Quantum computers would **break** most public-key cryptography deployed.
via Shor's algorithm [Shor'94]

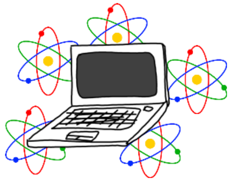


Need new cryptosystems that resist quantum attacks
a.k.a **post-quantum secure**

Data sensitive today might still be sensitive in 50 years!

Post-Quantum Security

Quantum computers would **break** most public-key cryptography deployed.
via Shor's algorithm [Shor'94]



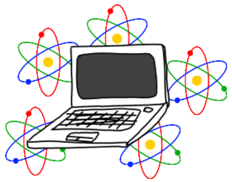
Need new cryptosystems that resist quantum attacks
a.k.a **post-quantum secure**

Data sensitive today might still be sensitive in 50 years!

Extremely active research, standardization processes all over the world
National Institute of Standards and Technology (NIST), ANSSI in France…

Post-Quantum Security

Quantum computers would **break** most public-key cryptography deployed.
via Shor's algorithm [Shor'94]



Need new cryptosystems that resist quantum attacks
a.k.a **post-quantum secure**

Data sensitive today might still be sensitive in 50 years!

Extremely active research, standardization processes all over the world
National Institute of Standards and Technology (NIST), ANSSI in France…

How do we ensure security against quantum attacks?

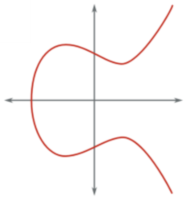
Surprisingly little attention given to this general question

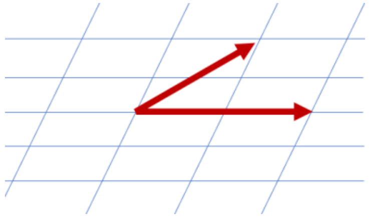
Back to Computational Hardness

Cryptographic security is proven under **computational assumptions**

Most cryptography can be broken in $NP \implies$ need to assume algorithmic hardness / $P \neq NP$

$$N = pq$$





Hard algorithmic problem

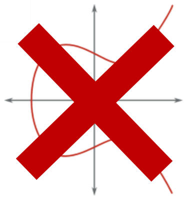
The choice of assumption matters a lot!

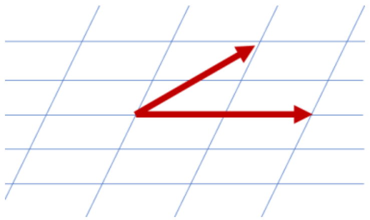
Back to Computational Hardness

Cryptographic security is proven under **computational assumptions**

Most cryptography can be broken in $NP \implies$ need to assume algorithmic hardness / $P \neq NP$

$\cancel{N = pq}$



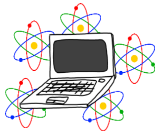


The choice of assumption matters a lot!

Quantumly easy

Quantumly hard

Security against quantum attacks



a.k.a **post-quantum security**

Hardness against quantum computers

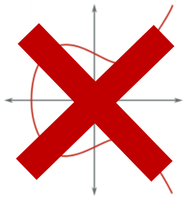
a.k.a **post-quantum assumptions**

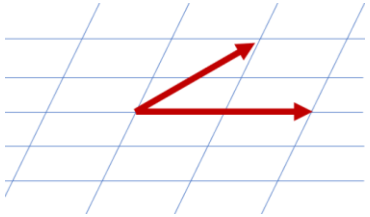
Back to Computational Hardness

Cryptographic security is proven under computational assumptions

Most cryptography can be broken in $NP \implies$ need to assume algorithmic hardness / $P \neq NP$

$\cancel{N = pq}$





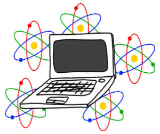
Quantumly easy

Quantumly hard

The choice of assumption matters a lot!

Security against quantum attacks

a.k.a **post-quantum security**



requires $\Longrightarrow$

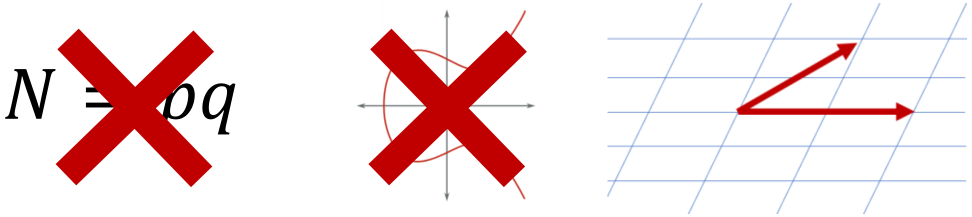
Hardness against quantum computers

a.k.a **post-quantum assumptions**

Back to Computational Hardness

Cryptographic security is proven under computational assumptions

Most cryptography can be broken in $NP \implies$ need to assume algorithmic hardness / $P \neq NP$



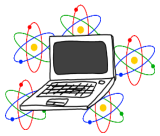
Quantumly easy

Quantumly hard

The choice of assumption matters a lot!

Security against quantum attacks

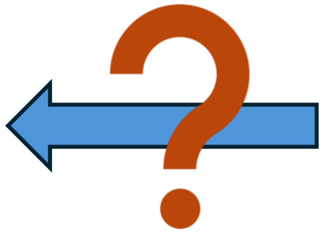
a.k.a **post-quantum security**



requires $\Longrightarrow$

Hardness against quantum computers

a.k.a **post-quantum assumptions**



Main Result

Is using post-quantum assumptions sufficient to ensure post-quantum security?

Surprisingly not explicitly asked before (??)

Main Result

Is using post-quantum assumptions sufficient to ensure post-quantum security?

Surprisingly not explicitly asked before (??)

Folklore: For “standard cryptography”*, **yes**

Implicit in two decades of research

*”Non-interactive” cryptosystems such as **encryption schemes**, **signatures**…
As opposed to *interactive* or *heuristic* cryptosystems

Main Result

Is using post-quantum assumptions sufficient to ensure post-quantum security?

Surprisingly not explicitly asked before (??)

Folklore: For "standard cryptography"*, **yes**

Implicit in two decades of research

Main Theorem [LMQW TCC'22]: **NO**

Post-quantum assumptions **are not** sufficient for post-quantum security

*"Non-interactive" cryptosystems such as **encryption schemes**, **signatures**…
As opposed to *interactive* or *heuristic* cryptosystems

Main Result

Is using post-quantum assumptions sufficient to ensure post-quantum security?

Surprisingly not explicitly asked before (??)

Folklore: For "standard cryptography"*, **yes**

Implicit in two decades of research

Main Theorem [LMQW TCC'22]: **NO**

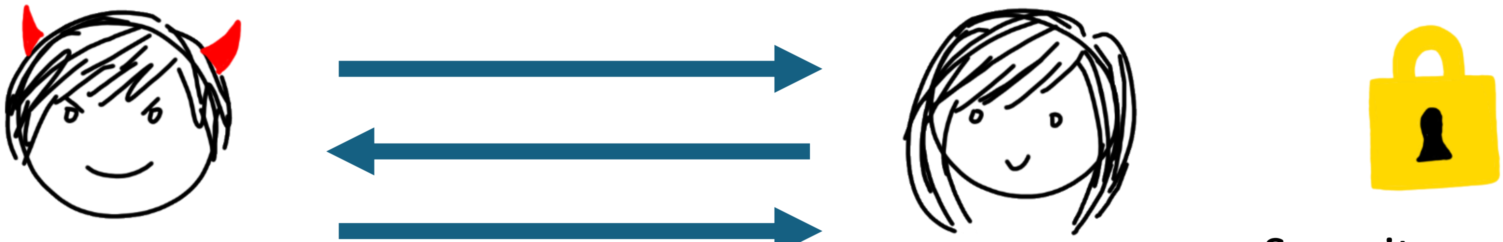
Post-quantum assumptions **are not** sufficient for post-quantum security

The folklore understanding is **wrong**!

*"Non-interactive" cryptosystems such as **encryption schemes**, **signatures**...
As opposed to *interactive* or *heuristic* cryptosystems

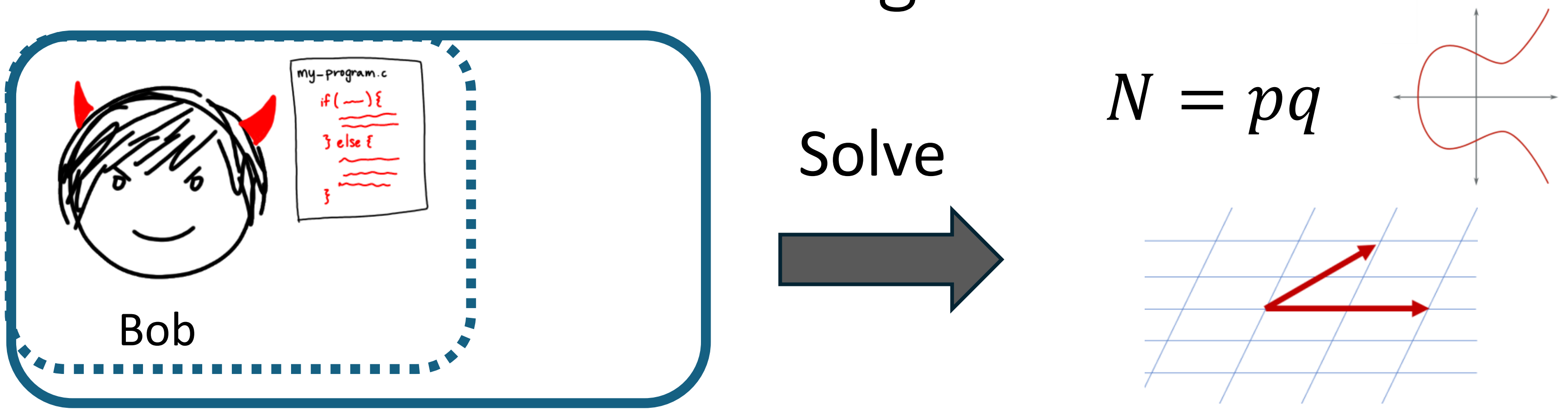
What Goes Wrong?

What Goes Wrong?



Successful attacks against implicitly solve a hard problem

What Goes Wrong?



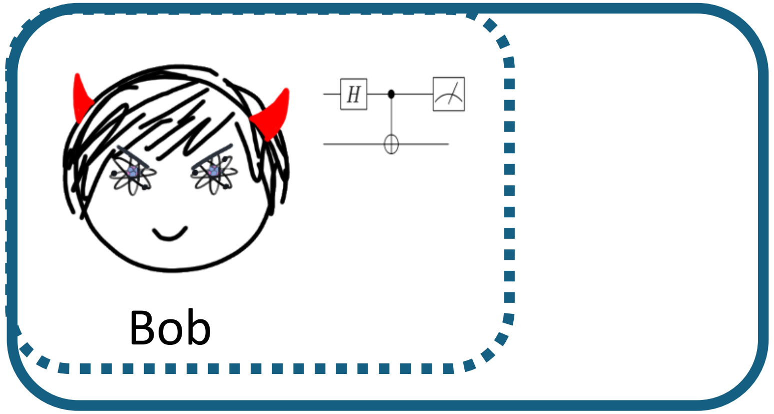
Reduction

Hard algorithmic problems

Reduction turns successful attacks into efficient algorithms

a.k.a **proof of security**

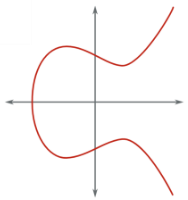
What Goes Wrong?

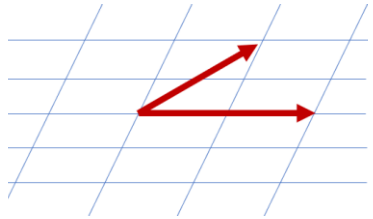


Reduction

Solve

$N = pq$



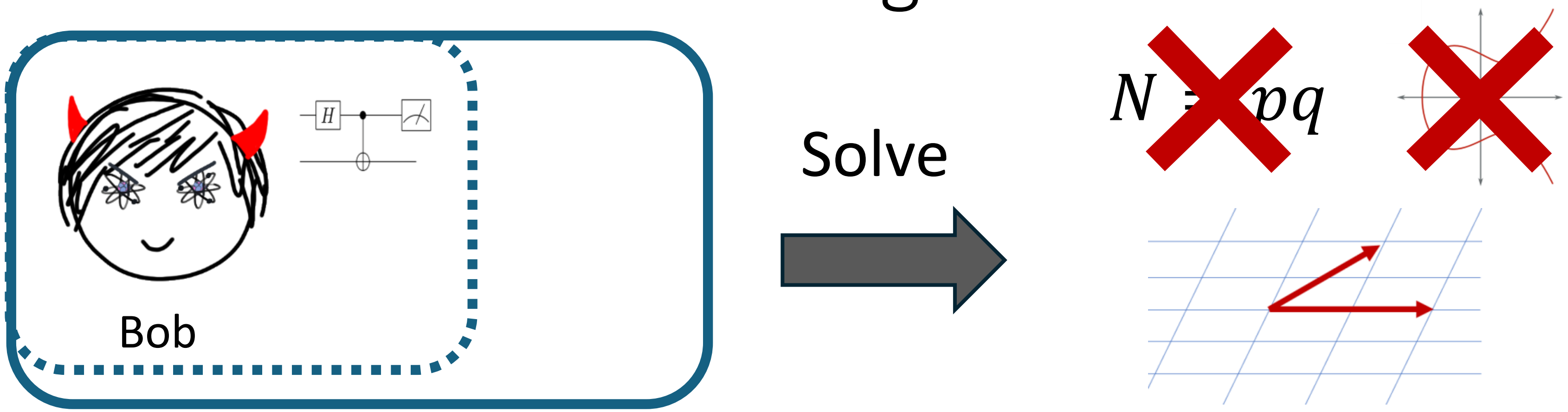


Quantumly hard problems

Reduction turns successful **quantum** attacks into efficient **quantum** algorithms

a.k.a **proof of post-quantum security**

What Goes Wrong?

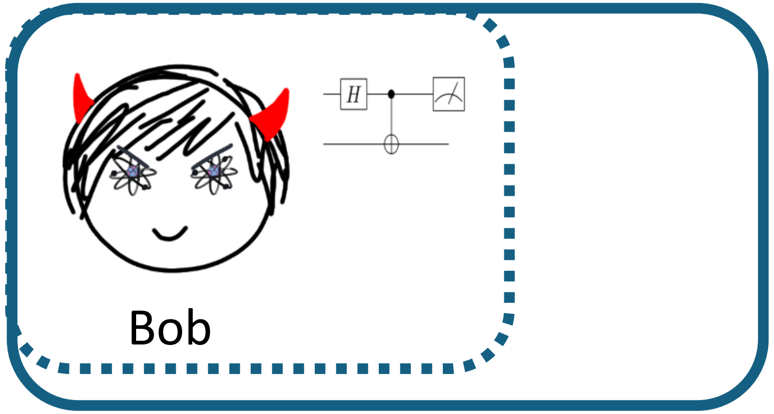


Reduction **Quantumly** hard problems

Reduction turns successful **quantum** attacks into efficient **quantum** algorithms

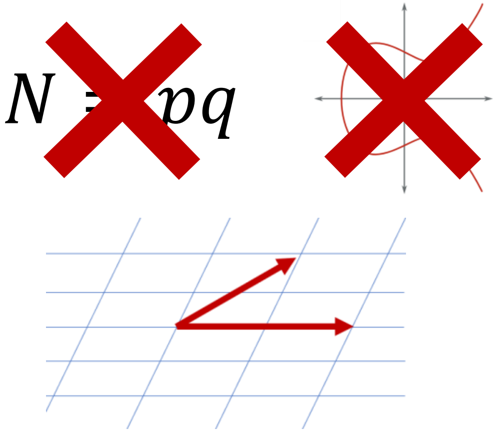
a.k.a **proof of post-quantum security**

What Goes Wrong?



Reduction

Solve



Quantumly hard problems

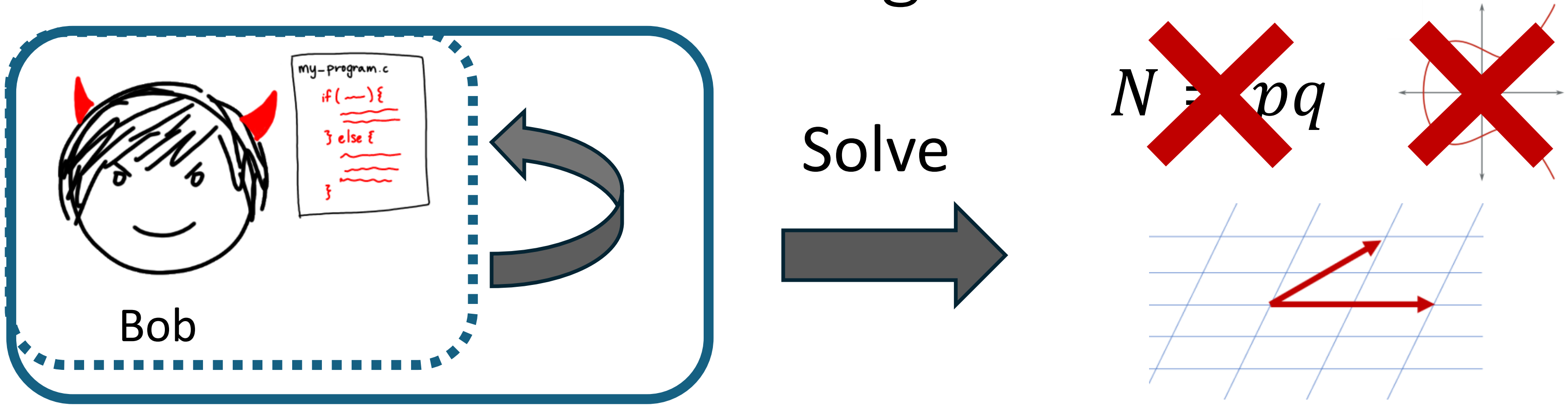
Reduction turns successful **quantum** attacks into efficient **quantum** algorithms

a.k.a **proof of post-quantum security**

Main issue: proofs of security *are not* proofs of post-quantum security

Quantum attacks behave very differently from classical attacks

What Goes Wrong?



Reduction

Quantumly hard problems

Reduction turns successful **quantum** attacks into efficient **quantum** algorithms

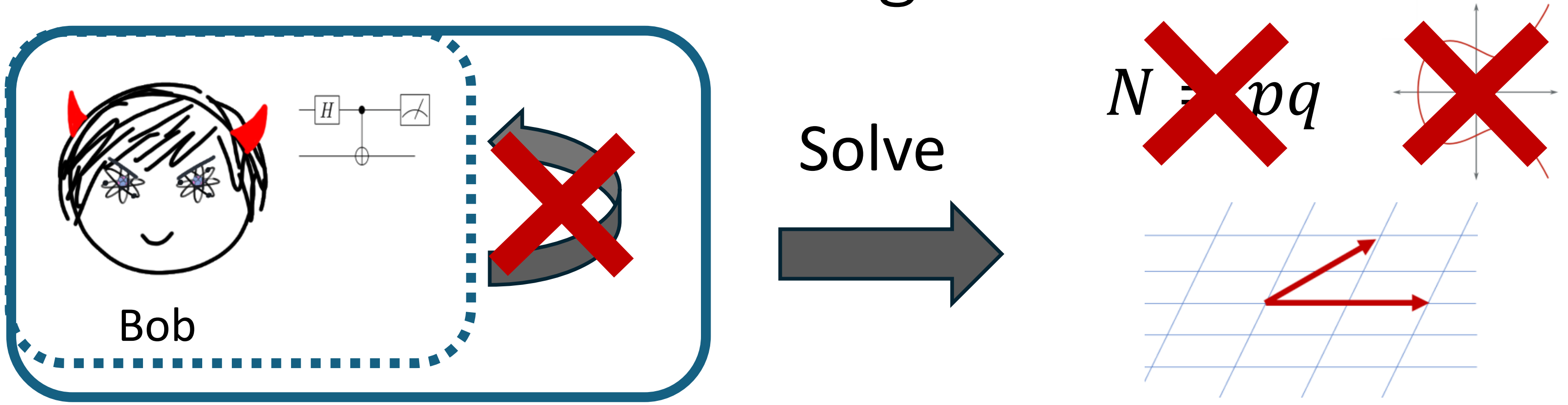
a.k.a **proof of post-quantum security**

Main issue: proofs of security *are not* proofs of post-quantum security

Quantum attacks behave very differently from classical attacks

- Stateful classical algorithms can be run several times (rewinding)

What Goes Wrong?



Reduction **Quantumly** hard problems

Reduction turns successful **quantum** attacks into efficient **quantum** algorithms

a.k.a **proof of post-quantum security**

Main issue: proofs of security *are not* proofs of post-quantum security
Quantum attacks behave very differently from classical attacks

- Stateful classical algorithms can be run several times (rewinding)
- Stateful quantum algorithms ***cannot*** in general (measurements are destructive)

Main Result (2)

Main Result (2)

Main Theorem [LMQW TCC'22] **: Explicit counter-examples:**

- Proven secure (classically) **under a post-quantum assumption**
- **Quantumly broken**

Includes symmetric-key encryption, digital signatures…

Main Result (2)

Main Theorem [LMQW TCC'22] **: Explicit counter-examples:**

- Proven secure (classically) **under a post-quantum assumption**
- **Quantumly broken**

Includes symmetric-key encryption, digital signatures…

Main observation: cryptographic attacks **can be stateful**

Reductions can interact with attacks in subtle ways

Reductions can run classical attacks twice, but not quantum attacks

Main Result (2)

Main Theorem [LMQW TCC'22] **: Explicit counter-examples:**

- Proven secure (classically) **under a post-quantum assumption**
- **Quantumly broken**

Includes symmetric-key encryption, digital signatures…

Main observation: cryptographic attacks **can be stateful**
Reductions can interact with attacks in subtle ways

Reductions can run classical attacks twice, but not quantum attacks

Technique: constructions of "**cryptographic proofs of quantumness**" with **stateless verifiers**

Main Result (2)

Main Theorem [LMQW TCC’22] **: Explicit counter-examples:**

- Proven secure (classically) **under a post-quantum assumption**
- **Quantumly broken**

Includes symmetric-key encryption, digital signatures…

Main observation: cryptographic attacks **can be stateful**
Reductions can interact with attacks in subtle ways

Reductions can run classical attacks twice, but not quantum attacks

Technique: constructions of “**cryptographic proofs of quantumness**” with **stateless verifiers**

Conceptually: Proofs of quantumness ≡ Counter-examples

⇐ breaking security “proves quantumness”

Takeaway: cannot simply plug-in post-quantum assumptions,
need special-purpose proofs of post-quantum security

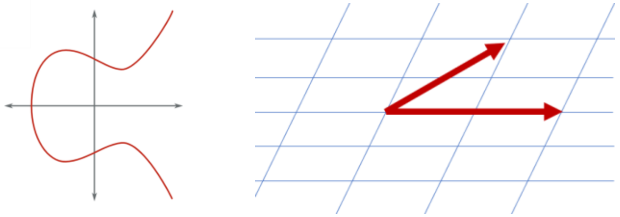
Research Project

Back to Computational Hardness (Again)

Cryptographic security is proven under computational assumptions

Most cryptography can be broken in $NP \Longrightarrow$ need to assume algorithmic hardness / that $P \neq NP$

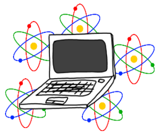
$$N = pq$$

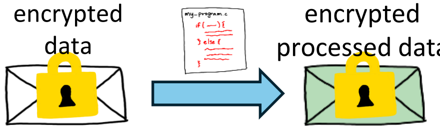


The choice of assumption matters a lot!

Hard algorithmic problem

<u>Property about the assumption:</u>

1. Security against quantum attacks  — Hardness against quantum computers

2. Strong functionalities 

— Exploitable algebraic structure

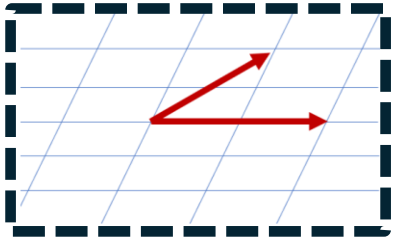
3. Foundations of cryptography  — Strength of assumption

Back to Computational Hardness (Again)

Cryptographic security is proven under **computational assumptions**

Most cryptography can be broken in $NP \implies$ need to assume algorithmic hardness / that $P \neq NP$

$N = pq$

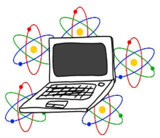


Hard algorithmic problem

Lattices are extremely convenient!

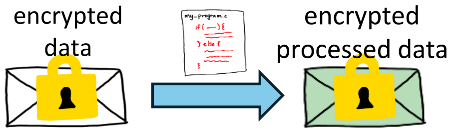
<u>Property about the assumption:</u>

① Security against quantum attacks



Hardness against quantum computers

② Strong functionalities

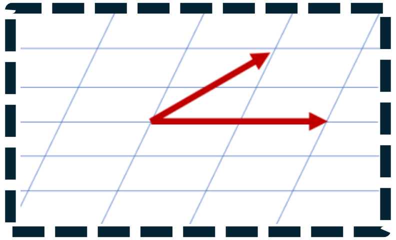


Exploitable algebraic structure

③ Foundations of cryptography

Strength of assumption

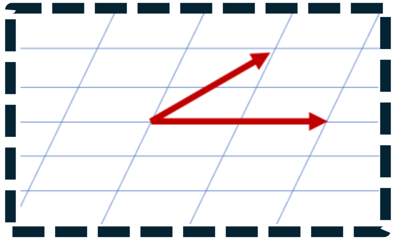
Back to Computational Hardness (Again)



Lattices are extremely powerful and convenient!

$\Rightarrow$ Main **post-quantum candidates**, only credible **homomorphic encryption**…

Back to Computational Hardness (Again)

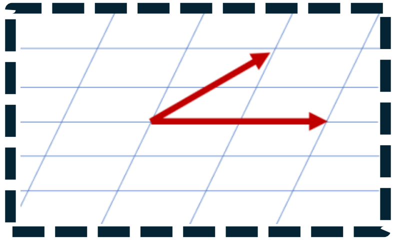


Lattices are extremely powerful and convenient!

⇒ Main **post-quantum candidates**, only credible **homomorphic encryption**…

… but we are starting to put all our eggs in the same basket

Back to Computational Hardness (Again)



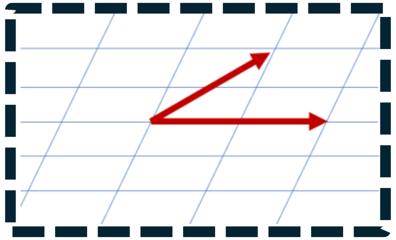
Lattices are extremely powerful and convenient!

⇒ Main **post-quantum candidates**, only credible **homomorphic encryption**…

… but we are starting to put all our eggs in the same basket

- Lattice-based assumptions could be broken…
- Lattices only provide very specialized techniques… lack of broad understanding

Back to Computational Hardness (Again)



Lattices are extremely powerful and convenient!

$\Rightarrow$ Main **post-quantum candidates**, only credible **homomorphic encryption**…

… but we are starting to put all our eggs in the same basket

- Lattice-based assumptions could be broken…
- Lattices only provide very specialized techniques… lack of broad understanding

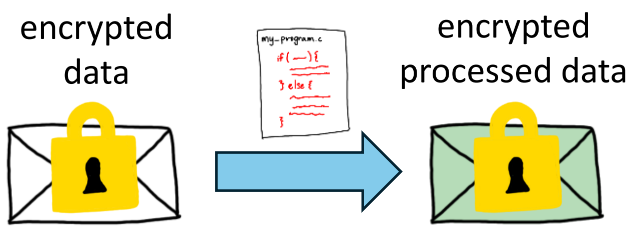
My goal: Leverage other sources of hardness in cryptography

Diversifying Assumptions in Cryptography

1

Strong functionalities from a **wide range of assumptions**

Can we build strong cryptography without lattices?

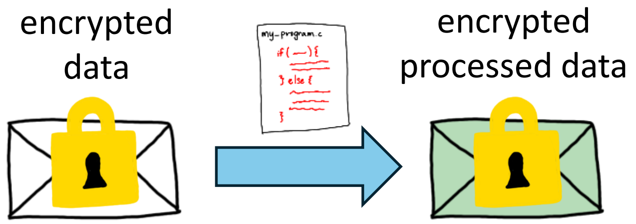


Diversifying Assumptions in Cryptography

1

Strong functionalities from a **wide range of assumptions**

Can we build strong cryptography without lattices?



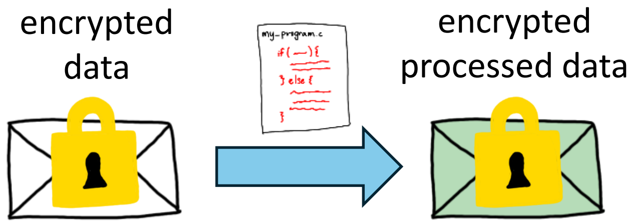
Long-term goal: develop new **generic paradigms** for cryptography

Diversifying Assumptions in Cryptography

1

Strong functionalities from a **wide range of assumptions**

Can we build strong cryptography without lattices?



Long-term goal: develop new **generic paradigms** for cryptography

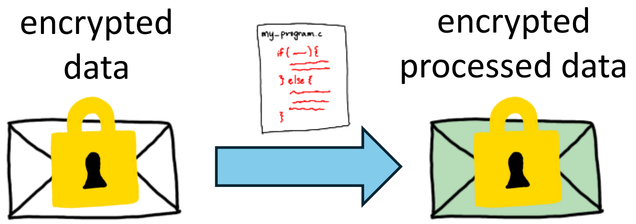
- Identify **technical barriers**, abstract out **concrete stepping stones** (e.g. relaxations)

Diversifying Assumptions in Cryptography

1

Strong functionalities from a wide range of assumptions

Can we build strong cryptography without lattices?



Long-term goal: develop new **generic paradigms** for cryptography

➢ Identify **technical barriers**, abstract out **concrete stepping stones** (e.g. relaxations)

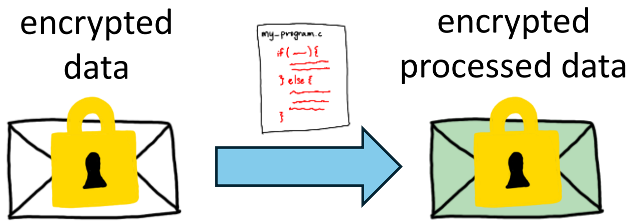
Example: allowing a **single** computation, fixed in advance, on encrypted data suffices in applications, avoids complexity-theoretic barriers!

Diversifying Assumptions in Cryptography

1

Strong functionalities from a wide range of assumptions

Can we build strong cryptography without lattices?



Long-term goal: develop new **generic paradigms** for cryptography

- Identify **technical barriers**, abstract out **concrete stepping stones** (e.g. relaxations)

  Example: allowing a **single** computation, fixed in advance, on encrypted data suffices in applications, avoids complexity-theoretic barriers!

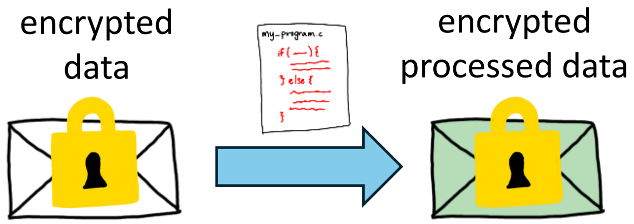
- Develop techniques suited to **other assumptions**

Diversifying Assumptions in Cryptography

1

Strong functionalities from a wide range of assumptions

Can we build strong cryptography without lattices?



Long-term goal: develop new **generic paradigms** for cryptography

- Identify **technical barriers**, abstract out **concrete stepping stones** (e.g. relaxations)

  Example: allowing a **single** computation, fixed in advance, on encrypted data suffices in applications, avoids complexity-theoretic barriers!

- Develop techniques suited to **other assumptions**

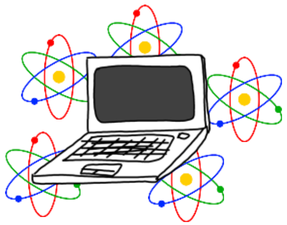
  New assumptions ignored by theory: lattice isomorphisms, isogenies, multivariate systems…
  But also old assumptions! (elliptic curves, coding theory…)

... or explain the absence of such techniques

Diversifying Assumptions in Cryptography (2)

2

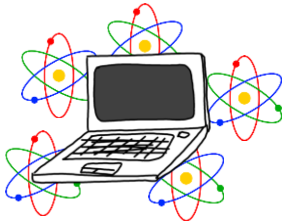
Quantum computation and cryptography



Diversifying Assumptions in Cryptography (2)

2

Quantum computation and cryptography

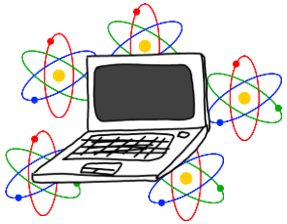


Quantum is usually a **threat** to cryptography

Diversifying Assumptions in Cryptography (2)

2

Quantum computation and cryptography



Quantum is usually a **threat** to cryptography

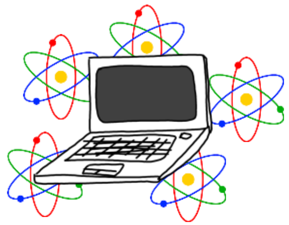
Can we use quantum computing for **stronger cryptography**?

a.k.a ***quantum cryptography***, where honest users use quantum computers, ciphertexts are qubits, etc

Diversifying Assumptions in Cryptography (2)

2

Quantum computation and cryptography



Quantum is usually a **threat** to cryptography

Can we use quantum computing for **stronger cryptography**?

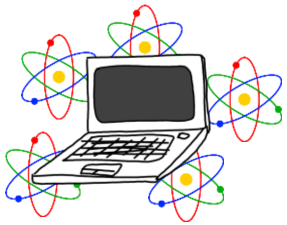
a.k.a ***quantum cryptography***, where honest users use quantum computers, ciphertexts are qubits, etc

The no-cloning principle is useful as a security feature!

Diversifying Assumptions in Cryptography (2)

2

Quantum computation and cryptography



Quantum is usually a **threat** to cryptography

Can we use quantum computing for **stronger cryptography**?

a.k.a ***quantum cryptography***, where honest users use quantum computers, ciphertexts are qubits, etc

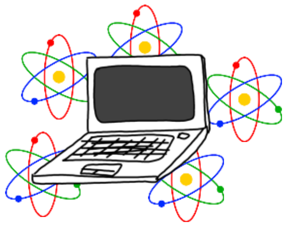
The no-cloning principle is useful as a security feature!

Can we devise entirely new applications?

Diversifying Assumptions in Cryptography (2)

2

Quantum computation and cryptography



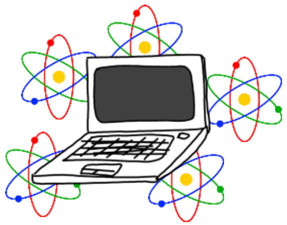
Quantum is usually a **threat** to cryptography

Can we use cryptography to **study quantum computation**?

Diversifying Assumptions in Cryptography (2)

2

Quantum computation and cryptography



Quantum is usually a **threat** to cryptography

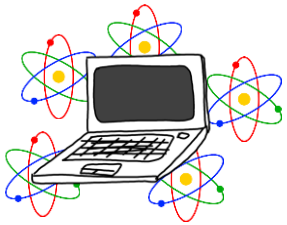
Can we use cryptography to **study quantum computation**?

- Cryptographic proofs of quantumness [BCMVV'18, Yamakawa-Zhandry'22]
- Classical verification of quantum computation [Mahadev'18]

Diversifying Assumptions in Cryptography (2)

2

Quantum computation and cryptography



Quantum is usually a **threat** to cryptography

Can we use cryptography to **study quantum computation**?

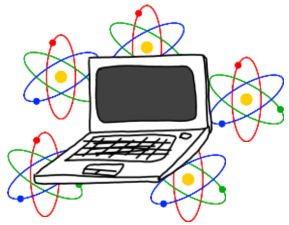
- Cryptographic proofs of quantumness [BCMVV'18, Yamakawa-Zhandry'22]
- Classical verification of quantum computation [Mahadev'18]

What are the "right" complexity-theoretic foundations of quantum cryptography?

Diversifying Assumptions in Cryptography (2)

2

Quantum computation and cryptography



Quantum is usually a **threat** to cryptography

Can we use cryptography to **study quantum computation**?

- Cryptographic proofs of quantumness [BCMVV'18, Yamakawa-Zhandry'22]
- Classical verification of quantum computation [Mahadev'18]

What are the "right" complexity-theoretic foundations of quantum cryptography?

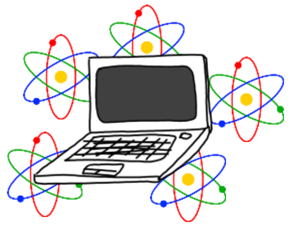
Standard complexity theory studies problems with **classical descriptions**

e.g. find a Hamiltonian cycle in a graph, break a *classical* ciphertext…

Diversifying Assumptions in Cryptography (2)

2

Quantum computation and cryptography



Quantum is usually a **threat** to cryptography

Can we use cryptography to **study quantum computation**?

- Cryptographic proofs of quantumness [BCMVV'18, Yamakawa-Zhandry'22]
- Classical verification of quantum computation [Mahadev'18]

What are the "right" complexity-theoretic foundations of quantum cryptography?

Standard complexity theory studies problems with **classical descriptions**
e.g. find a Hamiltonian cycle in a graph, break a *classical* ciphertext…

Need a new theory to reason about **inherently quantum problems**
e.g. breaking security of a *quantum* ciphertext

Integration in Teams

- DI-ENS, Paris, équipe CASCADE
  - David Pointcheval (elliptic curves, functional encryption…)
  - Phong Nguyen (lattices, quadratic forms…)
  - Brice Minaud (searchable encryption…)
  - Céline Chevalier (quantum uncloneable cryptography…)

- LIP6, Paris, équipe ALMASTY
  - Damien Vergnaud (randomness in cryptography, leakage-resilience...)
  - Charles Bouillaguet (alternate assumptions…)
  - QI team (e.g. Alex B. Grilo…) (foundations of quantum cryptography…)

Willy Quach

- Research area: **theory of cryptography**
  - Main axes: post-quantum security, advanced cryptosystems, foundations
  - Research project: **Diversifying sources of hardness in cryptography**
- 17 publications ("A* conferences": CRYPTO x6, EUROCRYPT x3, FOCS)
- 25 co-authors
- Program committees (PKC '23, CRYPTO '24, TCC'24)