Should We Start Preparing for Post-Quantum Crypto?

By Martin Rupp
SCIENTIFIC AND COMPUTER DEVELOPMENT SCD LTD

Introduction: With the arrival of the first quantum computers - while still imperfect, cryptologists from all around the world have started to ring the alarm bell: If a quantum computer is built, it can crack many of the widely used cryptography present in everyday life in several industries, including the banking industries. Here we aim at presenting facts regarding whether or not it is realistic to start already preparing for a Post-Quantum cryptographic migration.

What are Quantum Computers and what is Quantum Cryptography?

Quantum physics studies phenomena, mostly energy phenomena that occur at a very small scale in the matter. The theory was developed in the early 1900s by Max Planck, a German physicist, to explain phenomena at a subatomic level that classical physics could not explain.

Quantum physics is a hard field, and especially a very active field of research. Particle accelerators and synchrotrons are technologies that are almost entirely based on quantum physics.

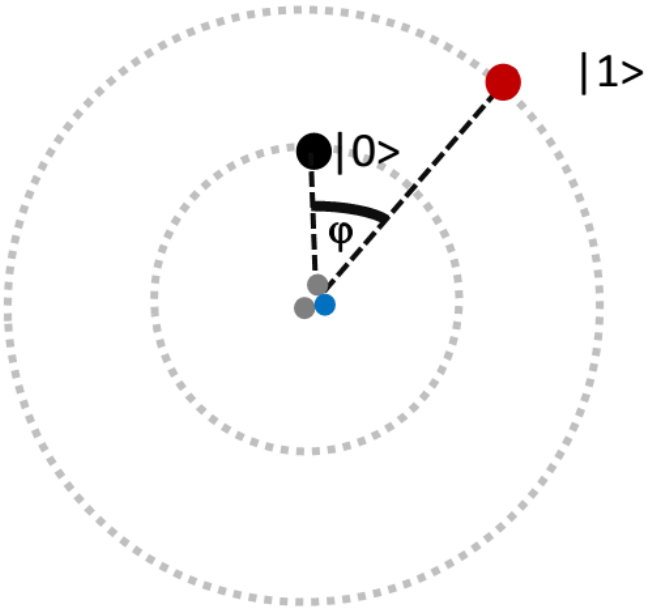
Quantum physics does not generally use a deterministic approach but rather a probabilistic one. This is mainly due to the very nature of quantum physics in which parameters cannot be measured without significantly perturbing the whole system.

The incertitude principle of Heisenberg when applied to the subatomic level is partly responsible for this.

Therefore quantum physics uses tools such as Wave functions and superpositions of states to describe the physics at subatomic levels.

In other terms a quantum system, usually subatomic particles such as electrons, photons, neutrons, bosons, fermions etc… will be described by a probabilistic model where the number of states and the probability they are actually in a given state is computed.

If we take a very simple model, the simplest quantum system with two states, where a particle can have two states **0** or **1**:



The wave function ψ is described by a superposition of state **0** with probability *a*<1 and **1** with probability *1-a*.

$$|\psi >= \sqrt{a}|0 >+ \sqrt{1 - a}.\quad exp(i\varphi)\,|1 >$$

The above equation uses the bra-ket notations. $|0 >$ and $|1 >$ are the Hilbert basis of the two-dimensional Hilbert space representing the wave functions.

The wave function is a function of the time t. The above equation implies that:

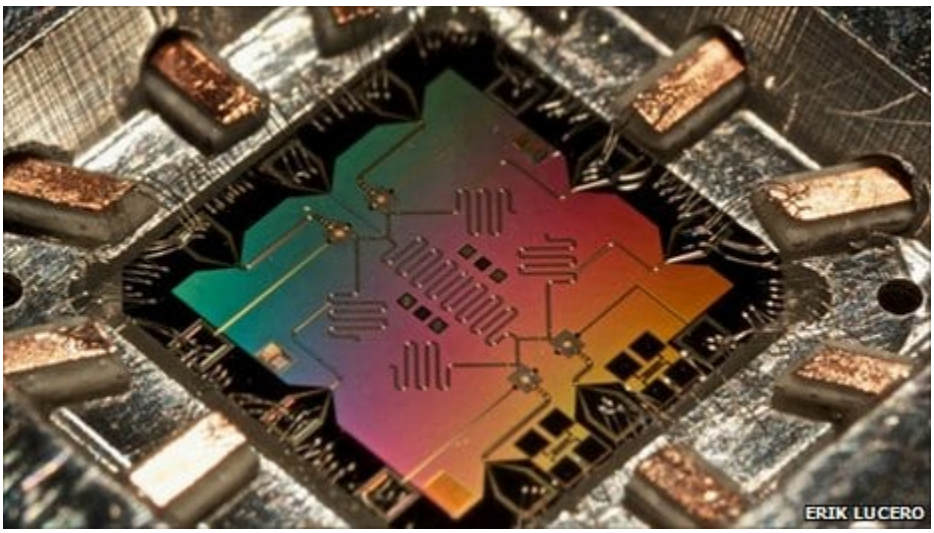
$$_{\psi}(t)=\sqrt{a}0(\psi) + (\sqrt{1 - a})exp(i\varphi)1(\psi)$$

Roughly and with great simplification, this is the physical property that quantum computers are using to create quantum computing.

While a digital computer works with *two* bits 0 and 1, quantum computers work with qubits- quantum bits. An n-quantum bit is a series of n-states of the wave function. What we just described previously is a 2-qubit (that we call simply the qubit).

From this, recently, quantum chips have been created using quantum circuits. Qubits encode information differently from digital bits and they can encode larger quantities of data. Anyway, the n-qubits are different than "just" n simultaneous bits[1]. We just want to give the reader a very basic overview and understanding of what a quantum computer is.

Here is a picture of a quantum processor using transmon superconducting qubits.



Quantum computers are being built - as of 2019 - and are still imperfect due to heavy noise.

IBM for example and the Fraunhofer Institute are very actively researching and building quantum computers.

[1] There are n-bits computers, they have been developed decades ago like the Ternary computers. They have nothing to do with quantum computing (the first electronic ternary computer was built in 1958 in the USSR) , however developing ternary quantum computers is possible.

Google, Rigetti, and D-Wave are among the other companies which are providing quantum computers.

Microsoft developed the Q# programming language to design and implement quantum algorithms.

Next, we investigate why Quantum computers are a threat to our "modern" cryptography.

Why Quantum Computers are a Threat to the actual cryptography

"Modern" cryptography results from the works of Alan Turing and a team of Polish cryptographers led by Marian Adam Rejewski whose combined efforts in the 30' and 40's resulted in breaking the "Enigma' German machine, which was an electro-mechanical computer.

Cryptography usually uses ciphering techniques where you must solve a challenge. If you have the key, solving the challenge is easy. If you do not have the key, solving the challenge is hard. And this is how hard it is to solve the challenge without the key which determines how secure a cipher is.

In the past, ciphers looked like puzzles with symbols being scrambled with hidden logic. That hidden logic was the key. It evolved to so-called 'modern' cryptography where the logic used to scramble the information (aka 'the cipher algorithm') is no more the real challenge, but to reverse a mathematical system

Using a Turing machine and therefore digital computers to cipher and decipher messages became our actual cryptography, post-WWII cryptography.

Messages are made up of bytes that are scrambled, combined with cryptographic keys (which are made up of bytes themselves as well), and transformed by all sorts of diffusion mechanisms until the output becomes a stream of apparently random bytes.

The Data Encryption Standard (DES/3-DES) is a product of such techniques, using so-called substitution tables (S-Tables).

Other techniques involve number theories such as Fermat's little theorem to produce what is known as the RSA public key cryptography system.

3DES (symmetric key algorithm) and RSA (asymmetric key algorithm) are among the encryption algorithms which are the most widely used all over the world. Emails, Web servers, ATMs, Credit Card Chip transactions (EMV), and many military encryption systems are for example using one or both of these algorithms.

Shor's Algorithm

Before any Quantum computer was even built, in the '80s, the power of quantum cryptography was studied, mainly by the physicist Richard Feynman. Shortly after, the mathematician Peter Shor described an algorithm that is using quantum computing to factor an integer into its prime factors (Shor's Algorithm).

That algorithm involves the creation of dedicated quantum circuits with the quantum Fourier Transform having a central role in it. It was proved that the time needed by the algorithm to factor numbers is polynomial, meaning that it is not a complex challenge in terms of quantum crypto. The RSA is therefore vulnerable to such attacks.

Given an integer N, find its prime factors P1,..., Pn. The problem is extremely simple to understand but extremely hard to solve. The best-known algorithm using 'conventional' digital computers is GNFS (general number field sieve) and it takes a time of

$$\mathbf{T}(b)=O\left(e^{\sqrt[3]{\frac{64}{9}b.log\left(b^2\right)}}\right)$$

to factor a b-bit integer! On a quantum computer, using Shor's algorithm, it takes only a time of

$$\mathbf{T}(b)=O\left(b^3\right).$$

To have a better understanding of the difference, we may consider that it will take time of

$$\mathbf{T}=10\ldots\ldots\ldots\ldots0 \text{ sec}$$

$$\leftarrow \ldots \sqrt[3]{b}\ 0's \ldots \rightarrow$$

to factor an integer coded with b bits on a digital computer while it will take a time of

$$\mathbf{T}=10\ldots\ldots\ldots\ldots 0 \text{ sec}$$

$$\leftarrow \ldots log(b)\ 0's \ldots \rightarrow$$

to factor it on a quantum computer...

With a 400-bit number, we see that we need a time of 1,000,000,000 seconds to break it on a digital computer, while it will take 10,000,000 seconds to break it on a quantum computer. Of course, that time is relative to one CPU or one core.

But it means that roughly if it takes **31 years for a digital computer to factor a 400-bit integer then it will take only 115 days for a quantum computer … to do the same!**

“Fast" Factoring a number into primes is equivalent to breaking RSA. Therefore a quantum computer can break most RSA ciphers on the planet unless they would be using ridiculously huge key sizes (which would dramatically slow down the RSA ciphering and deciphering operations).

Grover’s Algorithm

Grover's algorithm, the same as Schor's algorithm, can break 3DES using a probabilistic iterative method.

What is Post-Quantum cryptography?

As long as Quantum computers existed only on paper, there was no real matter for the cryptographers to be concerned about. Now, as the threat of a "real" quantum computer being built is becoming more and more possible, the rules of the game have changed... according to the US National Institute of Standards and Technology (NIST)

"*Researchers working on building a quantum computer have estimated that it is likely that a quantum computer capable of breaking 2000-bit RSA in a matter of hours could be built by 2030 for a budget of about a billion dollars.*"

Post-Quantum cryptography consists in migrating from what are considered theoretically weak cipher algorithms to what are considered theoretically as strong cipher algorithms regarding quantum computing.

Most Post-Quantum algorithms are using the following technique to make sure they are “Quantum proof”:

Lattice-Based Cryptography

Lattices are "just" Z-basis over an n-dimensional manifold. They can be easily visualized as equidistant grids like for example, a metal mesh. Such mathematical objects have been studied by Gauss or Minkowski during the past centuries. Lattice and elliptic curves are deeply connected with the most complex number theory problems. For instance, it took an incredible amount of work over hundreds of years to solve the Big Fermat Conjecture as it was linked to a special type of elliptic curve. Therefore, many problems involving lattices are among the hardest mathematical challenges known and for which there are no solutions. The only solution is an exhaustive search, which is unfeasible even for the most powerful quantum computer.

Learning with Error (LWE)

The learning with error problem consists in totally recreating or as close as possible, a function over a finite ring knowing only a given sample of that function, and some of these samples may be intentionally erroneous. This is linked to the general techniques used in Monte-Carlo methods to reconstruct laws of unknown phenomena given a set of samples. It is difficult to recreate such functions with samples with errors. That difficulty is the base of the security behind all LWE Post-Quantum crypto.

Isogeny Graphs

Isogeny is a transformation between elliptic curves which is slightly more than isomorphisms (where the j-invariant is the same). Supersingular curves are then special objects that lie all in a unique isogeny class. From that, supersingular isogeny graphs are created where vertices are the supersingular objects and where edges are

isogenies. It is extremely difficult to find paths inside these graphs so this is the base of all isogeny-related post-quantum crypto.

In general, all these algorithms are using the latest developments in algebraic geometry, which is the hardest field in research math.

The security of these algorithms is based on the assumed fact that if the human brain still could not break these challenges, a quantum computer won't be able to do it either, and will only be left with the option of an exhaustive search.

We could not rule out that, by following the same logic, Post-quantum crypto will, some days, use for instance, Lie groups or even Universal Teichmuller theory (when that theory becomes more understandable).

Here is a list of recommended quantum-proof algorithms:

- FrodoDH and frodoKEM, a Ring Learning With Errors (R-LWE) encryption and key exchange algorithm;

- SIDH, aka Supersingular Isogeny Diffie–Hellman key exchange, is an elliptic curve-based key exchange algorithm using the fact that the isogeny group of a supersingular elliptic curve is non-abelian;

- NewHopeDH, another Ring-Learning-with-Errors key exchange protocol;

- McEliece (Classic), an old asymmetric encryption algorithm relying on Goppa error code;

- SIKE, aka Supersingular Isogeny Key Encapsulation, using random walks on isogeny graphs; (note: broken in 2023)

- Kyber, a CRYSTAL (Cryptographic Suite for Algebraic Lattices) algorithm for key encapsulation using LWE;

- NTRU prime, another R-LWE cipher algorithm;

- Dilithium, the other CRYSTAL algorithm using the “Fiat-Shamir with Aborts” technique in lattice-based cryptography.

Should we start already to prepare for Post-Quantum cryptography?

The motivation to start preparing for a migration to quantum-proof algorithms is that cryptosystems may have dozens of years of the life of use and may still be in use when quantum computers can break them.

Nevertheless, should companies start preparing for something which is supposed to happen in about 10 to 20 years? We all know about the Greenhouse effect and the prediction of climatic changes. Their consequences may by far overpass the threat of a quantum computer… So should companies in Silicon Valley start to relocate to the mountains to prevent being destroyed by a possible tsunami that may occur in the next 10 years, as a result of climatic changes? Not to mention preparing for a global economic crisis or even a third world war whose effects would certainly make the fears for a full quantum computer being created look quite futile.

Quantum computers are real, yet they are still not able to break anything, or at least not significantly.

Besides, there is no real proof that quantum-resistant algorithms are resistant because there are simply no quantum computers to test them.

If an effective quantum computer were to be built, it would be created by a large country, namely the USA, China or Europe, or Russia. These countries already have a lot of intelligence allowing them to break cryptosystems using malware, trojans, or simply forcing designers to create backdoors into their cryptographic algorithms. So in a nutshell this would not be used by the average hacker group operating on the darknet.

There are therefore few reasons to start worrying about such a “threat”. Besides there are other sorts of computers being actively developed such as neuronal or biological computers which may use complex AI and who may have the ability to break the quantum-proof algorithms.

The rise of non-digital computers is a fact and when they will be able to break our "modern cryptography", it will be time to think of next-generation cryptography, post-digital cryptography.