Issue 2 | 2020

EDPS

TECH DISPATCH

Quantum Computing and Cryptography

Quantum computers can be highly beneficial to scientific developments due to the new, speedy way of performing computing. Once available, they however could break currently used cryptography and undermine the protection of (personal) data.

I. What is quantum computing?

The physical laws of *quantum mechanics* allow for an alternative method to how today's computers process information. Whereas traditional computers use bits (0 or 1) as a building block, **quantum computers employ quantum bits, or qubits,** that can be at the same moment a combination of $|0\rangle$ and $|1\rangle$.

The possible spectrum of values one qubit can adopt is best depicted by the surface of the Bloch sphere in Figure 1. While bits allow for two discrete values, qubits can store a point in a two-dimensional continuum, a surface of a sphere. Quantum computing can take advantage of those more powerful qubits and carry out operations not only for a determined value $|0\rangle$ or $|1\rangle$, but also for **all possible superpositions at the same time**. Consequently, quantum computing attains an efficiency advantage over binary computing for selected tasks. Some tasks would be rendered only feasible due to this efficiency boost, if the appropriate quantum computer hardware were available.

In sum, quantum computers have a speed advantage over classical computers for selected problems and could therefore perform types of computation not available to current classical computers.

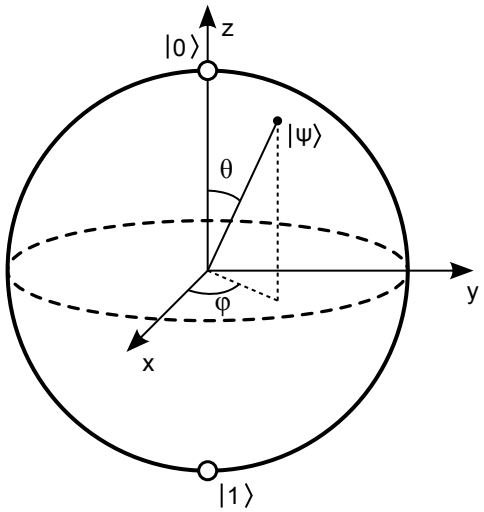

Figure 1: The Bloch sphere is a geometrical representation of a qubit. Qubits can take as value each point on the surface described by the two angles φ and θ. The pole points are $|0\rangle$ or $|1\rangle$.

II. What are the data protection issues?

There are many reasons why quantum computing could have significant implications for data protection in terms of **data security** and **confidentiality of communications**. One reason is the ability to **break cryptography**. Quantum computing can break many of today's classical cryptography and as such harm severely IT security. The risk extends to the core internet security protocols. Nearly all of today's systems that demand security, privacy or trust, would be affected.

II.1. Impact on public-key cryptography

Public-key cryptography, also known as asymmetric encryption, is a method of encrypting data with the

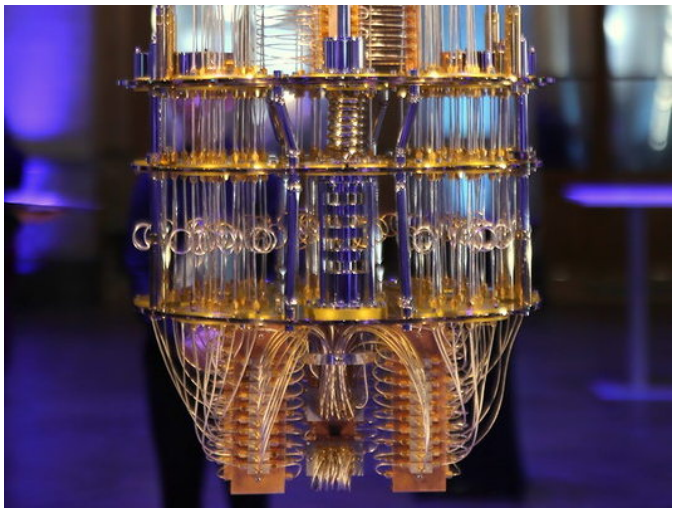

Figure 2: Quantum Computer IBM Q. Source: Pierre Metivier (detail, licensed under cc-by-nc 2.0)

use of cryptographic protocols based on algorithms. It requires two separate keys, a private and a public key. The Rivest-Sharmir-Adleman (RSA) algorithm is a cryptographic system that is used for public-key cryptography, and is commonly used when sending sensitive data over the internet. The RSA algorithm allows for both public and private keys to encrypt messages so their confidentiality and authenticity remain intact.

Quantum computers would allow for public-key cryptography systems to be jeopardised by adversaries in possession of a sufficiently powerful quantum computer, that could carry out the **decryption without prior knowledge of the private key**. Effected could be for instance digital signatures, essential Internet protocols like HTTPS (TLS) required for secure browsing, online banking, online shopping, etc.

II.2. Impact on symmetric cryptography

Quantum computing can also bring negative consequences for security guarantees of symmetric cryptography systems such as the Advanced Encryption Standard (AES). Asymmetric (e.g. RSA) and symmetric (e.g. AES) cryptography are often used together such as with the use of HTTPS. Symmetric cryptography needs practical ways of exchanging private keys in a confidential manner. To guarantee data security, the private key exchange must remain secure. But the **key exchange methods** used in practice today are based on problems that quantum computing may put at risk. To guarantee data confidentiality, the whole key exchange must remain secure.

II.3. Retrospective decryption

The technological progress in binary computing hardware, meaning today's widespread classic computers, is also a threat to IT security. With increasing computing power at decreasing costs, the **retrospective decryption of data from the past** becomes of use if the employed key lengths used at the time were sufficiently short. Security experts regularly call out for an increase of key lengths to keep data secure for a given period. Some governments' secret services are reported to collect data purposefully for future retrospective decryption. Quantum computers though follow different laws and would allow retrospective decryption in many cases much earlier.

II.4. Practical quantum computers

To be able to execute quantum algorithms with practical impacts, quantum computers would need to have thousands or millions of qubits with low error rates. This is something which is **beyond the reach of technology** in the foreseeable future.

In 2019, Google claimed to have demonstrated **quantum supremacy** with its 54-qubit quantum computer (Oliver 2019). The claim was that it took their quantum computer hundreds of seconds to perform computation that would take thousands of years for a powerful non-quantum supercomputer. While the solved task has no practical significance, it served as a proof of concept. It is likely that more similar results may be announced in this decade, but in the foreseeable future they will unlikely have a practical impact.

According to current understanding, to execute useful algorithms of practical relevance there is a need to build a quantum computer with more qubits and smaller error rates than what is possible today. The creation of a large and usable quantum computer within the next ten years is highly unlikely, but difficult to predict. It is this **unpredictability** that eventually leads to risks for IT security today.

II.5. Post-quantum cryptography

Post-quantum cryptography or quantum-safe cryptography refers to cryptography whose security is believed to be unaffected by quantum computers. This is achieved by the use of very different mathematical building blocks, which incorporate mathematical operations that quantum computers cannot solve more efficiently than other computers.

Post-quantum cryptography however will likely come with performance drawbacks and require larger computing resources to e.g. encrypt and decrypt data or sign and verify signatures and more networking resources to exchange lengthier keys and certificates. Post-quantum cryptography is not yet standardised. Sufficient and convincing knowledge must be available to conclude in a so-called cryptanalysis that such a solution is safe for both quantum and binary computing. The **US National Institute of Standards and Technology (NIST)** is working towards a Post-quantum cryptography standard and estimates to publish a draft with a first algorithm in 2022 or 2024. Once standardised, algorithms will need to be integrated with standard internet protocols like HTTPS.

As of 2020, prototypes of (non-standardised) postquantum cryptography are available for testing in the form of source code, software libraries (e.g. for OpenSSL), cloud services (e.g. Amazon AWS and Cloudflare) and consumer software (e.g. Google Chrome). It is estimated that a full transition could even take as long as 15-20 years in practice.

Organisations should consider for how long they need to guarantee absolute confidentiality of data and protection from retrospective decryption. Based on what we know today there is **no immediate threat posed by a quantum computer in the foreseeable future.** It may likely take decades to build a usable quantum computer that can execute known algorithms. But for data that needs to remain safe for very long, this uncertainty poses an issue that may require an early transition to post-quantum cryptography.

For this reason, some organisations may be interested in preparing appropriate risk assessment as well as contingency and migration plans. Such plans should always prioritise guaranteeing data security with respect to today's non-quantum security. When **transitioning to post-quantum systems**, organisations should consider existing risks and the usual considerations during migration of data that would guarantee data security (i.e. reliability, availability) as well as confidentiality (e.g. when the data is re-encrypted with post-quantum cryptography). The German Federal Office for Information Security (2020) has developed initial recommendations for the migration to post-quantum cryptography.

III. Recommended Reading

German Federal Office for Information Security (2020). *Post-Quantum Cryptography*.

Giles, Martin (2019). *Explainer: What is post-quantum cryptography?* In: *MIT Technology Review*.

Montanaro, Ashley (2016). *Quantum algorithms: an overview*. In: *npj Quantum Information* 2.1. DOI: 10.1038/npjqi.2015.23.

National Academies of Sciences, Engineering, and Medicine (2019). *Quantum Computing: Progress and Prospects*. The National Academies Press. DOI: 10.17226/25196.

Oliver, William D. (2019). *Quantum computing takes flight*. In: *Nature* 574.7779, pp. 487–488. DOI: 10.1038/d41586-019-03173-4.

Preskill, John (2018). *Quantum Computing in the NISQ era and beyond*. In: *Quantum* 2, p. 79. DOI: 10.22331/q-2018-08-06-79.

Shankland, Stephen (2019). *IBM's new 53-qubit quantum computer is its biggest yet*. In: *CNET*.

This publication is a brief report produced by the Technology and Privacy Unit of the European Data Protection Supervisor (EDPS). It aims to provide a factual description of an emerging technology and discuss its possible impacts on privacy and the protection of personal data. The contents of this publication do not imply a policy position of the EDPS.

Issue Author: Lukasz OLEJNIK, Robert RIEMANN
Editor: Thomas ZERDICK
Contact: techdispatch@edps.europa.eu

To subscribe or unsubscribe to the EDPS TechDispatch publications, please send a mail to techdispatch@edps.europa.eu. The data protection notice is online on the EDPS website.

ISSN 2599-932X
HTML: ISBN 978-92-9242-431-2
QT-AD-20-002-EN-Q
https://data.europa.eu/doi/10.2804/603798
PDF: ISBN 978-92-9242-432-9
QT-AD-20-002-EN-N
https://data.europa.eu/doi/10.2804/36404