For U & Me | Basics

A Cyber Security Perspective on Quantum Computing

By **Pradip Mukhopadhyay** - April 8, 2020

Along with the immense promise of quantum computing come the enhanced security threats too. This has opened up a whole new field known as post quantum security.

In his famous book ‘Across the Frontiers’ Werner Heisenberg wrote, “Not only is the Universe stranger than we think, it is stranger than we can think.” This quote is applicable to quantum computing, because of its promise and ability to solve otherwise non-solvable, complex problems in the classical computing world.

It’s not that quantum computing promises to speed up the processing of every individual instruction, thus defying Moore’s Law. But it promises to quickly solve the exponentially repetitive tasks, e.g., finding out two prime factors of a given big integer number. This makes it a potential

threat to the known cyber security universe – a threat to a computer's hardware, software and stored information. It's a potential threat to our existing cyber security concepts and techniques.

In this article we are going to review such a threat to gain a deeper understanding about it; we can then arrive at our own opinions, independently.

Figures 1 and 2 indicate the potential of the so-called quantum threat and the global investments in quantum computing, with China leading the pack.

Figure 1: Quantum threat timeline

Existing security techniques

Let's look at the current cyber security techniques. One obvious method of cracking an encryption code is brute force. A hacker can keep on trying all possible combinations till the code is broken. This method is not practical as it requires years to try out all combinations of the key. Currently, security across networks is based on a public key encryption system. Some well-known techniques are Diffie-Hellman, elliptic curve, RSA, etc.

Let us look at RSA. It is related to getting the private key by continuously factoring the public key, a big integer, into the product of two primes. Till now, this is non-trackable in the classical computer paradigm because it starts with a big enough integer — so it would take years to get the private key out, when compromised. Roughly, the key generation algorithm can be stated as below:

1. Get two equal sized random prime numbers, say p and q.
2. Make sure the product of p and q (let's call it n) is of the desired bit length, say 1024.
3. Let's compute the value of n and ǿ = (p-1) (q-1).
4. Let's select a proper integer e between 1 and ǿ.
5. Secret component derivation: d, again between 1 and ǿ, ω ed = 1 mod ǿ.
6. The public key part is (n, e) and private part is (d, p, q).
7. d, p, q and ǿ are secrets.

Figure 2: Investments in quantum computing

Quantum cyber security perspective

In this section we are going to discuss the proliferation of quantum computers in the cyber security space. The prime factorisation we discussed above, when tried out in classical computing, takes a very long time to be computed. This makes it practically invincible. We feel secure that our classical security model is intact and in place. However, that's not the case with the quantum computing paradigm. Figure 3 describes a mind-blowing comparison of prime factorisation across classical and quantum computing paradigms. The corresponding quantum computing prime factorisation algorithm is known as Shor's Algorithm.

Figure 3 vividly depicts the potential risks of the proliferation of quantum computing in the cyber security domain. To understand the contours of cyber security in the quantum age we need to first define what 'Quantum safe security' is.

Quantum safe security is often called 'post quantum security' as well. Just like the modelling of a security problem, let's start with the worst case scenario. Let's say the honest party has the classical computer and the adversary is quantum powered. Let's assume the adversary's quantum power does not necessarily exist today, since this can be a futuristic scenario also, to make the problem statement interesting. Now, in the classical world, we would like to build a security mechanism that cannot be compromised, even by the quantum powered adversary. So, winning in the unfavourable condition, is called post quantum security. This is one area attracting intense research interest today. Let's look at how to achieve such a post quantum security paradigm.

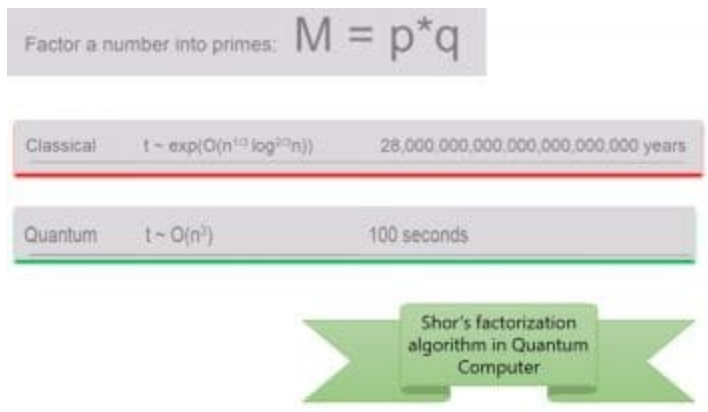

Figure 3: A comparison of computational time for prime factorisation in classical and quantum computing (Shor's algorithm

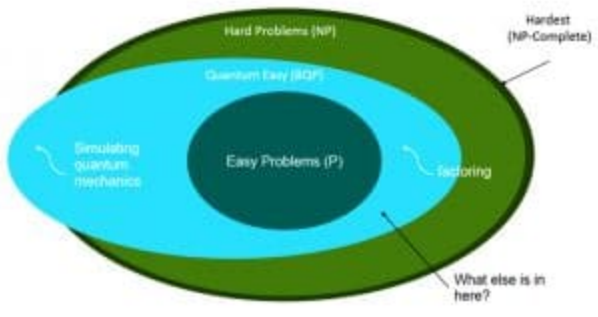

Figure 4: BQP solvability of quantum computers

To understand this seemingly unbelievable world of post quantum security, we need to understand what sort of problems a quantum computer can potentially solve. Can it solve any NP-complete problem? It cannot. Figure 4 depicts the BQP (Bounder Error Polynomial) time, which is the problem zone quantum computers can solve in polynomial time.

As we can see in this figure, there still exists an unsolvable zone which is called quantum hard. This means that it's beyond the capabilities of classical as well as quantum computers.

Now, intuitively, if we can devise our security primitives and constructs in that zone (i.e., the green coloured zone in Figure 4), then we are safe. Well, we are right, but only partially. Having security primitives in the green zone in Figure 4 is a necessary but not a sufficient condition to prove the quantum safety of the solution.

There are believed to be some security techniques available today that are promising in post quantum order, e.g., secret-key cryptography. However, the quantum property of the quantum computer, raises an additional security attack surface as well. One such example is the superposition attack. To put it in simple terms, superposition is a quantum property where a qubit (a bit in a quantum computer is called qubit) can pose 0, 1 or a mix of 0 and 1 values. Once you measure the qubit, it collapses to either classical 0 or classical 1. Now an adversary, powered by the quantum computer oracle, can potentially learn the superposition ciphertexts of some plain text and decipher the superposition using another algorithm (without directly measuring the superposition ciphertext) to acquire knowledge about the cryptosystem. That's it.

One can, of course, argue that to pose such a threat to our contemporary, classical security primitives, one needs to have a big enough (of many qubits), fault-tolerant and stable quantum computer. This will happen in the near future, but is not happening tomorrow. Then why should I have to bother about it, right now? The primary reasons are: an adversary can potentially steal your encrypted messages of today and

decipher them tomorrow, powered by the quantum oracle. So this sort of development requires a holistic research approach and an overhaul of the cryptographic infrastructure, which are time consuming. So it's better to start today.

Quantum gadgets

Is the picture painted very gloomy? Not really. There is a silver lining. We now have something called a quantum gadget which can be used to enhance the security of the classical communication primitives. One such example is quantum key distribution (QKD). The idea of QKD is derived from the fact that two honest parties can have a shared random secret key only known to them. If any adversary wants to intercept the secret random key, the adversary must read the key. Once a quantum state is read (i.e., measured) it collapses to one of the classical states – either 0 or 1. Hence any such adversary intrusion results in a detectable anomaly in the overall system.

There are other ways in which a quantum gadget can pave the way into our classical security systems and primitives, e.g., quantum fingerprints. One can think of it as a technique involving a quantum computer to generate a string like our classical cryptographic hash functions. There are various other examples also, but not limited to this—quantum random number generation, quantum signature generation, Byzantine agreement, quantum flip-the-coin, secure e-voting, secure multi-party computation, et al.

In a nutshell

Quantum computer research, as shown in Figure 2, is widespread across nations. One of the areas of immediate interest for research is related to making classical devices, communication and information to be adaptable and secure in the post quantum era. Basically, it means making them quantum safe. Of course, the journey has just started, so we are far from reaching any definitive answers.

TAGS opensource quantum computing

Previous article

A Starter Guide to Building Progressive Web Apps

Next article

SPA JS: Building Cross-Platform SPAs with Less Code

Pradip Mukhopadhyay

The author has 20 years of experience across the stack, from low level system programming to high level GUI. A FOSS enthusiast, he currently works for NetApp, Bengaluru.

RELATED ARTICLES

"Using open source means you're hiring the whole world as your...

Yashasvini Razdan - November 6, 2024

A Complete Guide to DevOps

Gopala Krishna Behara - November 4, 2024

Trusted Platform Modules: Locksmith in the Basement?

Aditya Mitra - November 1, 2024

NO COMMENTS

LEAVE A REPLY

Comment:

Name:*

Email:*

Website:

Save my name, email, and website in this browser for the next time I comment.

POST COMMENT

ABOUT US

Open Source For You is Asia's leading IT publication focused on open source technologies. Launched in February 2003 (as Linux For You), the magazine aims to help techies avail the benefits of open source software and solutions. Techies that connect with the magazine include software developers, IT managers, CIOs, hackers, etc. A free DVD, which contains the latest open source software and Linux distributions/OS, accompanies each issue of Open Source For You. The magazine is also associated with different events and online webinars on open source and related technologies.

FOLLOW US