Post-quantum Cryptography: Securing Data in the Age of Quantum Computers

As current security techniques like RSA and elliptic curves rely on mathematical problems vulnerable to quantum algorithms, the urgency to explore post-quantum cryptography alternatives becomes evident.

Published - July 31, 2023 04:23 pm IST

DEBAYAN GUPTA

Computation pervades today's world. From banking, to romance, to shopping, and even warfare, computers form one of the pillars of human civilization. However, there has been a lot of worry about quantum computing and its potential impact on computer security.

Governments and organisations across the world are rushing to develop quantum computing platforms and advanced security algorithms to defend against such machines. One prominent example of the latter is the U.S. National Institute of Standards and Technology's Post-Quantum Cryptography Standardization project. In India, Prime Minister Narendra Modi has recently announced collaborations with the U.S. in quantum computing and launched the National Quantum Mission. But, there is still much work to be done, both by the government and the industry. Data, as they say, is the new oil, and unless we protect ours, others will use it for their profit.

Much of our current security is based on techniques such as RSA, elliptic curves, Diffie-Hellman key exchange and almost all of them rely on a few "hard" mathematical problems, such as factorization and the discrete logarithm problem. Unfortunately, in 1994, Peter Shor developed a quantum algorithm that (with certain modifications) can break all of these with ease. Unless we find an unyielding barrier to the development of quantum computers, our security measures will eventually be broken.

While Shor's technique poses a threat to certain security algorithms, there are alternative methods that remain unaffected. Lov Grover's quantum algorithm, though impacting some of these to some extent, can often be fixed by increasing the key or password lengths. Fortunately, some common "symmetric" security algorithms like AES are not badly affected since they use the same password to lock and unlock the information.

Post-quantum cryptography involves exploring alternative techniques to counter vulnerabilities against quantum attacks. This need is more pressing than it initially sounds because attackers often record messages in case they can break them later. While Shor's algorithm poses particular concerns for certain methods, the field has rapidly evolved with promising approaches such as lattice algebra, multivariate cryptography, isogeny-based techniques, and code-based cryptography. This is a fast-changing field – one promising technique, supersingular isogeny Diffie-Hellman key exchange, was considered secure by many until it was utterly broken by Wouter Castryck and Thomas Decru last year.

It may be useful for the reader to gain a basic understanding of what a "quantum computer" is. Modern digital computers are all based on one idea: we make electricity do certain things using clever circuitry, and pretend that logical operations are occurring. "Pretend" is exactly the right word here. We could do the same thing with, say, water and pipes, by building some very clever piping mechanism or box (we computer scientists call these boxes "gates") with, say, three pipes, constructed so that the third pipe will release water if and only if both the first and the second have sufficient pressure. Then, we could pretend that this "water circuit" computes the answer to an "and" question. The same could be done with lasers, or even marbles rolling down wooden pathways with levers.

Of course, there's a reason we do this with electricity: we have developed circuits that can do logical computations incredibly fast and with astounding reliability. The idea of using electrical circuitry to implement two-valued logic is not as obvious as it sounds - it took many decades and some of the brightest minds on the planet to formalise this. In some sense, we are using physical reality (appropriately moulded and engineered) to simulate a logical statement.

But what if there are other bits of physics that could be useful? Perhaps if we built our circuits or gates using lasers, we could build new kinds of gates in addition to the basic ones – maybe a prism "naturally" computes a square root or something. As people explored these ideas, they found something amazing: the principles of quantum mechanics enabled a set of gates (at least mathematically) that were utterly impossible to build using electronics. In other words, using quantum states to represent logic (instead of high and low voltages, water pressure, etc.) allows us to compute very differently.

For example, one common classical gate is a "not" gate: this simply outputs the opposite of the input. A "true" input produces a "false" output, and vice versa. On a quantum computer, one could have a "square root of not" gate – something which would produce the opposite of the input, but only after passing through two such gates! This seems utterly incomprehensible. The mathematical principles involved are truly beautiful, which is why so many people are enamoured of these ideas.

This new, different kind of computation is very powerful, as it turns out. Many things that were complex and cumbersome when run on electronic logic become incredibly simple on a quantum system. Of course, this comes with its own problems, some of which have been solved, but many still remain. Current attempts are incredibly error-prone and have many missing pieces. In fact, we are probably decades away from a quantum computer powerful enough to do anything meaningful or dangerous. However, many experts believe that this is inevitable and we will eventually develop such machines. Given the advantage this will give to the first mover, it is important that we quickly and carefully transition to technologies secure against quantum attacks.

(Written by Debayan Gupta, Assistant Professor of Computer Science, Ashoka University)

Published – July 31, 2023 04:23 pm IST