SIGPwny x SIGQuantum: Quantum Cryptographic Primitives

Sasha Levinshteyn and Swetha Karthikeyan

A bit about SIGPwny

- Premier cybersecurity org within ACM

A bit about SIGPwny

- Premier cybersecurity org within ACM
- Offer general meetings, CTF team, Purple team, Embedded team

A bit about SIGPwny

- Premier cybersecurity org within ACM
- Offer general meetings, CTF team, Purple team, Embedded team
- Discord: https://discord.gg/cWcZ6a9

A bit about SIGPwny

- Premier cybersecurity org within ACM
- Offer general meetings, CTF team, Purple team, Embedded team
- Discord: https://discord.gg/cWcZ6a9
- All info available at https://sigpwny.com/

A bit about SIGPwny

- Premier cybersecurity org within ACM
- Offer general meetings, CTF team, Purple team, Embedded team
- Discord: https://discord.gg/cWcZ6a9
- All info available at https://sigpwny.com/
- Let us know if there is any content, collabs, or other events you would like to see from us!

A bit about SIGPwny

- Premier cybersecurity org within ACM
- Offer general meetings, CTF team, Purple team, Embedded team
- Discord: https://discord.gg/cWcZ6a9
- All info available at https://sigpwny.com/
- Let us know if there is any content, collabs, or other events you would like to see from us!

Outline

Impagliazzo's Five Worlds

Modern Cryptography

Classical and Quantum Cryptographic Primitives

Section 1

Impagliazzo's Five Worlds

Obligatory Complexity Speedrun

- A *decision problem* is a question with a yes-or-no-answer related to its inputs.

Obligatory Complexity Speedrun

- A *decision problem* is a question with a yes-or-no-answer related to its inputs.
- $\mathcal{P}$ is the class of decision problems that can be solved in polynomial time.

Obligatory Complexity Speedrun

- A *decision problem* is a question with a yes-or-no-answer related to its inputs.
- $\mathcal{P}$ is the class of decision problems that can be solved in polynomial time.
- $\mathcal{NP}$ is the class of decision problems that can be verified in polynomial time given a certificate/potential solution.

Obligatory Complexity Speedrun

- A *decision problem* is a question with a yes-or-no-answer related to its inputs.
- $\mathcal{P}$ is the class of decision problems that can be solved in polynomial time.
- $\mathcal{NP}$ is the class of decision problems that can be verified in polynomial time given a certificate/potential solution.
- So, if $\mathcal{P} \neq \mathcal{NP}$, there exists some decision problem that can be verified but not solved in polynomial time.

Obligatory Complexity Speedrun

- A *decision problem* is a question with a yes-or-no-answer related to its inputs.
- $\mathcal{P}$ is the class of decision problems that can be solved in polynomial time.
- $\mathcal{NP}$ is the class of decision problems that can be verified in polynomial time given a certificate/potential solution.
- So, if $\mathcal{P} \neq \mathcal{NP}$, there exists some decision problem that can be verified but not solved in polynomial time.
- However, if $\mathcal{P} = \mathcal{NP}$, every decision problem that can be efficiently verified can also be efficiently solved.

Impagliazzo's Five Worlds

- Cryptomania

Impagliazzo's Five Worlds

- Cryptomania
- Minicrypt

Impagliazzo's Five Worlds

- Cryptomania
- Minicrypt
- Pessiland

Impagliazzo's Five Worlds

- Cryptomania
- Minicrypt
- Pessiland
- Heuristica

Impagliazzo's Five Worlds

- Cryptomania
- Minicrypt
- Pessiland
- Heuristica
- Algorithmica

Cryptomania

- Public key cryptography exists.

Cryptomania

- Public key cryptography exists.
- As a result, one-way functions exist and secure multi-party computation is possible.

Cryptomania

- Public key cryptography exists.
- As a result, one-way functions exist and secure multi-party computation is possible.
- We cannot efficiently solve $\mathcal{NP}$ problems.

Minicrypt

- One-way functions exist but public key cryptography does not.

Minicrypt

- One-way functions exist but public key cryptography does not.
- RSA cannot be trusted.

Pessiland

- One-way functions do not exist but problems in $\mathcal{NP}$ are not easy on average.

Pessiland

- One-way functions do not exist but problems in $\mathcal{NP}$ are not easy on average.
- It is easy to come up with hard unsolved problems but hard to come up with solved instances.

Pessiland

- One-way functions do not exist but problems in $\mathcal{NP}$ are not easy on average.
- It is easy to come up with hard unsolved problems but hard to come up with solved instances.
- Classical cryptography doesn't exist but we can't solve algorithms quickly either.

Heuristica

- Problems in $\mathcal{NP}$ are still hard in the worst case but all problems encountered in reality can be solved in polynomial time.

Heuristica

- Problems in $\mathcal{NP}$ are still hard in the worst case but all problems encountered in reality can be solved in polynomial time.
- Classical cryptography is dead.

Algorithmica

- $\mathcal{P} = \mathcal{NP}$

Algorithmica

- $\mathcal{P} = \mathcal{NP}$
- Many optimization problems, as well as other kinds of problems, become easy.

Algorithmica

- $\mathcal{P} = \mathcal{NP}$
- Many optimization problems, as well as other kinds of problems, become easy.
- One-way functions do not exist (as they are in $\mathcal{NP}$) and classical cryptography is very, very dead.

Section 2

Modern Cryptography

Secure Cryptography

- Can secure cryptography exist?

Secure Cryptography

- Can secure cryptography exist?
- How do we prove that it does (or doesn't)?

The State of Modern Classical Cryptography

- We have several main encryption methods.

The State of Modern Classical Cryptography

- We have several main encryption methods.
  - RSA

The State of Modern Classical Cryptography

- We have several main encryption methods.
  - RSA
  - Diffie-Hellman

The State of Modern Classical Cryptography

- We have several main encryption methods.
  - RSA
  - Diffie-Hellman
- They all rely on assumptions about the hardness of specific algebraic problems, called *hardness assumptions*.

The State of Modern Classical Cryptography

- We have several main encryption methods.
  - RSA
  - Diffie-Hellman
- They all rely on assumptions about the hardness of specific algebraic problems, called *hardness assumptions*.
  - Factoring

The State of Modern Classical Cryptography

- We have several main encryption methods.
  - RSA
  - Diffie-Hellman
- They all rely on assumptions about the hardness of specific algebraic problems, called *hardness assumptions*.
  - Factoring
  - Discrete log problem

The State of Modern Classical Cryptography

- We have several main encryption methods.
  - RSA
  - Diffie-Hellman
- They all rely on assumptions about the hardness of specific algebraic problems, called *hardness assumptions.*
  - Factoring
  - Discrete log problem
- What happens if these hardness assumptions are wrong?

Complexity Theoretic Approach

- Ideally, we would like to assume as little as possible while being able to do as much as possible.

Cryptographic Primitives

- *Cryptographic primitives* are common, simple cryptographic algorithms/routines that are used to build up more complicated cryptographic protocols.

Cryptographic Primitives

- *Cryptographic primitives* are common, simple cryptographic algorithms/routines that are used to build up more complicated cryptographic protocols.
  - Each cryptographic primitive does a specific task in a very specific way.

Cryptographic Primitives

- *Cryptographic primitives* are common, simple cryptographic algorithms/routines that are used to build up more complicated cryptographic protocols.
  - Each cryptographic primitive does a specific task in a very specific way.
  - To build an effective cryptographic system from these building blocks, the cryptographic primitives need to be extremely reliable.

Complexity Theoretic Approach

- Ideally, we would like to assume as little as possible while being able to do as much as possible.

Complexity Theoretic Approach

- Ideally, we would like to assume as little as possible while being able to do as much as possible.
- General Idea

Complexity Theoretic Approach

- Ideally, we would like to assume as little as possible while being able to do as much as possible.
- General Idea
  - Find the weakest possible complexity assumption (such as *insert cryptographic primitive here* exists).

Complexity Theoretic Approach

- Ideally, we would like to assume as little as possible while being able to do as much as possible.
- General Idea
  - Find the weakest possible complexity assumption (such as *insert cryptographic primitive here* exists).
  - Build as many cryptographic primitives from this assumption as possible.

Complexity Theoretic Approach

- Ideally, we would like to assume as little as possible while being able to do as much as possible.
- General Idea
  - Find the weakest possible complexity assumption (such as *insert cryptographic primitive here* exists).
  - Build as many cryptographic primitives from this assumption as possible.
- Determine which primitives imply which other primitives.

Complexity Theoretic Approach

- Ideally, we would like to assume as little as possible while being able to do as much as possible.
- General Idea
  - Find the weakest possible complexity assumption (such as *insert cryptographic primitive here* exists).
  - Build as many cryptographic primitives from this assumption as possible.
- Determine which primitives imply which other primitives.
  - A primitive P implies another primitive Q if the ability to build P can be manipulated in some way to build Q.

Section 3

Classical and Quantum Cryptographic Primitives

Intro to Quantum

- A *polynomial-time quantum algorithm* is an algorithm that runs in polynomial time on a quantum computer.
- A *quantum state* is essentially a superposition over 'classical states' (bitstrings). We write these as vectors.
- The *inner product* of two quantum states is basically a dot product over the two vectors representing how close the two states are.
- The *no-cloning theorem* states that given a quantum state, you cannot copy it, resulting in two identical quantum states.

One-Way Functions

- A *one-way function* is a function that is easy to compute given any input but hard to invert given the output of a random input.

One-Way Functions

- A *one-way function* is a function that is easy to compute given any input but hard to invert given the output of a random input.
- A function $f : \{0,1\}^* \to \{0,1\}^*$ is one-way if f can be computed by a polynomial-time algorithm but any polynomial-time randomized algorithm F that attempts to compute a pseudo-inverse for f succeeds with negligible probability.

One-Way Functions

- A *one-way function* is a function that is easy to compute given any input but hard to invert given the output of a random input.
- A function $f : \{0,1\}^* \to \{0,1\}^*$ is one-way if f can be computed by a polynomial-time algorithm but any polynomial-time randomized algorithm F that attempts to compute a pseudo-inverse for f succeeds with negligible probability.
- Candidates: Multiplication and factoring, discrete exponential and logarithm, etc.

One-Way State Generators

- A *one-way state generator* is a quantum polynomial algorithm that outputs a quantum state $|\phi_k\rangle$ given classical bit string input k.

One-Way State Generators

- A *one-way state generator* is a quantum polynomial algorithm that outputs a quantum state $|\phi_k\rangle$ given classical bit string input k.
- It must be hard to find k' such that $|\langle\phi_k|\phi_{k'}\rangle|^2$ is non-negligible given polynomially many copies of $|\phi_k\rangle$.

One-Way State Generators

- A *one-way state generator* is a quantum polynomial algorithm that outputs a quantum state $|\phi_k\rangle$ given classical bit string input k.
- It must be hard to find k' such that $|\langle\phi_k|\phi_{k'}\rangle|^2$ is non-negligible given polynomially many copies of $|\phi_k\rangle$.
- These are the quantum analog of one-way functions.

Pseudorandom Generators

- A *pseudorandom generator* for a class of statistical tests is a deterministic procedure that maps a random seed to a longer pseudorandom string such that no statistical test in the class can distinguish between the output of the generator and the uniform distribution.

Pseudorandom Generators

- A *pseudorandom generator* for a class of statistical tests is a deterministic procedure that maps a random seed to a longer pseudorandom string such that no statistical test in the class can distinguish between the output of the generator and the uniform distribution.
- Let $\mathcal{A} = \{A : \{0,1\}^* \to \{0,1\}^*\}$ be a class of statistical tests/algorithms the pseudorandom generator will try to get past.

Pseudorandom Generators

- A *pseudorandom generator* for a class of statistical tests is a deterministic procedure that maps a random seed to a longer pseudorandom string such that no statistical test in the class can distinguish between the output of the generator and the uniform distribution.
- Let $\mathcal{A} = \{A : \{0,1\}^* \to \{0,1\}^*\}$ be a class of statistical tests/algorithms the pseudorandom generator will try to get past.
- A function $G : \{0,1\}^l \to \{0,1\}^n$ with $l < n$ is a pseudorandom generator against $\mathcal{A}$ with bias ε if, for every A in $\mathcal{A}$, the statistical distance between the distributions $A(G(U_l))$ and $A(U_n)$ is at most ε.

Pseudorandom Generators

- A *pseudorandom generator* for a class of statistical tests is a deterministic procedure that maps a random seed to a longer pseudorandom string such that no statistical test in the class can distinguish between the output of the generator and the uniform distribution.
- Let $\mathcal{A} = \{A : \{0,1\}^* \to \{0,1\}^*\}$ be a class of statistical tests/algorithms the pseudorandom generator will try to get past.
- A function $G : \{0,1\}^l \to \{0,1\}^n$ with $l < n$ is a pseudorandom generator against $\mathcal{A}$ with bias ε if, for every A in $\mathcal{A}$, the statistical distance between the distributions $A(G(U_l))$ and $A(U_n)$ is at most ε.
- Pseudorandom generators exist iff one-way functions exist.

Pseudorandom State Generators

- *Pseudorandom state generators* are efficient algorithms that produce states that are computationally indistinguishable from Haar random states.

Pseudorandom State Generators

- *Pseudorandom state generators* are efficient algorithms that produce states that are computationally indistinguishable from Haar random states.
- *Haar random states* are quantum states that are sampled uniformly from the entire state space of a system according to the Haar measure.

Pseudorandom State Generators

- *Pseudorandom state generators* are efficient algorithms that produce states that are computationally indistinguishable from Haar random states.
- *Haar random states* are quantum states that are sampled uniformly from the entire state space of a system according to the Haar measure.
- The *Haar measure* is a way to define a uniform probability distribution over the group of unitary operators.
- These are the quantum analog of pseudorandom generators.

Digital Signatures

- A *digital signature* is a scheme for verifying the authenticity of a digital message.

Digital Signatures

- A *digital signature* is a scheme for verifying the authenticity of a digital message.
- Three (probabilistic polynomial time) Algorithms (G, S, V)

Digital Signatures

- A *digital signature* is a scheme for verifying the authenticity of a digital message.
- Three (probabilistic polynomial time) Algorithms (G, S, V)
  - Key generation - G generates a public key pk and a corresponding private key sk on input 1^n

Digital Signatures

- A *digital signature* is a scheme for verifying the authenticity of a digital message.
- Three (probabilistic polynomial time) Algorithms (G, S, V)
  - Key generation - G generates a public key pk and a corresponding private key sk on input 1^n
  - Signing - S returns a tag t after being given the private key sk and a string x

Digital Signatures

- A *digital signature* is a scheme for verifying the authenticity of a digital message.
- Three (probabilistic polynomial time) Algorithms (G, S, V)
  - Key generation - G generates a public key pk and a corresponding private key sk on input 1^n
  - Signing - S returns a tag t after being given the private key sk and a string x
  - Signature verifying - V accepts or rejects depending on the inputs of the public key pk, a string x, and a tag t

Digital Signatures

- A *digital signature* is a scheme for verifying the authenticity of a digital message.
- Three (probabilistic polynomial time) Algorithms (G, S, V)
  - Key generation - G generates a public key pk and a corresponding private key sk on input 1^n
  - Signing - S returns a tag t after being given the private key sk and a string x
  - Signature verifying - V accepts or rejects depending on the inputs of the public key pk, a string x, and a tag t
- The probability that a polynomial time adversary A can generate a valid signature for a party without knowing that party's private key should be negligible.

Quantum Money Mini-Schemes

- A *quantum money mini-scheme* is a scheme for verifying if quantum money is authentic, ensuring that no one can forge quantum money.

Quantum Money Mini-Schemes

- A *quantum money mini-scheme* is a scheme for verifying if quantum money is authentic, ensuring that no one can forge quantum money.
- Money is represented by unique quantum states that cannot be duplicated due to the *no-cloning theorem*.

Quantum Money Mini-Schemes

- A *quantum money mini-scheme* is a scheme for verifying if quantum money is authentic, ensuring that no one can forge quantum money.
- Money is represented by unique quantum states that cannot be duplicated due to the *no-cloning theorem*.
- Critical Properties

Quantum Money Mini-Schemes

- A *quantum money mini-scheme* is a scheme for verifying if quantum money is authentic, ensuring that no one can forge quantum money.
- Money is represented by unique quantum states that cannot be duplicated due to the *no-cloning theorem*.
- Critical Properties
  - No adversary should be able to forge quantum money by replicating the quantum states.

Quantum Money Mini-Schemes

- A *quantum money mini-scheme* is a scheme for verifying if quantum money is authentic, ensuring that no one can forge quantum money.
- Money is represented by unique quantum states that cannot be duplicated due to the *no-cloning theorem*.
- Critical Properties
  - No adversary should be able to forge quantum money by replicating the quantum states.
  - There must be a verification mechanism that allows the owner of the money to check if the quantum money is authentic without revealing the associated quantum state, typically by measuring the state in a way that doesn't destroy its information.

Quantum Money Mini-Schemes

- A *quantum money mini-scheme* is a scheme for verifying if quantum money is authentic, ensuring that no one can forge quantum money.
- Money is represented by unique quantum states that cannot be duplicated due to the *no-cloning theorem*.
- Critical Properties
  - No adversary should be able to forge quantum money by replicating the quantum states.
  - There must be a verification mechanism that allows the owner of the money to check if the quantum money is authentic without revealing the associated quantum state, typically by measuring the state in a way that doesn't destroy its information.
- These are the quantum analog of digital signatures.

EFI Pairs

- *EFI pairs* are pairs of efficiently samplable quantum states that are both statistically far but computationally indistinguishable.

EFI Pairs

- *EFI pairs* are pairs of efficiently samplable quantum states that are both statistically far but computationally indistinguishable.
- Once a value is committed using one of the EFI pair states, it cannot be altered.

EFI Pairs

- *EFI pairs* are pairs of efficiently samplable quantum states that are both statistically far but computationally indistinguishable.
- Once a value is committed using one of the EFI pair states, it cannot be altered.
- Computational indistinguishability ensures that the EFI pair states are kept hidden.

EFI Pairs

- *EFI pairs* are pairs of efficiently samplable quantum states that are both statistically far but computationally indistinguishable.
- Once a value is committed using one of the EFI pair states, it cannot be altered.
- Computational indistinguishability ensures that the EFI pair states are kept hidden.

Minimum Assumption in Classical Cryptography

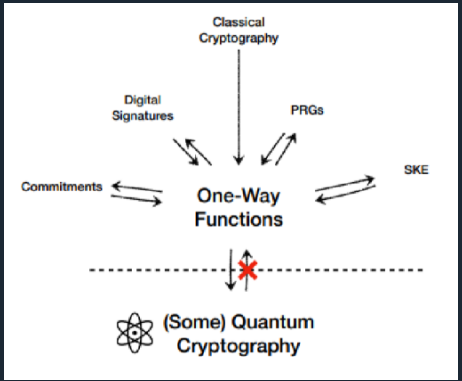
- Every classical cryptographic primitive implies one-way functions.

Minimum Assumption in Classical Cryptography

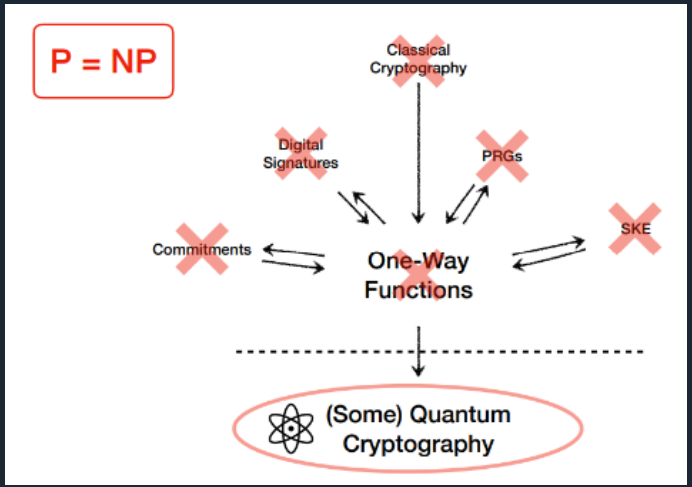
- Every classical cryptographic primitive implies one-way functions.
- Thus, one-way functions are the weakest assumption in classical cryptography.

Minimum Assumption in Classical Cryptography

- Every classical cryptographic primitive implies one-way functions.
- Thus, one-way functions are the weakest assumption in classical cryptography.



Nightmare Scenario for Cryptography



Minimum Assumptions in Quantum Cryptography

- Quantum cryptography can still work in the nightmare scenario.
- For instance, Quantum Key Distribution (QKD) gets its security from the Laws of Physics.

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

Conclusion

- Quantum cryptography can still exist when classical cryptography absolutely fails.

Conclusion

- Quantum cryptography can still exist when classical cryptography absolutely fails.
- Associating classical cryptographic primitives is a huge field of study.

Conclusion

- Quantum cryptography can still exist when classical cryptography absolutely fails.
- Associating classical cryptographic primitives is a huge field of study.
- Researchers are now working on relating quantum cryptographic primitives.

Conclusion

- Quantum cryptography can still exist when classical cryptography absolutely fails.
- Associating classical cryptographic primitives is a huge field of study.
- Researchers are now working on relating quantum cryptographic primitives.
- One-way state generators and EFI pairs are the likely minimum assumptions in quantum cryptography. [KT24]

SIGQuantum

- Join SIGQuantum!!! We meet Tuesdays 6 - 7 pm.
- We run weekly meetings, as well as some projects and Hackathons!
- Find the Discord through the ACM Discord or website.

Bibliography I

Dakshita Khurana and Kabit Tomer.

Commitments from quantum one-wayness.

https://doi.org/10.48550/arXiv.2310.11526, 2024.

Accessed: 09-17-2024.