University of Minho
School of Engineering

Multi-Party Computation: Providing a Post-Quantum Solution (part 1)

quantUM Seminars

Henrique Faria

HasLab
Departement of Informatic Engeneering
University of Minho

March 3, 2023

Overview

University of Minho
School of Engineering

1. Basic notions
2. Symmetric & Assymetric Encryption
3. Impact of Post-Quantum Attacks
4. Solutions to Post-Quantum Attacks
5. Multi-Party Computation

What is Cryptography?

- Cryptography (...), is the practice and study of techniques for secure communication in the presence of adversarial behavior".

What is Cryptography?

- Cryptography (...), is the practice and study of techniques to ensure the confidentiality, integrity, authentication and non-repudiation of messages in the presence of adversarial behavior".

  Confidentiality: keep sensitive information private.

  Integrity: Assure the data received is valid.

  Authentication: Prove who you are.

  Non-repudiation: Emmiter can not deny sending a message.

Security is a Belief System

University of Minho
School of Engineering

In Cryptography we work with hard problems.

A good example: inverting hash functions ($h : \{0,1\}^m \rightarrow \{0,1\}^n$).

Pre-image resistance: Given an output y it is infisible to find any input x such that $h(x) = y$.

Second pre-image resistance: For a given specific input x_1 it is infisible to find an input x_2 such that $h(x_1) = h(x_2)$.

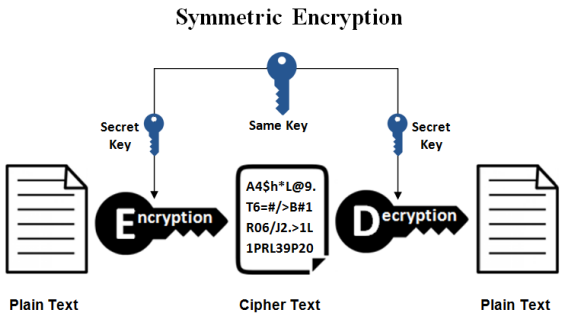
Collision resistance: It is hard to find any two inputs x_1 and x_2 such that $h(x_1) = h(x_2)$.

Let us toss a coin!

Symmetric Encryption

Symmetric Encryption

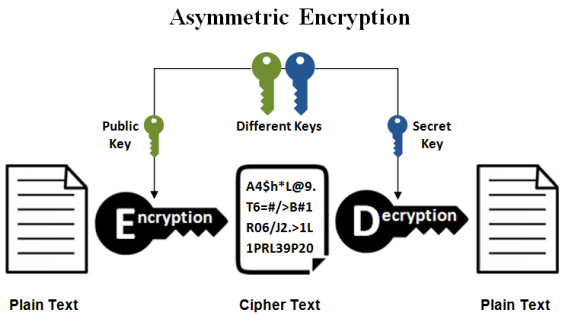
- Emmiter and receiver have the same key.
- Fast with short signatures.



Asymmetric Encryption

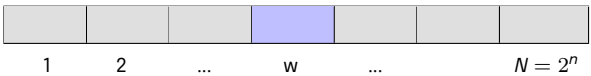
Asymmetric Encryption

- Emmiter and receiver both have a key-pair.
- Slow with big signatures.



Post-Quantum Attacks: Grover's Algorithm

$f : \{0,1\}^m \rightarrow \{0,1\}^n$



- Brute-force approach: 2^{n-1}
- Grover's algorithm: $2^{\frac{n}{2}}$

- Solution: Double key space ($2^{\frac{2n}{2}}$).

Post-Quantum Attacks: Shor's Algorithm

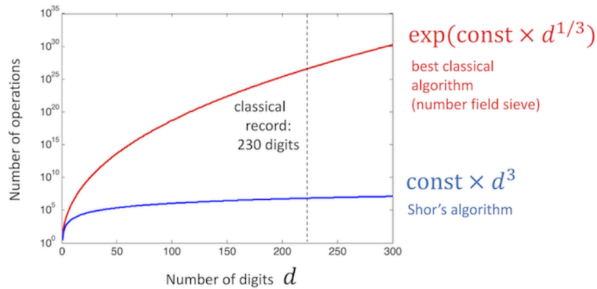
University of Minho
School of Engineering

Factor an integer *N* with *d* decimal digits

Brute force approach: 2^d (exponential in the number of digits *d*)

General Number Field Sieve approach: $2^{\sqrt[3]{d}}$

Shor's algorithm: d^3



NIST-PQC

In 2017, the American National Institute of Standards And Technologies (NIST) released a contest to find and standardize post-quantum secure schemes (NIST-PQC).

Key Encapsulation Mechanisms (KEM)

Digital Signature Schemes (DSS)

Key Encapsulation Mechanisms (KEM)

University of Minho
School of Engineering

Chosen to Standardize:

- CRYSTALS-Kyber (Lattice-based)

Postponed to the 4° round:

- BIKE (Bit Flipping Key Encapsulation)
- Classic McEliece (Binary Goppa Code)
- HQC (Hamming Quasi-Cyclic)
- SIKE (Supersingular Isogeny Key Encapsulation)

Digital Signature Schemes

Chosen to Standardize:

- CRYSTALS-Dilithium (Lattice-based)
- Falcon (Lattice-based)
- SPHINCS+ (hash-based)

All other schemes were dropped!

NIST is due to start a new competition to find and standardize new Digital Signature Schemes (NIST-PQC: DSS).

Why is MPC a solution

PICNIC (Multi-Party Computation) was also present in the 3° round.

- PICNIC was faster than SPHINCS+ but had larger signatures.
- "Obtaining further improvements under the same paradigm as Picnic (...) may (...) lead to a signature scheme with significantly better performance than the current design."
- In recent several other MPC schemes appeared with significant improments on PICNIC's signature size and speed.

Multi-Party Computation (MPC)

Multiple parties computing a function's output jointly while keeping their respective shares private.

A = 45

B = 65

C = 75

Avg(A,B,C) = 61.7

Multi-Party Computation (MPC)

Imagine we have three players:

Alice: 45
Bob: 65
Charlie: 75

Objective: Compute the average of their incomes without revealing those incomes.

Multi-Party Computation (MPC)

University of Minho
School of Engineering

First step: Each player divides its incomes into three shares.

Alice: 45 $\rightarrow$ (-11, 24, 32)
Bob: 65 $\rightarrow$ (35, 45, -15)
Charlie: 75 $\rightarrow$ (10, 15, 50)

Second Step: Each player shares two of his/hers three shares.

Players	Alice	Bob	Charlie	Income
Alice	-11	24	32	45
Bob	35	45	-15	65
Charlie	10	15	50	75

Multi-Party Computation (MPC)

Third step: Sum each players' new shares.

Players	A	B	C	Income
Alice	-11	24	32	45
Bob	35	45	-15	65
Charlie	10	15	50	75
Computed Values	34	84	67	-

Fourth step: Compute the average of the new values.

Avg(45,65,75) = Avg(34,74,67) = 61,7

Multi-Party Computation in the head

Depending of the channel used latency can increase or decrease.

- Talking
- Email
- Letters

Solution: Do multi party computations in the head (Alice, Bob and Charlie become fictional).

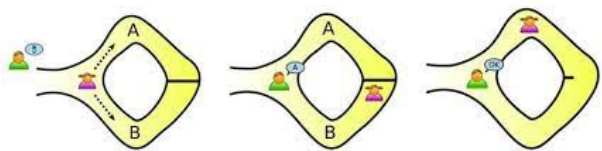
Zero-Knowledge MPC

Zero-knowledge: Revealing we know a secret without disclosing it.

Bob want to go around the tunnel but does not know the pin code.

Alice knows the pin code and will sell it to Bob.

Bob wants to make sure Alice actually knows the secret code before paying.



University of Minho
School of Engineering

Multi-Party Computation: Providing a Post-Quantum Solution (part 1)

quantUM Seminars

Henrique Faria

HasLab
Departement of Informatic Engeneering
University of Minho

March 3, 2023