POST QUANTUM CRYPTOGRAPHY

Applied Cryptography

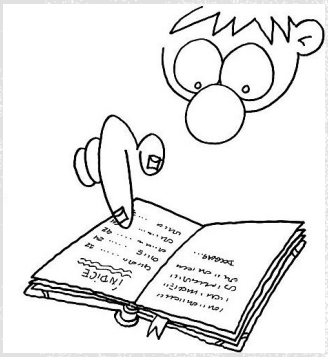
Silvio Ranise [silvio.ranise@unitn.it or *ranise@fbk.eu*]

ST SECURITY & TRUST

FONDAZIONE BRUNO KESSLER

CONTENTS

- Overview
- Quantum computing
- Relevance to cryptography
  - Shor and Grover algorithms
- Is quantum computing relevant to cryptography?
- Post Quantum Cryptography (PQC)
- NIST Approach to PQC



OVERVIEW

Symmetric key cryptography

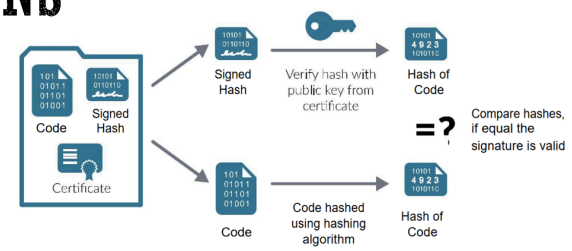
- Block/Stream Cipher
  - Encryption of data
  - Confidentiality/Secrecy
- Message Authentication Codes
  - Authentication of data
  - Authenticity
- Hash function
  - Cryptographic checksum
  - Allows efficient comparison

Public key cryptography

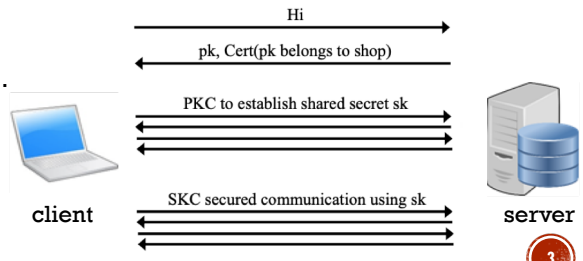
- Digital signature
  - Proof of authorship
  - Authentication & Non-repudiation
- Public-key encryption & key exchange
  - Establishment of shared secret key
  - Confidentiality/Secrecy

SELECTED APPLICATIONS

- Code signing (Signatures)
  - Software updates
  - Software distribution
  - Mobile code



- Communication security (PKI)
  - TLS, SSH, ...
  - eCommerce, online banking, eGovernment, ...
  - Private online communication



TODAY CRYPTO ECOSYSTEM

- Symmetric key cryptography
  - Wide range of different schemes
  - Based on design principles rather than hard mathematical problems
- Public key cryptography
  - Deployed schemes are based on RSA-factorization and discrete logarithm problem
    - Including Diffie-Hellman and Elliptic Curves
  - Based on computationally hard problems

WHAT HAPPENS IF THE TWO PROBLEMS ARE SOLVED?

Potentially dramatic impact…

- No (practical) secure communication
- No online payment
- No e-Commerce
- No Internet privacy (this is questionable, recall Tor)
- No private online communication
  - with insurance company, public institutions, etc.
  - with private contacts (this includes messaging applications although these are already questionable today…)
- Everyone in same WiFi network can listen to your connection

6 QUANTUM COMPUTING

A HIGH LEVEL CHARACTERIZATION

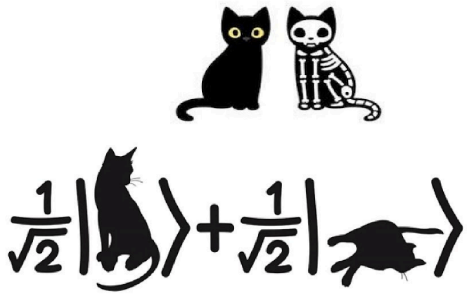
- *Quantum computing is the use of quantum phenomena such as superposition and entanglement to perform computation. […]* ***Quantum computers are believed to be able to solve certain computational problems, such as integer factorization (which underlies RSA encryption), substantially faster than classical computers***

https://en.wikipedia.org/wiki/Quantum_computing

- **Superposition** refers to a combination of states we would ordinarily describe independently.
  - To make a classical analogy, if you play two musical notes at once, what you will hear is a superposition of the two notes
- **Entanglement** is a famously counter-intuitive quantum phenomenon describing behaviour we never see in the classical world.
  - Entangled particles behave together as a system in ways that cannot be explained using classical logic

ON SUPERPOSITION

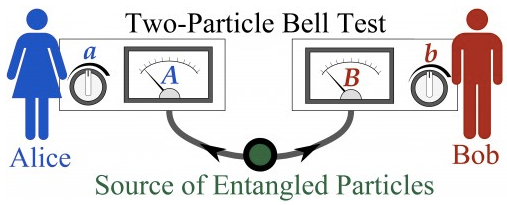
Schrodinger's Cat



- Quantum computing is based on the fact that tiny particles, such as electrons, can simultaneously take on *states* that we would normally deem mutually exclusive
  - For instance, they can be in several places at once
- We never see this *superposition* of different states in ordinary life because it somehow disappears once a system is observed: when you measure the location of an electron, all but one of the possible alternatives are eliminated and you will see just one

https://www.youtube.com/watch?v=UjaAxUO6-Uw

ON ENTAGLEMENT



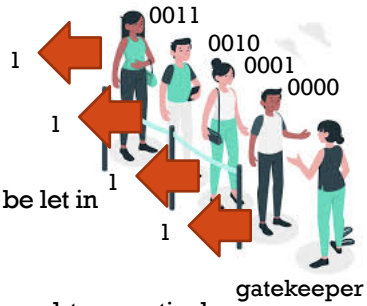
https://www.newswise.com/articles/researchers-limit-experimental-free-will-to-fake-quantum-entanglement

- There is more to quantum physics than just superposition
- If you look at a system of more than one qubit, then the individual components are not generally independent of each other; instead, they can be *entangled*
- When you measure one of the qubits in an entangled system of two qubits, for example, then the outcome — whether you see a 0 or a 1 — immediately tells you what you will see when you measure the other qubit
- Particles can be entangled even if they are separated in space, a fact that caused Einstein to call entanglement "spooky action at a distance"

SUPERPOSITION & ENTANGLEMENT FOR QUANTUM COMPUTING

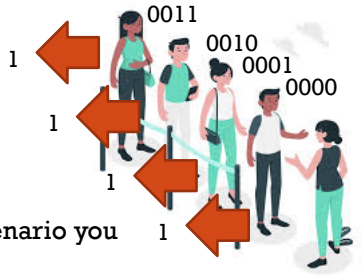
- A quantum computer works with particles, representing quantum bits (qubits), that can be in superposition
  - I.e. qubits can take on the value 0, or 1, or both **simultaneously**
- Entanglement implies that a quantum computer cannot be described using classical information theory since its states are not simply the result of stringing together the descriptions of the individual qubits but you need to describe all the *correlations* between the different qubits
- As you increase the number of qubits, the number of those correlations grows exponentially: for n qubits there are 2^n correlations
- While a quantum algorithm can take entangled qubits in superposition as input, the output will also usually be a quantum state — and such a state will generally change as soon as you try to observe it
- The art of quantum computing is to find ways of gaining as much information as possible from the unobservable

AN EXAMPLE (1)



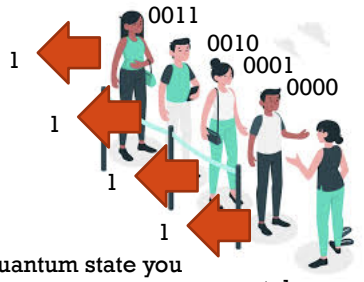
- Imagine a line of people waiting at a gate to see whether they will be let in
- The has labelled all the people with numbers written in binary
- Assume there are $2^3 = 8$ people in line
- The gatekeeper records her decision to let a person in by allocating a 1 to a particular bit-string and 0 otherwise
  - I.e. the gatekeeper defines a Boolean function
- It is unknown what the gatekeeper is going to decide to do with each individual, but we know there are two possible outcomes
  - the gatekeeper lets everybody in (every bit-string gets allocated a 1)
  - the gatekeeper lets exactly half the people in (half of bit-strings get allocated a 0 and the other half a 1)
- The problem is to find whether the gatekeeper lets everybody or only half of the people in
- How many values of the gatekeeper's Boolean function do you need to look up to find out which of the two alternatives it is?

AN EXAMPLE (2)



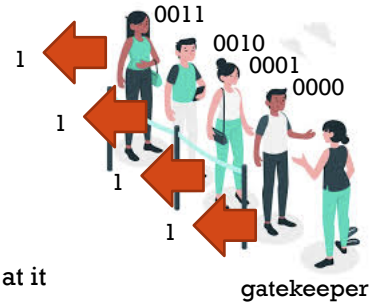
- If you work like a classical computer, then in the worst-case scenario you will have to look the function up to 5 five times
  - Even if you see a 1 allocated to the first 4 bit-strings you check, you still cannot be sure that *all* the bit-strings come with a 1: there is still the possibility that it is only half of them, so you do need that 5th look-up
- If you have a quantum computer you can get it to look up the function value for all the eight people *simultaneously*, so you only need one look-up
- For a line consisting of 2^n individuals,
  - a classical computer would need to look up the function $2^{n-1}+1$ times, a number that grows very quickly with n
  - a quantum computer would always only need to look once

AN EXAMPLE (3)



- Notice that
  - your eight simultaneously-looked-up values will be encoded in a quantum state you cannot actually read, since any measurement of it will disturb it
- Luckily, though, you are not trying to find out what will happen to each individual but only want to know whether the gatekeeper will let everybody in or only half of the people
- In other words, it is a matter of answering only a single yes-no question and that requires to extract only a small amount of information about a lot of values
- It is possible to perform an extra operation on your quantum state, one which teases the simple piece of information you are after into just the right places for you to be able to read it off

AN EXAMPLE (4)



- The situation can be explained by means of a metaphor
- It is like a house of cards that will collapse as soon as you look at it
- You might never be able to see it in its full glory, but if it was constructed in just the right way, you may at least be able to ascertain some information on what it looked like from the collapsed heap
  - That is one reason why quantum computers are more powerful than classical ones
- In summary, to find even simple patterns or structures within systems of many components, contrary to a classical computer that must consider them one after the other, a quantum computer can evaluate all of them simultaneously
- Although you may not be able to read off all those individual values, you can often extract just enough information to glean a pattern in them

More information at https://plus.maths.org/content/really-how-do-quantum-computers-work

NOISE IN QUANTUM COMPUTING (1)

- Noise is the central obstacle to building large-scale quantum computers
- The problem can be explained with a metaphor
  - qubits are like can of beers
- It is easy to carry a six-pack of unopened beers around
  - One can walk, run, hop, skip, and jump and it is unlikely he will spill any of the unopened beverages
- Once opened, the barriers to the liquid inside are no more in place and it becomes more difficult to carry all six open containers without spilling anything
- The situation becomes more and more difficult, until it is no more manageable, as soon as we start doubling the number of cans
- Quantum decoherence happens when qubits (cans) lose information (beer) to the environment (spilling) over *time*
- The "timer" does not start until we try to do something with qubits, like measure them or perform a computation
- The second we open a can of quantum, it begins to lose its fizz as decoherence sets in

NOISE IN QUANTUM COMPUTING (2)

- In other words, there is a certain threshold for noise (called fault tolerance) where quantum computers will theoretically be reliable enough to be considered useful
- Arguably, error-correction is the biggest impediment to crossing the 100-qubit barrier
- Some experts say that we will never overcome the noise problem
- Others say that we will overcome it by using artificial intelligence
  - The idea is to use machine learning algorithms that are capable of correcting errors by learning
  - For more information, see the paper at https://arxiv.org/abs/1802.05267

TO SUM UP

"Every time you make the measurement, you destroy the entangled state."

https://spectrum.ieee.org/tech-talk/computing/hardware/20-entangled-qubits-brings-the-quantum-computer-closer

- Qubits carry huge amount of information until they are observe
- Unfortunately, to learn the result of computation one has to measure and….
- … this collapses qubits to basis state, i.e. 1 qubit leads 1 classical bit of information
- The game is to increase the number of qubits while allowing for extracting useful information from quantum states
- IBM
  - 2020: 65 qubits
  - 2021: 127 qubits
  - 2022: 433 qubits
  - 2023: 1,000 qubits
- Google
  - 2018: 72 qubits
  - in 10 years: 1 million qubits

Quantum supremacy is the goal of demonstrating that a programmable quantum device can solve a problem that no classical computer can solve in any feasible amount of time (irrespective of the usefulness of the problem)

https://science.sciencemag.org/content/sci/early/2020/12/02/science.abe8770.full.pdf

18

RELEVANCE TO CRYPTOGRAPHY

SHOR ALGORITHM (1994)

- Algorithm composed of two parts
  - first turns the factoring problem into the problem of finding the period of a function (may be implemented classically)
  - second finds the period using the quantum Fourier transform (responsible for the quantum speedup)

- **Polynomial-time quantum computer algorithm for integer factorization**
  - Problem: Given an integer *N*, find its prime factors
  - Complexity: polynomial in *log(N)*
  - Exponentially faster than the most efficient known classical factoring algorithm, the general number field sieve method
- If a quantum computer with a sufficient number of qubits could operate without succumbing to quantum noise and other quantum-decoherence phenomena, then Shor's algorithm could be used to break public-key cryptography schemes, such as the widely used RSA scheme
- Shor's algorithm shows that factoring integers is efficient on an ideal quantum computer, so it may be feasible to defeat RSA by constructing a large quantum computer
- In 2001, Shor algorithm was demonstrated on a quantum computer at IBM to factorize 15
- In 2019, 21 was factorized using Shor algorithm on a quantum computer

https://www.scottaaronson.com/blog/?p=208

19

GROVER ALGORITHM (1996)

- Quantum computer algorithm that finds with high probability the unique input to a black box function that produces a particular output value, using just $O(\sqrt{N})$ evaluations of the function where N is the size of the function domain
- The analogous problem in classical computation cannot be solved in fewer than $O(N)$ evaluations
  - Since the Nth-member of the domain can be the right one
- Unlike Shor algorithms, which provides an exponential speedup, Grover's algorithm provides only a quadratic speedup
- Even quadratic speedup is considerable when N is large
- Grover's algorithm could brute-force a 128-bit symmetric cryptographic key in roughly *2^(64)* iterations, or a 256-bit key in roughly *2^(128)* iterations
- It is sometimes suggested that symmetric key lengths be doubled to protect against future quantum attacks

21

SO, IS QUANTUM COMPUTING RELEVANT AT ALL TO CRYPTOGRAPHY?

RISK ASSESSMENT (1)

- Let k be the number of years for which the keys need to be secure
- Let i be the number of years to harden cryptographic infrastructure to be secure against quantum computer attacks
- Let q be the number of years to build a large scale quantum computer

If $q<k+i$ then quantum computing is relevant

- Contrast these two laws
  - **Moore's law** (roughly) states that computing power doubles every two years
    - Exponential
  - **Neven's law**: quantum computers are gaining computational power on classical ones at a doubly exponential rate
    - Double exponential

RISK ASSESSMENT (2)

- Two root cases for Neven law

1. Quantum computers have an intrinsic exponential advantage over classical ones
   - If a quantum circuit has four quantum bits, it takes a classical circuit with 16 ordinary bits to achieve equivalent computational power
   - This would be true even if quantum technology never improved
2. Rapid improvement of quantum processors
   - Neven says that Google's best quantum chips have recently been improving at an exponential rate because of a reduction in the error rate in the quantum circuits
   - Reducing the error rate has allowed the engineers to build larger quantum processors

- No general agreement on this view
- In any case, quantum computing is improving at a rapid pace…

RISK ASSESSMENT (3)

Quantum computing technology is improving because of substantial funding

- The European Union launched a one billion Euro project on quantum technologies
- Similar range is spent in China
- The United States administration passed a bill on spending $1.275 billion US dollar on quantum computing research
- Google, IBM, Microsoft, Alibaba, and others run their own research programs
- So, it is better to start worrying about the security of cryptography now

In a nutshell
- Quantum computers are powerful but not almighty
- They can be used to break some crypto but not all
  - Deployed asymmetric falls
  - Symmetric survives
- Unclear when large scale QC's ready

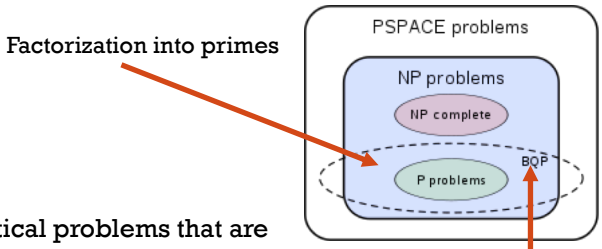
QUANTUM KEY DISTRIBUTION (QKD)

- Protocols for key sharing based on quantum principles
- Key observation
  - The security of encryption that uses quantum key distribution relies on the foundations of quantum mechanics and not on computationally difficult problems
- Quantum key distribution enables two communicating users to detect the presence of any third party trying to gain knowledge of the key
- This is because the process of measuring a quantum system disturbs the system
  - A third party trying to eavesdrop on the key must in some way measure it, thus introducing detectable anomalies
- The main drawback of Quantum Key Distribution is that it usually relies on having an authenticated classical channel of communications
- Having an authenticated classical channel means that one has already exchanged
  - either a symmetric key of sufficient length
  - or public keys of sufficient security level
- With such information already available, one can achieve authenticated and secure communications **without using QKD**

26

POST QUANTUM CRYPTOGRAPHY (PQC)

IDEA & SETUP



- Design cryptosystems based on mathematical problems that are **not** solvable by Shor algorithm
- There are several possible alternatives
  - Lattices
  - Error-correcting codes
  - Multivariate polynomials
  - Hash functions
  - Elliptic curve isogenies
  - …
- Since 2015, NIST is actively researching new, quantum-resistant algorithms to improve and extend its official standards which are binding for all federal entities, including Digital signatures and Key exchange protocols

Bounded-error quantum polynomial time (BQP) is the class of decision problems solvable by a quantum computer in polynomial time, with an error probability of at most 1/3 for all instances

Arbitrary value, complexity class does not change if we take exponentially small values in the size of the input

27

CONJECTURED QUANTUM-SECURE PROBLEMS

- Solving multivariate quadratic equations
  - Multivariate Crypto
- Bounded-distance decoding (BDD)
  - Code-based crypto
- Short(est) and close(st) vector problem
  - Lattice-based crypto
- Breaking security of symmetric primitives (SHA-x-, AES-,... problem)
  - Hash-based signatures / symmetric crypto
- For an introduction, see the book at

https://www.e-reading-lib.com/bookreader.php/135832/Bernstein,_Buchmann,_Dahmen_-_Post_Quantum_Cryptography.pdf

29

NIST APPROACH

NIST: REQUIREMENTS ON PQC

- **Public-key encryption**: shall include algorithms for key generation, encryption, and decryption
  - Bottom line, the scheme shall support the encryption and decryption of messages that contain symmetric keys of length at least 256 bits
- ***Key encapsulation mechanism (KEM)***: shall include algorithms for key generation, encapsulation, and decapsulation.
  - Bottom line, KEM shall support the establishment of shared keys of length at least 256 bits
- **Digital signature**: shall include algorithms for key generation, signature generation and signature verification
  - The scheme shall be capable of supporting a message size up to *2^(63)* bits

NIST: SECURITY LEVELS

- Any attack that breaks the relevant security definition must require computational resources comparable to or greater than those required for

1. key search on a block cipher with a 128-bit key (e.g., AES128)
2. collision search on a 256-bit hash function (e.g., SHA256/SHA3-256)
3. key search on a block cipher with a 192-bit key (e.g., AES192)
4. collision search on a 384-bit hash function (e.g., SHA384/SHA3-384)
5. key search on a block cipher with a 256-bit key (e.g., AES 256)

FINAL SUBMISSIONS RECEIVED

- The deadline is past – no more submissions
- 82 total submissions received
  - 23 signature schemes
  - 59 Encryption/KEM schemes

2017

	Signatures	KEM/Encryption	Overall
Lattice-based	4	24	28
Code-based	5	19	24
Multi-variate	7	6	13
Hash-based	4		4
Other	3	10	13
Total	23	59	82

S.

32

NIST: SELECTION IN ROUNDS

- In Round **1**, NIST analyzed the **security** of proposals
- In January 2019, **26 proposals** have been admitted to Round 2
- In July 2020, **15 proposals** have been admitted to Round 3
- NIST head of the selection committee said
  - "*The likely outcome is that at the end of this third round, we will standardize one or two algorithms for encryption and key establishment, and one or two others for digital signatures. But by the time we are finished, the review process will have been going on for five or six years, and someone may have had a good idea in the interim. So we'll find a way to look at newer approaches too.*"
- Details can be found in the document available at

  https://csrc.nist.gov/publications/detail/nistir/8309/final

S. Ranise - Security & Trust (FBK)

33

HOWEVER…

- One of the algorithms selected for further study was SIKE (Supersingular Isogeny Key Encapsulation)
- SIKE is a key encapsulation (KEM) algorithm based upon a fundamentally different approach (Supersingular Isogeny) than the lattice-based Kyber algorithms chosen for KEM applications
- Researchers at KU Leuven have published a preliminary paper claiming they were able to find an **efficient key recovery attack for using a single core processor in about one hour's time with Magma**
  - Sometimes these deficiencies can be fixed by small modifications to the algorithm
  - But if it cannot be fixed, then the SIKE algorithm will be dropped from further consideration for PQC standardization
- Right now, it is still too early in the process to know what the ultimate fate of the SIKE algorithm will be. But it certainly makes the case for using **crypto-agility** so algorithms can be changed out easily if a problem is found

Full details at https://eprint.iacr.org/2022/975