Quantum Physics and Computing

Does quantum computing put our digital security at risk?

Robin Wilton • June 2020

The computers we use today are based on binary values (**"bits"**) representing a value of either 0 or 1. However, quantum computers use a quantum bit (**"qubit**"), which uses a property of sub-atomic particles to maintain (or **"superpose"**) different states at the same time. This means a qubit can be both 0 and 1 at the same time. A quantum computer can therefore compute multiple values at the same time, whereas a classical computer cannot. This could undermine the ways we use encryption to secure much of our digital life, from protecting confidential data like banking information to keeping our online communications private.

For instance, when trying to solve problems with multiple possible answers, picking the correct one will, statistically, take many tries by a classical computer. However, if a quantum computer can try all the possible solutions at once, the time it takes to find the right answer will drastically diminish. This can be applied to attack the two dominant forms of encryption used today: **symmetric** and **asymmetric**.

Quantum Computers and Encryption

Symmetric encryption uses a key to "lock" the data, and an identical key to "unlock" it: just like a petty cash box. One method of breaking symmetric encryption is an "exhaustive attack": the attacker tries every possible decryption key until they find the correct one.

Good symmetric encryption algorithms are designed to ensure, first, that without the key, the most efficient way to decrypt data is by exhaustive attack. They are also designed so that the number of possible keys is so huge that exhaustive attack is simply impractical for a classical computer. The amount of effort required (**"work factor"**) to mount an exhaustive attack can be quantified, based on the key length and the resources needed, like computing power, memory, energy and money. If the keys are long enough, the number of possible wrong answers is so colossal that the work factor exceeds practical limits of space and time. There might not be enough energy to power enough computers to do the work, or there might not be enough silicon to make enough computer chips to make the computers.

However, quantum computing would mean many possible keys can be tried simultaneously, and - combined with new ways of sorting through the results[1] - would greatly reduce the time needed to find the correct key. The reduction is so great that it's as if you had halved the length of the key used, reducing the difficulty of the problem to its square root. To give a trivial example - if the key length means there are 10,000 possible keys to try, halving the key length would reduce the work factor to having to try just 100 possible keys.

Asymmetric encryption uses one key to "lock" the data and a different key to "unlock" it, like locking a padlock. Anyone can close an open padlock, but only the person with the key or combination can open it again. Many communication protocols rely on asymmetric encryption, particularly to secure an initial exchange of symmetric keys between communicating partners.

Asymmetric encryption is based on mathematical operations which are easy to do in one direction, but harder to reverse. To illustrate: it is much easier to work out 1303x1307, than to work

1 For more on this aspect, look up "Grover's algorithm" for symmetric keys and "Shor's algorithm" for factorization-based asymmetric encryption.

out what two numbers you must multiply to get 1,703,021[2]. Attacks on this type of encryption are based on trying to solve these mathematical problems, rather than exhaustively searching for a key. Yet - as in the case of symmetric encryption - a combination of quantum computing and sorting techniques could significantly reduce the time and effort needed for an attack.

Quantum computing is not fatal for encryption ... yet

Practical challenges

The number of qubits in a working quantum computer has been increasing as technology improves, from around a dozen in 2010, to around 80 in 2019. But it is still short of the number needed to attack a 128-bit symmetric key, let alone a 4096-bit asymmetric one.

Based on a rule of thumb for what are currently considered "reasonably strong"[3] keys for each cryptographic algorithm type, the following table illustrates the number of qubits needed.

Algorithm type	Length of "reasonably strong" key	Number of qubits required per key bit	Total qubits required
Symmetric (e.g. AES)	128 bits	1	128
Elliptic Curve	256	~9	2304
RSA	3072	2 (plus 2 more)	6146

Figure 1: number of usable qubits needed for different algorithm types

Another challenge is that qubits tend to "decay", especially at room temperature. They need a lot of cooling, and are easily disrupted by electrical or environmental effects, and even each other. Stable usability is an issue, and solving it costs money.

If existing cryptographic mechanisms for encrypting and signing data are vulnerable to attack, then so is the data encrypted and signed using those techniques. We also rely on encryption to secure authentication. Entering your password to login to a website, entering your PIN to authorize a card transaction, even unlocking your car remotely: all these everyday actions are secured using encryption mechanisms. However, replacing obsolete components or unsafe mechanisms throughout an enterprise and network infrastructure is known to be a slow process. Migrating from one set of encryption algorithms to another typically involves technical, operational and procedural change across the organization, and competes for priority, resources, and budget, with day-to-day business activities.

If you have been storing encrypted archives of data over the years, imagine having to re-encrypt all those archives at short notice, because quantum cryptanalysis has suddenly made decryption feasible. Or imagine having to replace the digital signatures on an archive of long-term documents such as title deeds. Or reissuing physical keys for all cars of a particular model.

While quantum computing would potentially weaken popular asymmetric algorithms such as RSA and Elliptic Curve, research is identifying a number of quantum-resistant alternatives based on other kinds of mathematical problem[4].

What should stakeholders do?

Consumers may not be able to provide technical solutions, but we should understand the issues and express an informed view, given the opportunity, to decision-makers and service providers.

Since viable quantum computing would have the effect of halving the effective key length for symmetric algorithms, the obvious countermeasure for encryption product developers is to at least double the length of the keys used.

Decision-makers should ensure that encryption technology is treated as a critical element of IT infrastructure, with corresponding investment in governance, risk assessment, and planning. Their strategy should:

- Monitor developments in quantum computing and quantum-resistant encryption.
- Include encryption technology in regular organizational risk assessment cycles.

2 Note: Yes, you can multiply 1 and 1,703,021, but they don't count here, because 1 is not a very useful key.

3 "BlueKrypt" key length comparison tool: https://www.keylength.com/en/4/

4 This Wikipedia article gives pointers to some of the types of problem being considered: https://en.wikipedia.org/wiki/Post-quantum_cryptography

- Explore relevant national and regional guidance, such as that published by the US National Institute for Standards and Technology (Quantum encryption algorithm selection and validation[5]; guidance on cryptographic mechanisms[6];draft guidance on Getting Ready for Post-Quantum Cryptography[7]).
- Plan for the re-encryption of data-at-rest, and the re-signing of digitally signed artefacts.[8]
- Maximize algorithm agility in case a change of algorithms/ technology is needed, especially at short notice.[9]
- Cultivate the organisation's ability to refresh and deploy security technology in step with best practice.[10]
- Take care that superseded security technology is not able to persist in the infrastructure beyond its "safe use" period.