



The Second
Quantum Revolution:
**The impact of quantum
computing and quantum
technologies on
law enforcement**



Acknowledgements

This report is a collaborative effort of the European Commission's Joint Research Centre (JRC), Europol's European Cybercrime Centre (EC3), and the Europol Innovation Lab.

THE SECOND QUANTUM REVOLUTION – THE IMPACT OF QUANTUM COMPUTING AND QUANTUM TECHNOLOGIES ON LAW ENFORCEMENT

An Observatory Report from the Europol Innovation Lab

PDF | ISBN 978-92-95220-92-8 | ISSN 2600-5182 | DOI: 10.2813/42230| QL-AS-23-001-EN-N

Neither the European Union Agency for Law Enforcement Cooperation nor any person acting on behalf of the agency is responsible for the use that might be made of the following information.

Luxembourg: Publications Office of the European Union, 2023

© **European Union Agency for Law Enforcement Cooperation, 2023**

Reproduction is authorised provided the source is acknowledged.

For any use or reproduction of photos or other material that is not under the copyright of the European Union Agency for Law Enforcement Cooperation, permission must be sought directly from the copyright holders.

While best efforts have been made to trace and acknowledge all copyright holders, Europol would like to apologise should there have been any errors or omissions. Please do contact us if you possess any further information relating to the images published or their rights holder.

Photo credits:

Page 4: © Nicolas Peeters.

Page 5: © European Commission.

Cite this publication: Europol (2023), The Second Quantum Revolution – The impact of quantum computing and quantum technologies on law enforcement, Europol Innovation Lab observatory report, Publications Office of the European Union, Luxembourg.

This publication and more information on Europol are available on the Internet.

www.europol.europa.eu



Contents

04	Foreword
06	Executive Summary
07	Five key recommendations for law enforcement
09	Introduction
11	Before you start: What is quantum computing?
13	The impact of quantum computing on cryptography
14	Store now, decrypt later – a key criminal threat Impact and outlook Deep dive: Cryptology & cryptography
18	Quantum password guessing – an opportunity for law enforcement Impact and outlook Deep dive: Password storage and quantum computing
21	New digital forensic investigation techniques Impact and outlook Deep dive: side-channel attacks and fault injection attacks
23	Protecting sensitive information with post-quantum cryptography Impact and outlook Deep dive: Post-quantum cryptography
26	The impact of quantum technologies
26	Quantum machine learning – the potential use of quantum computers to accelerate AI applications Impact and outlook Deep dive: Quantum machine learning
30	Quantum communications – new, highly secure networks to exchange information Impact and outlook Deep dive: quantum key distribution
31	Quantum metrology and quantum sensors: improving crime scene investigation and forensics analysis Impact and outlook Deep dive: quantum sensors
35	Conclusion
38	Glossary

Foreword

Quantum computing and quantum technologies have the potential to significantly impact law enforcement activities. These key emerging technologies can help us become even more effective in our fight against organised crime and terrorism to come up with innovative ways of doing so. Examples include enhanced analysis of large and complex datasets, improved forensic capabilities, as well as new ways of communicating securely. But these technologies will also lead to significant threats, such as the potential to break the cryptography we use to keep our information safe. We need to anticipate these developments and mitigate the resulting risks. In order to keep up with the rapid pace of technological progress and the resulting changes in the security landscape, law enforcement agencies need to proactively monitor these trends.

As the EU agency at the forefront of law enforcement innovation, Europol recognises this important need. Only by working closely together can we keep abreast of new technological trends and ensure that we are adequately prepared for them. The Innovation Lab's Observatory, hand-in-hand with the operational expertise of the European Cybercrime Centre (EC3), and our colleagues at the European Commission's Joint Research Centre (JRC), have collaborated on this Observatory report to provide an in-depth assessment of the impact of quantum computing and quantum technologies on law enforcement. I am confident that this latest Observatory report will offer invaluable insight into this innovative field for our stakeholders and serve as a first step of the European Law Enforcement community into the 'second quantum revolution'.



Catherine De Bolle
Executive Director of Europol

In April 2021, the European Commission published an ambitious EU Strategy to tackle organised crime, calling for 'law enforcement and judiciary fit for the digital age'. The Joint Research Centre (JRC), a Commission service providing independent, evidence-based science and knowledge, supporting EU policies to positively impact society, was well-placed to support Europol in addressing this endeavour from the start.

We know that quantum technologies have the potential to revolutionise forensics and security practices. Quantum computing, in particular, is undoubtedly going to impact the field of cryptography and consequently cybersecurity. As quantum computers will achieve an impressive speed in solving complex mathematical problems, today's protection of much sensitive information is going to become vulnerable in the future. This enhanced computing capacity will both challenge and benefit law enforcement activities.

Anticipating, building links between the different scientific and policy areas, and measuring the impact of scientific developments in quantum technologies have therefore become essential. They help us to better assess future operational needs for law enforcement, and to foster successful innovation for internal security in compliance with the EU regulatory framework.

The core strengths offered by the JRC are exactly those of anticipation, integration and impact. They are interconnected and enable us to prepare the scientific input needed to address future complex policy challenges. This is why we have been pleased to offer, from the very beginning, our scientific and technical knowledge to support Europol and the Innovation Lab Observatory in their exploration of the possible impact of quantum technologies on law enforcement activities.



Stephen Quest
Director-General of the
Joint Research Centre (JRC)

Executive Summary

Quantum computing and quantum technologies hold significant potential to improve a wide range of applications and tasks. At the same time, recent technological progress in this field, also referred to as the 'Second Quantum Revolution', is threatening to break the encryption we use to keep our most sensitive information safe. The purpose of this report is to provide a forward-looking assessment of the impact of quantum computing and quantum technologies from the law enforcement perspective. In offering an extensive look at the wide range of potential applications in this context, this report is the first of its kind.

The report is the result of a collaborative effort of the European Commission's Joint Research Centre (JRC), Europol's European Cybercrime Centre (EC3), and the Europol Innovation Lab. It aims to inform decision-makers, policy-makers, and practitioners on the benefits and threats stemming from quantum computing and quantum technologies. The report provides an update on the current state-of-play, and offers concrete recommendations to better prepare for the future.

Quantum computing and quantum technologies have the potential to revolutionise the work of law enforcement. One of the most immediately significant areas quantum computers will impact is cryptography. As such, a large part of the cryptographic protocols currently used are threatened by the arrival of quantum computers. This includes both symmetric and asymmetric cryptography. While symmetric cryptography can be relatively easily patched, widely used asymmetric cryptography would collapse entirely if subjected to this process.

The realisation that quantum computers pose a significant threat to currently used cryptography has led to post-quantum cryptography, which aims to keep sensitive information secure from this emerging threat. From the perspective of law enforcement, post-quantum cryptography has two major areas of impact. First, law enforcement agencies need to prepare already to ensure that sensitive information and systems are protected adequately. Second, the transition to post-quantum cryptography might reveal new vulnerabilities that could be exploited in the future.

At the same time, the impact of quantum computing in this field offers numerous potential advantages for law enforcement. As such, quantum computers can support the investigation of cold cases, improve password guessing, and allow for new digital forensics techniques.

In addition to the impact quantum computing will have on cryptography, the overall field of quantum technologies is expected to bring significant advancements across several other areas. This includes improvements in data analysis, machine learning and artificial intelligence, which may benefit from quantum algorithms to process large amounts of data at scale. Quantum communications can enable the establishment of highly secure communications channels through which sensitive law enforcement data can be

transmitted. Finally, quantum sensors can improve the reliability of evidence, decrease the chance of wrongful convictions, and improve the surveillance and detection of objects.

In order for law enforcement to better prepare for the future of quantum computing and quantum technologies, five key recommendations have been identified.

While the development of universal quantum computers is still a future scenario, important steps can and should already be taken today to ensure better preparedness.

Quantum computing and quantum technologies have the potential to revolutionise the work of law enforcement. At the same time, these technologies are likely to pose criminal threats that will need to be mitigated. Only by understanding this impact and taking relevant action, can law enforcement agencies fully leverage these opportunities. This report aims to provide the first step in this endeavour.

Five key recommendations for law enforcement



1. OBSERVE QUANTUM TRENDS

The quantum computing field is highly dynamic, with frequent technical advances being announced and the full scale of potential provided by this type of technology is only starting to emerge. Law enforcement should foster efforts to monitor relevant developments in this area to ensure better preparedness for the potential impact, as well as to be able to respond rapidly to any relevant developments. Law enforcement should also consider advances from quantum technologies beyond the quantum computer, which may be still decades away. Quantum communication and quantum sensing applications are already being developed now, and law enforcement should not miss the opportunities brought by these technologies adjacent to the quantum computer. This analysis regards not only the potential to use quantum computing for the benefit of law enforcement, but also to detect any emerging threats in an early manner.



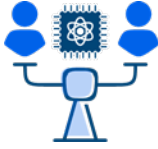
2. BUILD UP KNOWLEDGE AND START EXPERIMENTING

While the full impact of quantum computing and related technologies is still expected to be a number of years away, efforts should be made now to ensure that law enforcement can take full advantage of these developments in the future. This includes learning more about the field, identifying key stakeholders within the respective law enforcement organisations as well as academic institutions, and experimenting on already available quantum computers and quantum sensors.



3. FOSTER RESEARCH AND DEVELOPMENT (R&D) PROJECTS

The law enforcement community should consider setting up its own (or supporting) dedicated research and development projects in the area of quantum technologies. This includes closely engaging with the scientific community and relevant research partners, providing subject matter expertise, and building a network of key stakeholders.



4. ASSESS THE IMPACT OF QUANTUM TECHNOLOGIES ON FUNDAMENTAL RIGHTS

While new technologies offer meaningful opportunities, their use also poses the risk of violating fundamental human rights. New technological solutions may have a profound impact in this area and should be carefully assessed in this regard. A thorough fundamental rights assessment will be needed to ensure that law enforcement can use quantum technologies while respecting and protecting fundamental rights.



5. REVIEW YOUR ORGANISATION'S TRANSITION PLANS

Given the threat quantum computers pose to currently used cryptography, it is critical for law enforcement agencies to review their plans regarding the transition to post-quantum cryptography. This includes: establishing an overview of currently used cryptography and which data it protects, prioritising the most critical systems, and agreeing on plans to ensure that the move to post-quantum cryptography can be executed as quickly and efficiently as possible.

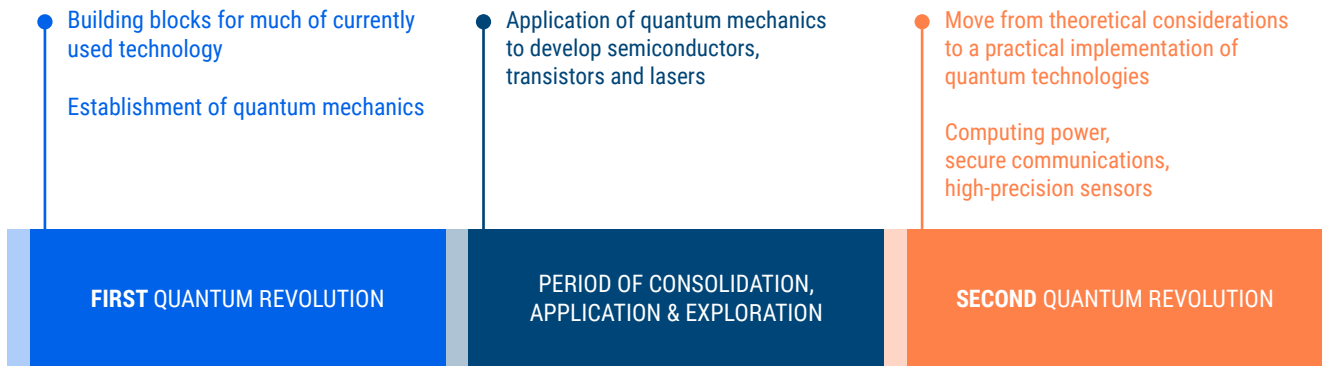
Introduction

A few decades from 2023, news of high-profile data leaks is dominating the headlines, as criminals and hostile actors obtain extremely sensitive information, ranging from law enforcement databases and national security documents to hospital patient records and banking credentials. At the same time, the most innovative law enforcement agencies have managed to supercharge their criminal investigative capabilities through revolutionary improvements in machine learning, the analysis of large and complex datasets, decryption and forensics. These scenarios are not science fiction, but a preview of a probable, not-too-distant future: the advent of quantum computing and related technologies.

The first proposal for the concept of a quantum computer dates back to the 1980s, becoming popular when physicist Richard Feynman famously described ideas of a computer with the ability to exploit the laws of quantum mechanics¹. This idea was further developed in the years to follow and sparked an entirely new field of scientific research: to build a device capable of directly leveraging the laws of quantum mechanical systems for computing. The field reached a new milestone in 1994, when Peter Shor published the first quantum algorithm able to efficiently factorise the product of two very large prime numbers. While it may sound easy, it is a well-known complex problem upon which the security of widely used cryptographic standards relies. In other words, Shor's algorithm would be able to break most asymmetric encryption standards still in use today. Understandably, this discovery generated significant public interest in the development of quantum computers².

The scientific quest to develop a fully functional quantum computer has faced numerous challenges over the past 40 years, with timelines for reaching this goal having been repeatedly amended and postponed. Academia and the private sector have however achieved significant progress in the last decade, especially in the past few years. We have now reached the point where quantum supremacy, that is to say the demonstration that a quantum computer is able to solve a mathematical problem much faster than a classical computer, may actually be close to being reached beyond scientific doubt³. Several researchers have already published peer-reviewed work claiming to have achieved quantum supremacy, although these results have not been met with unanimous agreement among the scientific community⁴.

-
- 1 Nature, '40 years of quantum computing', 2022, [accessed 22/06/2023], <https://www.nature.com/articles/s42254-021-00410-6>.
 - 2 Shor, P.W., 'Algorithms for quantum computation: discrete logarithms and factoring', Proceedings 35th Annual Symposium on Foundations of Computer Science, 1994, p. 124–134.
 - 3 Quantamagazine, 'New Algorithm Closes Quantum Supremacy Window', 2023, [accessed 22/06/2023], <https://www.quantamagazine.org/new-algorithm-closes-quantum-supremacy-window-20230109/>.
 - 4 The Guardian, 'Google claims it has achieved quantum supremacy – but IBM disagrees', 2019, [accessed 22/06/2023], <https://www.theguardian.com/technology/2019/oct/23/google-claims-it-has-achieved-quantum-supremacy-but-ibm-disagrees>.



In a broader view, quantum computers are but one element of the renewed interest into general quantum technologies, for example also including quantum information and communication systems or quantum sensors. The subsequent technological progress that has been achieved has also been referred to as the second quantum revolution⁵. The first quantum revolution gave the world the building blocks for much of the currently used technology, by developing technologies which could only be understood in the framework of applied quantum physics, such as with the development of transistors or lasers. The new wave of research and development in the area of quantum technologies marks a move from theoretical considerations to a practical implementation of technology not only relying on the understanding of materials through quantum physics, but by directly leveraging laws of quantum mechanics to implement new technologies.

A large part of this pursuit is motivated by the vast promises quantum computing offers for several applications. Simulating quantum systems with quantum computers could enable significant progress in the research of new materials and medicine. The modelling of molecular processes, for instance, could help enable the development of life-saving drugs. At the same time, an improved ability to analyse vast amounts of data and solve optimisation tasks may offer new opportunities to develop advanced financial risk models and solve complex logistical challenges⁶. This capability of quantum computing may ultimately also lead to meaningful progress in the areas of machine learning and artificial intelligence, as well as all of its potential applications.

All these applications are also relevant in the context of law enforcement. Enhanced data analysis could allow for faster identification of patterns and trends in crime analysis and password guessing, while advancements in machine learning and AI might improve critical AI systems. For instance, quantum machine learning may enable law enforcement agencies to more efficiently process large amounts of unstructured evidence. Other foreseen use cases of new quantum technologies, beyond full

5 NIST, 'The Second Quantum Revolution', 2023, [accessed 22/06/2023], <https://www.nist.gov/physics/introduction-new-quantum-revolution/second-quantum-revolution>.

6 Forbes, 'The Promise of Quantum Computing', 2022, [accessed 22/06/2023], <https://www.forbes.com/sites/forbestechcouncil/2022/06/13/the-promise-of-quantum-computing/?sh=2e95b5a7429e>.

scale computers, are already much more mature: they range from improved reliability of evidence and the forensic detection of currently invisible traces to more secure ways of communication. These fields are already being developed now, and law enforcement should not miss the opportunities. Overall, the rise of quantum technology promises to significantly improve the effectiveness of law enforcement in addressing numerous complex challenges.


As history shows, technology should be understood as a double-edged sword, with technological advancements often posing threats, in addition to its opportunities. This also applies to quantum computing. The expected capability of quantum computers to achieve a significant speed-up⁷ in solving certain mathematical problems means that the state-of-the-art encryption that is universally used today to protect sensitive information will effectively be broken. In what is known as 'store now, decrypt later', encrypted data collected today may become available to malicious actors in the not-too-distant future. The availability of sensitive information to criminals may facilitate a variety of criminal activities, including social engineering and phishing, ransom demands, and more. Additionally, quantum computing-facilitated advancements in AI may lead to an exacerbation of criminal threats already seen today.

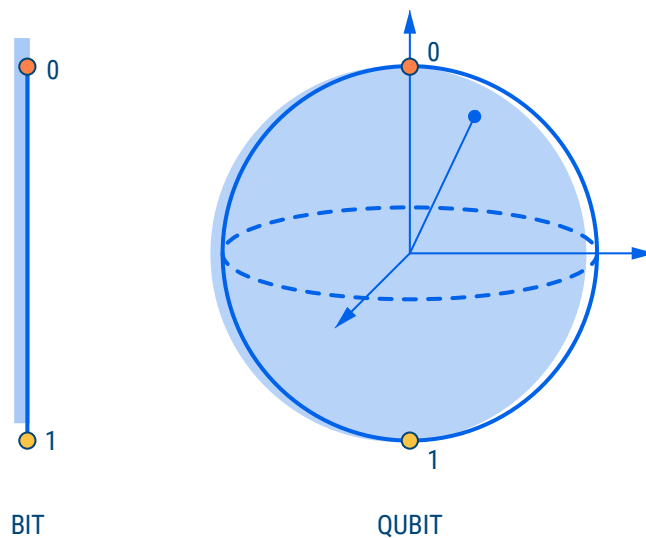
Law enforcement is at the early stages of examining the impact that quantum computing will have on its work. While the technology is not yet ready, some actions can and should be taken already today in order to ensure better preparedness for an emerging quantum future.

This report provides a first assessment of quantum computing from the law enforcement perspective. Each sub-chapter briefly introduces its topic, highlights the concrete impact for law enforcement, as well as provides a concise outlook and more detailed background explanation of the technology in question. Finally, the report makes recommendations with a view to improving the overall preparedness of the law enforcement community. Attached at the end of this report is a 'technology deep dive' analysis on quantum computing in general.

Before you start: What is quantum computing?

Quantum computers are not universally faster than classical computers, but are vastly more suitable for solving a range of specific mathematical problems. This is mainly due to the fact that, while classical computers use binary bits to perform calculations, quantum computers use quantum bits (qubits). In essence, whereas bits can only have two values (0 or 1), qubits can exist in a combination of both states simultaneously.

 ⁷ Speed-ups refer to improvements in how quickly or efficiently an algorithm can be executed. Speed-ups are typically compared to another algorithm and measure differences in performance in relation to a certain task.



Qubits offer different possibilities by exploiting quantum effects, such as superposition and entanglement (see technology deep dive). By making use of qubits to execute certain algorithms, quantum computers significantly reduce the number of calculations needed compared to classical computers for specific problems. This unlocks a number of new possibilities in the development of algorithms.

Specifically designed quantum algorithms leverage these new possibilities to give quantum computers advantages over classical computers in certain tasks. Famous examples include Shor's and Grover's quantum algorithms, which exploit the capability of quantum computers to process multiple inputs simultaneously to solve problems upon which current cryptography is based. Run on a quantum computer, this would effectively mean that the encryption used to keep our most sensitive information safe nowadays would effectively be broken. At the same time, quantum computers can offer a number of important benefits for law enforcement, ranging from enhanced password guessing and digital forensics to improved big data analysis and machine learning applications.

Quantum computing is an active field of research. Given the cutting-edge nature of this technology, several challenges will need to be overcome before the arrival of the universal quantum computer. These include scaling up the hardware, increasing the speed of executing quantum algorithms, and achieving practical quantum error correction. The latter is of particular importance, as qubits are highly sensitive to their environment. Noise, such as through internal or external interferences, can introduce errors and make the quantum computer unreliable as a result. The first experimental quantum devices (so called 'NISQs' or simulations on classical computers) are already available for research purposes, but are still limited by their low number of qubits and noise levels. Universal quantum computers represent the ultimate goal in the quantum computing field. These are quantum computers that are fault-tolerant, universally programmable, and that provide a real, proven advantage over classical computers.

The impact of quantum computing on cryptography

Quantum computing promises improvements in a vast array of different applications. While some of these are more speculative, one of the more immediate areas universal quantum computers are going to impact is the field of cryptography and therefore, more broadly, security. This mainly refers to Shor's and Grover's algorithms, which will achieve a speed up in solving mathematical problems upon which modern cryptography relies. This means that the way sensitive information is protected today is going to be vulnerable to this type of technology.

A malicious actor having access to a quantum computer could hence break currently used cryptography protocols. This includes not only encryption but also signatures, key exchange or authentication. Passwords are also at risk, as Grover's algorithm considerably speeds up brute-force attacks⁸.

At the same time, the impact of quantum computing on cryptography offers numerous potential advantages for law enforcement. As such, quantum computers can support the investigation of cold cases, improve password guessing and allow for new digital forensics techniques.

The potential impact of quantum technologies on law enforcement and criminals are twofold. Law enforcement should act now to reduce the risk of criminals taking advantage in the future. The table below outlines these risks and what law enforcement should do to mitigate them.

Area	Law enforcement	Criminals
General	Raise awareness on the threat of quantum computers and stay abreast of technological developments to combat risks at the earliest stage possible. Ensure law enforcement is leveraging the latest technology.	Reconsider their current <i>modi operandi</i> and identify potential to abuse availability of quantum computers.
Store now, decrypt later	Hold on to currently inaccessible encrypted data resulting from criminal investigations with a view to later decryption.	Accumulate and store encrypted information (for instance obtained from data breaches) with a view to later decryption.
Quantum password guessing	Significantly improve their technical ability to access password-protected data and devices from criminal investigations.	Be pushed to find alternative solutions for secure communications or increase operational security by using stronger passwords and multi-factor authentication. More easily hack into password-protected data and devices.
Digital forensics	Use new side-channel attacks and fault injection vulnerabilities to improve ability to gain access to criminal devices.	Employ counter measures or identify alternative technological solutions to increase operational security.
Post-quantum cryptography	Put into place transition plans to post-quantum cryptography for own data storage.	Switch to quantum-safe solutions.

⁸ Durmuth M., Golla M., Markert P., May A., Schlieper L., 'Towards Quantum Large-Scale Password Guessing on Real-World Distributions', International Conference on Cryptology and Network Security, 2021.

This section discusses in more detail the impact of quantum computing on current cryptography, the potential opportunities and threats resulting from it for law enforcement, and briefly touches upon post-quantum cryptography as a means of preparing for this future.

Store now, decrypt later – a key criminal threat

While quantum computers are not yet available, their potential capability already has a profound impact on current data protection. Data encrypted today could be stored for an unlimited amount of time until a quantum computer powerful enough to decrypt it is available. This is known as the ‘store now, decrypt later’ approach (also known as ‘harvest now, decrypt later’ or ‘retrospective decryption’), triggering the need to consider how long encrypted data needs to stay confidential. This includes both symmetric and asymmetric cryptography. While symmetric cryptography can be relatively easily patched, widely used asymmetric cryptography would collapse entirely.

Examples of symmetric cryptography that will be vulnerable to quantum computers include, among others:

- Data encryption (at rest and in transit)
- Secure file transfers
- Secure network communications
- Virtual Private Networks (VPNs)
- Wireless network security

Symmetric cryptography is mostly affected by Grover’s algorithm, which speeds up the brute force attack on its key. These attacks can be relatively easily patched by doubling the size of the secret key for most of the symmetric schemes, including AES or SHA-3. This also includes hash functions, used among others in cryptocurrencies, for which the size of the output would need to be doubled to reach the same security level.

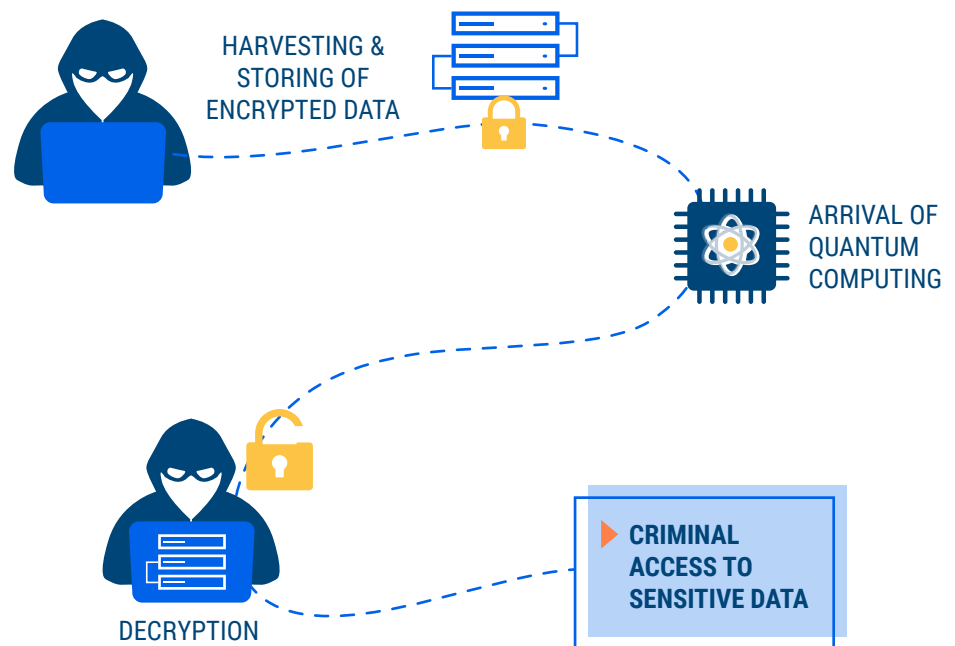
Asymmetric encryption is typically used to securely exchange symmetric encryption keys. Examples include:

- Secure email (i.e. PGP and S/MIME)
- Secure websites (HTTPS)
- Digital signatures
- Cryptocurrencies
- Public Key Infrastructure (PKI)
- SSH (authentication between server and client)

Asymmetric cryptography is threatened more radically by quantum attacks, as its security is based on complex problems (namely factorisation or discrete logarithm problems), which quantum computers can solve efficiently with Shor's algorithm. This means that classical asymmetric schemes completely collapse, triggering the need for replacements⁹.

IMPACT AND OUTLOOK

The concept of 'store now decrypt later' may offer an opportunity for law enforcement to gain later access to encrypted evidence that is obtained now. Similarly, criminal actors may already today accumulate encrypted information, such as databases, protected files, or communications data, and hold onto it with a view to later decryption. While it is expected to take a while for quantum computers to be universally accessible even once the technology is mature enough, malicious actors may benefit from using cloud-based solutions, such as quantum-as-a-service, for decryption purposes.



In practice, this means that any information not sufficiently protected against quantum computers today (see *post-quantum cryptography p23*) may be accessible to criminals later, if it is obtained now. This could lead to new types of ransom demands or a flood of sensitive information (such as account credentials and personal information) being available to criminals for crimes such as social engineering and phishing. The availability of quantum computers may further threaten any system that has not successfully transitioned to post-quantum cryptography.

⁹ Bernstein D., 'Introduction to post-quantum cryptography', 2009, [accessed 22/06/2023], https://www.pqcrypto.org/www.springer.com/cda/content/document/cda_downloaddocument/9783540887010-c1.pdf.

Any information not sufficiently protected against quantum computers today may be accessible to criminals later, if it is obtained today. This could lead to new types of ransom demands or a flood of sensitive information (such as account credentials and personal information) becoming available to criminals. This could lead to the facilitation of criminal activities such as social engineering and phishing.

This warning is expressed in *Mosca's Inequality Theorem*¹⁰. It states that if the sum of the time an organisation wishes its data to be secure, in addition to the time it will take to transition to post-quantum cryptography, exceeds the time left until quantum computers become widely available, that data is at risk. It expresses the urgent need to act in order to keep sensitive data secure.

The technological landscape is changing fast. As a result, theoretical concepts, such as 'store now, decrypt later', can rapidly become operational reality and have a real impact on law enforcement and criminals. With the world moving closer to the arrival of a universal quantum computer, the realisation that currently secure data may be exposed in the future is going to set in over time. If action is not already taken now, however, for many it may be too late.

DEEP DIVE: CRYPTOLOGY & CRYPTOGRAPHY

Cryptology refers to the science of secrecy. It aims at ensuring the confidentiality, authenticity and integrity of the information exchanged between the sender and the receiver. Cryptography usually refers to the elaboration of secure protocols, while cryptanalysis refers to the attacks performed on the schemes.

Cryptographic protocols are divided into two broad families, namely the symmetric and asymmetric schemes. In the symmetric settings, both the sender and the receiver of a message share the same secret key. Symmetric cryptography offers fast encryption protocols like AES (Advanced Encryption Standard), or previously DES (Data Encryption Standard, now deprecated for most applications). The security of symmetric protocols relies on the use of seemingly random transformations that depend on the shared secret key¹¹.

In asymmetric settings, on the other hand, the sender and the receiver have a pair of keys each: a public key that can be shared, and a private key that remains secret. Asymmetric cryptography protocols are usually slower for encryption, but they offer other crucial capabilities that are unavailable in the symmetric settings

¹⁰ Mosca, M., Mulholland, J., 'A Methodology for Quantum Risk Assessment', 2017, [accessed 05/10/2023], <https://globalriskinstitute.org/publication/a-methodology-for-quantum-risk-assessment/>.

¹¹ The more random the transformations, the harder it is for an attacker to decrypt the information, given the number of possibilities.

such as signatures or zero-knowledge protocols. Famous asymmetric cryptographic primitives¹² include RSA¹³ or elliptic curve cryptography. The security of asymmetric cryptography relies on complex algebraic problems such as the factorisation problem or the discrete logarithm problem.

Cryptanalysis refers to the analysis of cryptosystems with the goal of finding weaknesses that can be used to compromise desired security aspects. The objective of cryptanalysis is, therefore, not necessarily to retrieve the secrets that have been used by one or many of the participants within a protocol. It can, for example, be limited to a controlled modification of a message conveyed in an encrypted manner impacting the integrity of the system. The techniques used in cryptanalysis are varied and include statistical analysis, the algebraic approach and side-channel attacks, among others. It should be noted that while the concept of cryptanalysis is about weakening or even breaking cryptosystems, it contributes to the effort of reinforcing security in general by helping to identify potential risks at an early stage.

Both Shor's and Grover's algorithms fall into the category of cryptanalysis techniques as they have been proven to break or weaken certain cryptosystems. The practicality of those algorithms is still uncertain as it is not yet known if or when a quantum system will be capable of running those algorithms on pertinent data. Nevertheless, those algorithms are theoretically valid given their expected capability to significantly diminish or break, in the case of those vulnerable to Shor's algorithm, the security of cryptosystems. It should be noted that further improvements in quantum computing, should they occur, could make the implementation of those algorithms easier in practice.

From another perspective, other quantum approaches might and will be considered to perform cryptanalysis with a different attack vector. SAT (satisfiability) solvers are one amongst many tools that can be used in cryptanalysis. This is for example well suited to find solutions to complex logical formulas, also known as Boolean expressions, derived from specific cryptosystems¹⁴. Quantum SAT solvers is an active field of research, with some solutions having already been proposed with a theoretical advantage over classical approaches¹⁵.

12 Cryptographic primitives refer to building blocks of cryptographic systems.

13 Rivest, R., Shamir, A., Adleman, L., 'A Method for Obtaining Digital Signatures and Public-Key Cryptosystems', 1978.

14 Such as the S-boxes used in AES.

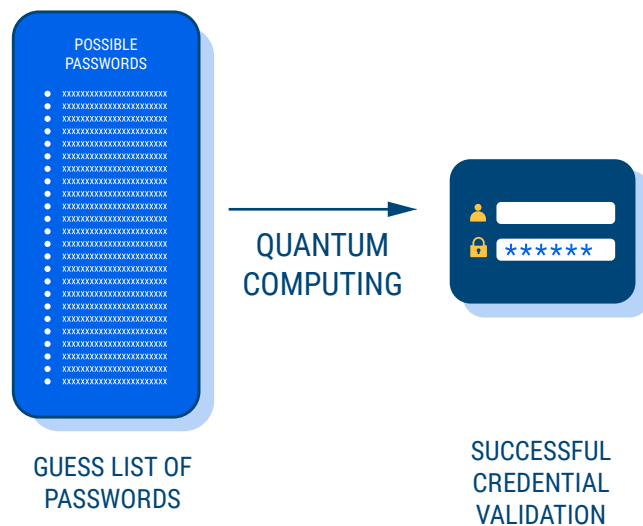
15 Castryck, W., Decru, T., 'An efficient key recovery attack on SIDH', 2022, [accessed 22/06/2023], <https://eprint.iacr.org/2022/975.pdf>.

Quantum password guessing – an opportunity for law enforcement

Passwords play a critical role in restricting access to sensitive information. As they are customisable, they are easier to remember for humans than complex cryptographic keys, and as such have been the preferred way of digital authentication during the last decades. Password guessing relies on the human tendency to prefer certain passwords, which narrows down the list of possibilities. Still, even with a narrow scope, testing all possible combinations (of letters, numbers, symbols and entire words) constitutes a monumental task. This is where quantum computers could provide an advantage.

IMPACT AND OUTLOOK

Given the ability of quantum computers to process multiple possibilities at the same time, quantum computing is going to have a significant impact on password cracking, namely the action of retrieving a password from its stored secure form. Grover’s algorithm, for instance, seems particularly fit for such task, as it is optimised to look for an input that matches a particular function. In this case, the algorithm would look for a password that matches the output of the secure hash function applied to this password. This means in practice that law enforcement may be able to use quantum computers to significantly improve its ability to gain access to password-protected information in high-profile criminal cases. Applications include investigations of child sexual abuse and exploitation, which has an important digital component, or terrorism, which is often extremely time sensitive and, as such, requires efficient investigation measures.



Quantum computing is going to have a significant impact on password cracking.

As the capability of law enforcement to guess passwords may significantly increase with the advent of quantum computers, criminals may move to adjust their use of passwords or to choose new hash functions. Quantum computing changes the notion of what is today considered a strong password, which may lead to longer and more complex passwords becoming widely used in the future in order to counteract quantum-based password guessing, or the wider adoption of biometric identification methods.

Quantum computers could offer new possibilities for law enforcement to gain access to password-protected information in high-profile criminal investigations. At the same time, the actual application of this approach will still need to be proven and translated into practice. As research progresses, this impact will become increasingly within reach. To leverage these new opportunities, active research and experimentation can help law enforcement agencies be better prepared to make the most of quantum password guessing in the future.

DEEP DIVE: PASSWORD STORAGE AND QUANTUM COMPUTING

Password usage can be categorised in two large categories¹⁶. When used for the sole purpose of authentication, a service will compare the password entered by the user with a stored piece of information. To preserve a certain level of security in case of a data leak, the password should not be stored in clear text. The common practice is to store the output of a one-way function, typically a hash function, taking as input the password. In case of a breach, the password cannot be retrieved directly from its hash.

In other cases, the password is used as a seed from which a cryptographic key will be derived and used for cryptographic purposes, such as encryption or signatures. Such derivation protocols are known as key derivation functions (KDF). A KDF often takes the user's password, includes unique and random strings ('salt') and applies the algorithm several times. By mixing the user's password with the salt and running several iterations of the algorithm, a derived key that is highly resistant to brute-forcing or dictionary attacks is created. A widespread construction from the PKCS#5 standard is the PBKDF2 (Password-Based Key Derivation Function version 2) family of functions. The derived key can be used to encrypt a pre-determined magic cookie¹⁷ which could then be stored and used similarly to a hash. The key can also be used to encrypt a data container or to realise full-disk encryption of a system.

In both cases, the only way to retrieve a password is to evaluate password candidates by applying the same process until a match is found, under the assumption that the underlying functions are

16 While there are some edge cases that do not fall in these categories, they have been left out of these explanations for the sake of simplicity.

17 A piece of data exchanged by systems for the purposes of authentication and session handling.

flawless. Typically, however there is a real loss of information during the hashing process, which cannot be retrieved in any manner.

At this stage, such an approach is still speculative as the ‘oracle’ function¹⁸, most of the time a hash function in this scenario, must be transposed into an efficient quantum circuit to be evaluated by Grover’s algorithm. Examples of quantum circuits for specific hash functions have already been proposed¹⁹, leaving few doubts about the feasibility of this aspect. The set of passwords to be evaluated (e.g. all combinations of 10 lowercase characters) must be converted into a quantum state, so that it can be processed by a quantum computer. This involves transposing the information from bits to qubits. First, this would require a very large number of qubits, which is not currently available. Second, while an exhaustive search of possible password combinations at a binary (0 or 1) level would be easily feasible, the resulting search space would still be incredibly large. The speed-up brought by the quantum algorithm would not be sufficient to explore such candidate space in a short amount of time²⁰.

Brute-force password cracking, however, has its limitations and is typically used as a last resort due to its complexity. If people selected their passwords as purely random sequences of characters and never reused them, this approach would be the most efficient. However, people are predictable and modern password cracking approaches exploit this human bias to increase their success rate. Those techniques range from the ‘dictionary attack’, simply trying the most widely used passwords, to more sophisticated attacks relying on natural language processing (NLP) or neural networks. NLP heavily relies on the analysis of large data sets to identify common words and phrases, contextual variations, as well as predictions of likely sequences of characters. As is shown in chapter 3, quantum machine learning could offer significant advantages for these types of applications. Such non-uniform distribution needs to be transposed in a quantum state to benefit from Grover’s algorithm which is the challenge to tackle for quantum password guessing.

However, this does not appear to be a dead-end, as has been highlighted in the research article of Durmuth et al.²¹. If this is the case, and assuming again that the underlying function can be transposed as a quantum circuit, it would have a real impact in the field of password guessing. This could benefit law enforcement

18 An ‘oracle function’ in the context of cryptography is a theoretical tool used to evaluate the strength of a cryptographic system.

19 Song, G., Jang., K., Kim., H., Seo, H., ‘A Parallel Quantum Circuit Implementations of LSH Hash Function for Use with Grover’s Algorithm’, *Appl. Sci.* 2022, 12(21), 2022, [accessed 22/06/2023], <https://www.mdpi.com/2076-3417/12/21/10891>
<https://eprint.iacr.org/2020/1418.pdf>.

20 For instance, considering a single-byte encoding such as UTF-8, where 8 bits are used to encode a character, only up to three characters could be brute-forced with the same number of operations as in the previous example.

21 Durmuth M., Golla M., Markert P., May A., Schlieper L., ‘Towards Quantum Large-Scale Password Guessing on Real-World Distributions’, *International Conference on Cryptology and Network Security*, 2021, pp 412–431.

agencies in their investigations when facing password-protected encrypted material.

Post-quantum cryptography security will still rely on the usage of cryptographic keys which will even become longer in practice. As these can still be protected by passwords, the transition to those algorithms will consequently have a limited impact on the usage of passwords. While the overall security of authentication mechanisms is drastically improved when multi-factor authentication is implemented and enforced, and any quantum-based authentication factors will likely complement existing authentication mechanisms²², there is no significant impact expected on the password-based factor itself.

Quantum computing could have a real impact in the field of password guessing. This could benefit law enforcement agencies in their investigations when facing password-protected encrypted material.

New digital forensic investigation techniques

In times of rapid global digitisation, more and more relevant data is stored on encrypted electronic devices. As these sources of electronic evidence are critical for a vast amount of criminal investigations, access to this type of information is a core aim of digital forensics. One way to enable access is through so-called physical attacks aimed at circumventing specific software and hardware security measures. Examples of these types of physical attacks include side-channel attacks and fault injection attacks.

IMPACT AND OUTLOOK

Quantum devices may offer new opportunities for these types of forensic attacks. For instance, law enforcement could exploit new quantum side-channels by leveraging the decoherence of a quantum system, such as by intentionally increasing it. This is especially critical as the implementation of relevant security and safety measures is not the priority at this stage of the development of quantum computers. It is, nevertheless, solely speculative at this stage.

At the same time, analysis of data extracted from an attack could benefit from quantum computation. For example, Grover's algorithm could be used to retrieve a correct 'trace', that is a piece of data extracted during the attack, among a set of samples leading to the deduction of the key. Quantum SAT solvers could also be beneficial here to solve complex Boolean equations deduced from the side-channel analysis. As a result, quantum computers could increase the success ratio of existing techniques, moving them from the field of potential attacks to practical attacks.

²² Murray, H., Malone, D., 'Quantum multi-factor authentication', 2021, [accessed 22/06/2023], <https://arxiv.org/abs/2110.05344>.

Countermeasures to side-channel techniques and fault injection exist. They can rely on algorithmic solutions to ensure that the computation steps do not leak any relevant piece of information. They can also be hardware-based, enforcing technical impossibility to collect the data without interfering in a way or another with the data itself. Quantum mechanisms could be envisaged to reinforce those counter measures relying on photon exchange such as in the Quantum Key Exchange. On the other hand, the introduction of quantum-safe algorithms and also quantum devices can open the door to new opportunities. The implementation of quantum safe algorithms can be vulnerable to classical or new side-channel attacks. Quantum based devices, such as those used in the quantum key distribution relying on photons, could also leak information, such as data about the exchanged key. The channel itself is considered secure but the starting point, the end point or the potential relay used in between could be vulnerable.

Quantum computers could increase the success ratio of existing techniques, moving them from the field of potential attacks to practical attacks.

In the context of criminal investigations, new forensic approaches are critical to ensure law enforcement remains able to access relevant electronic evidence. As most crime areas involve at least some digital component, digital forensics can provide the key to effectively investigate cases of serious organised crime and terrorism.

New digital investigation techniques are a vital component of effective law enforcement operations. Technological progress in the field of quantum computing is of significant interest in this regard, as new methods are likely to emerge. Law enforcement will need to observe these developments closely to ensure that any relevant new opportunities can be leveraged.

DEEP DIVE: SIDE-CHANNEL ATTACKS AND FAULT INJECTION ATTACKS

Side-channel attacks and fault injection attacks are types of cryptanalysis techniques aiming to weaken or break the security of a cryptosystem. However, they target specific implementations exploiting hardware vulnerabilities, which differ from other – more theoretical – approaches, focusing solely on algorithmic or mathematical vulnerabilities.

- ▶ Side-channel attacks allow forensic investigators to extract sensitive information from a system by examining a system's inputs and outputs. This 'side' data can compromise the security infrastructure of the system and reveal information relating to encryption keys or other sensitive data. Examples include

analysing the system's power consumption²³, time needed to perform certain operations, or electromagnetic emanations.

- ▶ Fault injection refers to the purposeful injection of faults into a system to get the system to malfunction. This malfunction can reveal sensitive information or weaken in-built security measures. Examples include introduction software glitches or physically tampering with the hardware.

Protecting sensitive information with post-quantum cryptography

The realisation that quantum computers pose a significant threat to currently used cryptography has led to efforts aimed at keeping sensitive information secure from this emerging threat. These efforts have given rise to the field of post-quantum cryptography, which aims to ensure the safety of data in the post-quantum world by developing and implementing cryptographic schemes that can run on classical computers without being vulnerable to quantum computers.

For a malicious actor not having access to a quantum computer, most classical attacks on encryption would be rendered more difficult theoretically, as post-quantum cryptography encryption and signature schemes tend to have a stronger classical security, particularly in the hybrid approach²⁴. When considering passwords, new hash functions with longer outputs are likely to be used, making brute-force attacks less efficient. However, social engineering attacks (weak or reused passwords, targeted search) still apply.

IMPACT AND OUTLOOK

From the perspective of law enforcement, post-quantum cryptography has two major areas of impact. First, there is a need to prepare immediately to ensure that sensitive information and systems are protected adequately. This includes identifying relevant systems that might be affected, prioritising the most critical systems, and agreeing on plans to ensure that the move to post-quantum cryptography can be executed as quickly and as efficiently as possible. A key area of concern in this regard relates to the fact that the transition might be slow, meaning that some weak schemes could still be used despite being deprecated.

Second, the transition to post-quantum cryptography might reveal new vulnerabilities that could be exploited in the future, including potential attacks leveraged by quantum computers. Moreover, the

²³ To illustrate what a side-channel attack could be, a suitable example relates to the RSA algorithm able to extract the RSA key from a hardware device in linear time. The bits of the key can be processed sequentially and, depending on if it is a 0 or a 1, a different operation is handled. The power consumption of the device can highlight this difference, giving the possibility to reconstruct the key from the power consumption analysis.

²⁴ A hybrid approach, in this context, refers to a combination of classical and post-quantum cryptographic methods.

possibility of a weak post-quantum candidate being standardised exists due to their relative novelty.

It remains difficult, or even impossible, to predict what the next type of attacks could be. Nevertheless, it is almost certain that quantum computers will provide new opportunities. Law enforcement should maintain a good technological watch to detect and benefit from such new opportunities.

Most of the cryptography currently used is threatened by the arrival of quantum computers. In a concept known as 'store now, decrypt later', criminal actors may already today harvest encrypted data with a view to decrypting it once quantum computers are universally available, triggering the need to review for how long data should be kept secure. Quantum computing is going to have a significant impact on password cracking. Post-quantum cryptography offers a promising solution to the threat posed by quantum computers on cryptography, but needs to be carefully assessed regarding potential security-related weaknesses. It should not be forgotten that quantum attacks are not more powerful than classical attacks, but they work differently. Therefore, being secure against quantum computers does not ensure overall security.

DEEP DIVE: POST-QUANTUM CRYPTOGRAPHY

The efforts of the cryptographic community have been gathered by NIST, which launched a contest in 2017 to standardise key encapsulation (for two parties to agree on a shared private key to be used in symmetric settings) and signature protocols resistant against attacks by quantum computers²⁵. Similar competitions have already been organised by NIST, for example to define a symmetric block cipher standard. The selection process took place between 1997 and 2000. The sole aim was to identify an efficient and secure replacement for the DES cipher, namely AES, without any consideration about quantum resistance at that time. Another process was conducted between 2007 and 2012 to standardise a new secure hash function, leading to the selection of the SHA-3 function.

For post-quantum cryptography, NIST received 69 valid submissions in December 2017. After several rounds of selection and elimination, the finalists were announced in 2022. The chosen submissions are based on lattice²⁶ and error-correcting code²⁷ problems for which quantum computers do not seem to provide an advantage over classical ones. NIST also announced a new call

25 NIST, 'Post-quantum cryptography standardization', 2023, [accessed 22/06/2023], <https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization>.

26 Lattice-based cryptography refers to cryptographic systems based on lattices (geometric structures in which lines are connected by points). Because some of these patterns can theoretically extend infinitely, lattice-based cryptography has become a popular proposed solution to the threat of quantum computers.

27 Error-correcting codes have been proposed to offer protection from the threat of quantum computers as they allow for the construction of new mathematical problems that are exceedingly difficult to solve – even for quantum computers.

for signatures based on different hard problems, and an additional round for some key encapsulation protocols, meaning that other standards might be selected in the near future. The aim is to have post-quantum protocols based on different security hypotheses, so that if one is discovered to be weak in the years to come, another selected one can be used instead.

Compared with classical protocols, post-quantum schemes involve (much) larger key-size and slower computation. The transition between classical and post-quantum cryptography should take place with the use of hybrid protocols that use two layers: one post-quantum layer to protect against attacks by quantum computers, but also a classical layer in case of failure in the former layer. In particular, content for which long-term secrecy is needed should already be encrypted in this hybrid form to avoid 'store now, decrypt later' strategies. Therefore, the transition should be planned and prepared now.

It should not be forgotten that quantum computers are not more powerful than classical ones, but they work differently. Therefore, being resistant to quantum computer attacks does not ensure overall security.

Nevertheless, quantum computers are not more powerful than classical ones, but they work differently. Therefore, being resistant to quantum computer attacks does not ensure overall security. This has been perfectly illustrated by the research of W. Castryck and T. Decru from KU Leuven²⁸, who presented a classical attack (meaning an attack not using a quantum computer) to perform cryptographic key recovery against a presumably quantum safe key exchange protocol known as SIKE. It is, thus, worth bearing in mind that the introduction of new algorithms to increase security against quantum computers could also open new opportunities using classical means. Furthermore, in the future, there could be new types of quantum attacks that could solve the building block(s) of the new system. This is one of the reasons why NIST organised a new standard request competition specifying that the solution should not rely on the security of lattice-based cryptography. Lattice-based cryptography is one of the leading contenders in the field of post-quantum cryptography due to its supposed strength. However, if the solution to the security assumption behind lattice-based cryptography is eventually found, there is already an alternative that has been analysed and that is ready to be deployed as a replacement.

28 Castryck, W., Decru, T., 'An efficient key recovery attack on SIDH', 2022, [accessed 22/06/2023], <https://eprint.iacr.org/2022/975.pdf>.

The impact of quantum technologies

In addition to the impact quantum computing will have on cryptography, the overall field of quantum technologies is expected to bring significant advancements in several other areas. Firstly, there are data analysis, machine learning and artificial intelligence, which may benefit from quantum algorithms for more efficient processing, e.g. to process large amounts of data at scale. Secondly, there is potential for law enforcement in secure quantum communications and quantum sensors, e.g. for crime scene forensics.

The potential impact of quantum technologies on law enforcement and criminals are twofold. Law enforcement should act now to reduce the risk of criminals taking advantage in the future. The table below outlines these risks and what law enforcement should do to mitigate them.

Area	Law enforcement	Criminals
Quantum machine learning	Enhance AI systems, i.e. for data analysis, computer vision, biometrics, etc., but also improve search and password guessing capabilities.	Advancements in AI could be abused by criminals through exploiting commonly available AI tools
Quantum communications	Establish highly secure communication channels for information exchange, which may in particular facilitate the sharing of relevant information in the context of criminal investigations.	Criminal, terrorist or state actors could make use of quantum channels to evade law enforcement detection and prevent criminal prosecution.
Quantum metrology & sensors	<p>Improve the reliability of evidence and decrease the chance of wrongful convictions by significantly enhancing detection and analysis of clues, as well as by speeding up post-data processing times.</p> <p>Improve surveillance and detection of relevant objects at greater distances and through objects.</p> <p>Provide law enforcement officers with faster and more accurate decision-making in critical situations through real-time data processing with quantum sensors.</p>	Be pushed to find alternative solutions for secure communications or increase operational security by using stronger passwords and multi-factor authentication. More easily hack into password-protected data and devices.

Quantum machine learning – the potential use of quantum computers to accelerate AI applications

Artificial intelligence, machine learning and data analysis techniques are rapidly changing technologies. With an ever-growing access to large amounts of data, such as from text, images, audio, or video content, they also have an increasing impact on law enforcement, as more and more criminal investigations involve the processing and analysis of significant amounts of data. In recent years, it has become evident that machine learning and techniques for processing large and complex datasets are poised to eventually

benefit from the potential offered by quantum computers. This has created the young interdisciplinary research subject of *quantum machine learning*²⁹. In due course, with the availability of more mature quantum devices, techniques from quantum machine learning could have a significant impact on internal security and law enforcement.

Relevant applications range from predictive tools and the analysis of large and complex datasets, digital forensic and pattern recognition techniques for the identification of perpetrators or the localisation of crimes, biometrics and computer vision for sensors or image analytics, to the more recent promises of large language models and generative AI.

At the same time, AI can be considered a classical dual-use technology. Cybercriminals are equally making use of those techniques to their own advantage via: AI-based malware, the exploitation of AI-specific vulnerabilities in software systems, using machine learning to enhance hacking and password guessing capabilities. Other techniques include AI-based content generation with large language models or diffusion models to create deep fakes in criminal activities.

IMPACT AND OUTLOOK

- ▶ **Increased impact of typical AI fields** (more efficient algorithms, quantum acceleration): pattern recognition (e.g. unstructured evidence, clustering, classification, identification, etc.), computer vision, biometrics, predictive tools, safety and security (cybersecurity tools, sensing algorithms for sensors).
- ▶ **Potential impact on big data algorithms, database search and large-scale data mining** (proven computational advantages with algorithms such as Grover and HHL).
- ▶ **Algorithmic advances:** currently unclear, but examples could include quantum representations and Quantum Neural Network (QNN) features. Explicit examples from generative models include password guessing, data augmentation/synthetic training data.

A fundamental task in the analysis of large and complex datasets is binary classification of substantial amounts of high-dimensional data. In a forensic setting, this may include the classification of media files such as video or image content into different classes of source cameras using techniques³⁰ to digitally identify the source of incriminating evidence. It has been shown that using a quantum algorithm for a wide-spread classical approach in big data classification – a quantum support vector machine – would yield an exponential quantum advantage³¹, which would result in a

29 Wittek, P., 'Quantum Machine Learning. What Quantum Computing Means to Data Mining', 2014.

30 Signal processing routines.

31 Reberntrost, P., Mohseni, M., Lloyd, S., 'Quantum Support Vector Machine for Big Data Classification', Phys. Rev. Lett. 113, 2014.

significant speed-up of data processing for large amounts of data, which can be crucial in ongoing investigations.

Analysing large amounts of data is becoming increasingly critical to the success of criminal investigations. For instance, a case may involve a large-scale search through a law enforcement database, such as on images with certain properties or to match certain features of digital evidence such as source media or fingerprints. The information collection may also include large-scale analysis of open-source intelligence, including the internet or live feed information for an immediate suspect. In any of such cases, potential speed-ups due to a quantum-accelerated data analysis pipeline may prove crucial to achieve timely and accurate results. Examples may include Grover's algorithm as the basis for search tasks, quantum optimisation tasks for the clustering of data or matching and classification using quantum machine learning.

As with all current technology based on quantum computing, for the time being quantum machine learning is an experimental and purely explorative research subject. There is considerable hype around the potential use of quantum computers to accelerate AI applications, which is largely driven by the already existing hype around AI systems alone. Nonetheless, potential benefits are real, and considering the enormous amounts of data from which the analysis of large and complex datasets, predictive tools and machine learning algorithms can benefit, quantum acceleration on the predicted scales would make a real difference. In addition, law enforcement is facing increasing amounts of data, which will lead to a growing need to sort and analyse increasing amounts of investigative data. As digital transformation changes the face of crime, faster processing can make all the difference.

DEEP DIVE: QUANTUM MACHINE LEARNING

Several proven, fundamental quantum algorithms have been shown to guarantee exponential speed-ups for some crucial machine learning and basic data analysis routines once a universal, fault-tolerant quantum computer will be available. The range of basic routines known as QBLAS ('Quantum Basic Linear Algebra Subroutines') alone could eventually have a significant impact in accelerating statistical data analysis and machine learning³². Important examples include Grover's algorithm for search tasks in large databases (quadratic speed-up), the quantum Fourier transform for data processing (exponential speed-up), the HHL algorithm and its successors for fundamental tasks in implementing statistical estimation and machine learning algorithms such as matrix inversion, or approaches to faster finding of eigenvalues and vectors (quadratic speed-ups).

32 Biamonte, J., Wittek, P., Pancotti, N., Rebentrost, P., Wiebe, N., Lloyd, S., 'Quantum Machine Learning', 2017, [accessed 22/06/2023], <https://www.nature.com/articles/nature23474/>.

In addition, even current NISQ devices are already usable in those fields for approximation algorithms. There is justified hope and initial restricted work^{33,34} showing that hybrid quantum-classical approaches and approximate algorithms on NISQ devices could show a quantum advantage for machine learning at some point. Some examples include the thriving research field of quantum kernel-based machine learning³⁵, experiments with quantum neural networks by replacing computational layers with qubit representations and variational and optimisation algorithms originally more aimed at quantum system simulation such as the quantum approximate optimisation algorithm (QAOA) or quantum annealing, all showing some potential for machine learning, optimisation tasks and data analysis.

Additionally, the advantages derived from quantum approaches may be driven by more than improved performance in machine learning algorithms, as quantum technology has a wider range of applications. For instance, machine learning is already very well suited and used to employing hardware accelerators, such as GPUs, and it stands to reason to expect a similar class of quantum accelerators³⁶, long before universal quantum computers will be available. Moreover, there is considerable discussion that quantum algorithms and quantum data representations might lead to approaches with better generalisation behaviour. Generalisation behaviour refers to the concept of an algorithm being able to handle input or information that lies outside of the range of data on which it has been trained. In practice this means that a model can generalise learned patterns and apply them to other areas. For that reason, it may mitigate the notorious issue of overfitting³⁷ in deep learning³⁸. All these developments may create an opportunity which should be carefully watched for an emerging, potential near- and mid-term quantum advantage, albeit often with no theoretical guarantees of success³⁹.

Hybrid quantum-classical approaches and approximate algorithms on NISQ devices show potential to improve machine learning, optimisation tasks and data analysis.

- 33 Havlicek, V., Corcoles, A.D., Temme, K., Harrow, A.W., Kandala, A., Chow, J.M., Gambetta, J.M., 'Supervised learning with quantum-enhanced feature spaces', Nature 567, 2019, p. 209-212.
- 34 Saggio, V., Asenbeck, B.E., Hamann, A., Strömberg, T., Schianky, P., Dunjko, V., Friis, N., Harris, N.C., Hochberg, M., Englund, D., Wölk, S., Briegel, H.J., Walther, P., 'Experimental quantum speed-up in reinforcement learning agents', Nature 591, 2021, p. 229-233.
- 35 Reberntrost, P., Mohseni, M., Lloyd, S., 'Quantum Support Vector Machine for Big Data Classification', Phys. Rev. Lett. 113, 2014.
- 36 Quantum accelerators refer to specialised devices designed to harness quantum system capabilities that can work together with classical computers in order to accelerate computational problems typically suitable for quantum algorithms. Examples include specialised processing units, software development kits, cloud services, and more.
- 37 Overfitting in the context of deep learning refers to the concept of a model showing very good performance on training data but failing to generalise patterns to handle 'new' data outside of the training data set.
- 38 Wittek, P., 'Quantum Machine Learning. What Quantum Computing Means to Data Mining.', 2014.
- 39 Aaronson, S., 'Read the fine print', Nature Physics 11, 2015, p.291-293.

Quantum communications – new, highly secure networks to exchange information

Quantum communications primarily refers to the Quantum Key Distribution. The same technology underlying the design of qubits can be employed beyond the aim of building quantum computers. This wider scope is broadly referred to as quantum technologies. An already relatively mature field of quantum technologies is the field of quantum communication and quantum channels, which designs networks to exchange information between quantum systems. Single qubits or entangled groups of qubits can already be exchanged in this way. Applications range from designing quantum computing networks to specific uses in the area of secure communication. This applies in particular to quantum key distribution and exchange protocols, which may provide new means of secure communication for any party in possession of this technology⁴⁰. This can of course be employed both for security purposes, as well as by criminal actors.

IMPACT AND OUTLOOK

Quantum key distribution is already possible for distances of 50 to 100 km, but theoretical studies have shown that for distances greater than 300 km, classical repeaters would be needed to propagate further the quantum information, meaning the loss of quantum end-to-end security. Several options are considered to secure these relays from tampering, such as using satellite relays.

- ▶ **Positive:** Law enforcement may be able to make use of quantum communications to establish highly secure communication channels for information exchange, which may particularly facilitate the sharing of relevant information in the context of criminal investigations.
- ▶ **Negative:** criminal / terrorist / state actors could make use of quantum channels to evade law enforcement detection and prevent criminal prosecution.

Quantum communications primarily refers to quantum key distribution, but this should be extended to signatures and authentication protocols in the future, with the aim of building quantum networks, or even a quantum internet.

In order to keep up with the progress of the US, China, Japan and Korea on quantum networks, the European Union has launched a Quantum Communication Infrastructure program. There are already several quantum networks in Europe such as in the Netherlands or

40 Lewis, A., Travagnin, M., 'A Secure Quantum Communications Infrastructure for Europe: Technical background for a policy vision', EUR 31133 EN, Publications Office of the European Union, Luxembourg, 2022, ISBN 978-92-76-53705-2, 2022, [accessed 22/06/2023], doi:10.2760/180945, JRC129425.

in Italy, which encourage further developments and studies of this technology⁴¹.

DEEP DIVE: QUANTUM KEY DISTRIBUTION

Quantum key distribution refers to the process of exchanging a secret key between a receiver and a sender by means of quantum technology, which can later be used in a symmetric (classical) cryptographic encryption protocol. It works by using entangled quantum particles, such as for example photons, to encode random bits and transmit their information through a quantum channel. The advantage is that, by quantum mechanical principles, any interaction with the quantum particles would modify their state, thereby offering inherent protection against eavesdropping or active tampering of the information. This would provide highly secure key exchange protocols to protect sensitive communications, data and critical infrastructures.

Quantum metrology and quantum sensors: improving crime scene investigation and forensics analysis

Within the evolving landscape of new quantum technologies, quantum metrology and the use of quantum sensors are predicted to play a significant role in transforming various sectors, including law enforcement. Although they are not as prominently featured in the headlines, new quantum sensors are by far the most advanced⁴² technology discussed in this report, already reaching unprecedented levels of measurement accuracy in laboratory experiments today⁴³.

Quantum sensors have the potential to drastically improve the accuracy, precision and sensitivity of measurements, enabling a host of innovative applications with potential impact on law enforcement strategies and operations, such as forensics, crime scene investigation, surveillance and detection methods or situational decision-making based on sensor data.

41 European Commission, 'The European Quantum Communication Infrastructure (EuroQCI) Initiative', 2023, [accessed 03/07/2023], <https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci>.

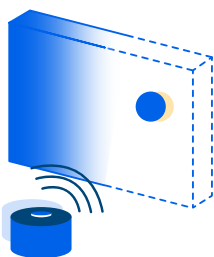
42 Defense One, 'Quantum Sensors – Unlike Quantum Computers – Already Here', 2022, [accessed 22/06/2023], <https://www.defenseone.com/ideas/2022/06/quantum-sensorsunlike-quantum-computersare-already-here/368634/>.

43 Giovannetti, V., Lloyd, S., Maccone, L., 'Advances in quantum metrology', Nature Photonics(5), 2011, p. 222-229, [accessed 22/06/2023], <https://www.semanticscholar.org/paper/Advances-in-quantum-metrology-Giovannetti-Lloyd/5115b3ba9e6b8fb68685bc50f303457564d4d993>.

Metrology & sensors



PRECISION FORENSICS



IMPROVED SURVEILLANCE & DETECTION



REAL-TIME DECISION MAKING

IMPACT AND OUTLOOK

- ▶ **Precision Forensics:** the enhanced sensitivity and miniaturisation of quantum sensors could impact forensic science and crime scene investigation techniques. New techniques may allow for the detection and analysis of clues and trace substances at a crime scene that would be undetectable to current technologies, including chemicals and fingerprint analysis. In general, the forensic survey of crime scenes could be aided by miniaturised devices and new in-situ tests, potentially moving some forensic analyses from the laboratory into manageable time frames on the scene. Crime scene forensics may in general benefit from enhanced capabilities in quantum computing, by opening the potential to decrease post-data processing times for sorting through data and 3D scene reconstructions down from days to much shorter time scales. All this could improve the reliability of evidence and decrease the chance of wrongful convictions.
- ▶ **Improved Surveillance and Detection:** surveillance and detection capabilities may be dramatically affected by quantum sensors. For instance, quantum radar and LIDAR (Light Detection and Ranging) systems could detect objects or individuals at distances at accuracies that are currently unattainable. Quantum ghost imaging allows optical cameras to record images of objects at extremely low levels of light or beyond the line-of-sight or blocked by other objects⁴⁴. Quantum-enhanced magnetic sensors could be used to detect hidden weapons, and quantum gravimeters could detect underground structures with unprecedented capabilities, both examples providing significantly enhanced or even entirely new sources of information.

44 Pittman, T.B., Shih, Y.H., Strekalov, D.V., Sergienko, A.V., 'Optical imaging by means of two-photon quantum entanglement', Phys.Rev.(52), 1995, [accessed 22/06/2023], <https://doi.org/10.1103/PhysRevA.52.R3429>.

- ▶ **Real-time Decision Making:** real-time data processing with quantum sensors could provide law enforcement officers with faster and more accurate decision-making in critical situations. For instance, quantum-based GPS systems unaffected by jamming or spoofing could provide dependable location data, essential in time-sensitive operations⁴⁵.

Crime Scene Forensics with Quantum Sensors

Forensic crime scene investigation relies on a wide range of forensic sensors, including for instance for biological trace analysis, drug screening, toxicological testing, biometrical analysis such as taking trace fingerprints or environmental testing, ballistics and physically surveying the crime scene. At a crime scene, speed, specificity and sensitivity of the forensic analysis are critical factors for the success of an investigation and for the fairness and impartiality of the judiciary.

New types of sensors based on modern quantum technologies may hold the potential to replace costly forensic laboratory tests with faster, significantly smaller, cheaper and potentially even better in-situ sensors employed at a crime scene, or to dramatically increase the sensitivity and specificity of existing tests.

Typical examples of relevant quantum sensing systems in development are nanoparticle-based biosensors for biological traces, e.g. based on so-called quantum dot designs⁴⁶, which are already employed in medicine but have yet to find widespread application in forensics analysis⁴⁷. Similar sensors are already proposed for environmental screening of chemicals and toxicological substances, e.g. traces of explosives or toxins⁴⁸. Equally, proposals exist for in-situ forensic investigation of fingerprints using quantum-sensing fluorescence techniques.

While quantum sensing is still an emerging technology, it is considerably more mature than quantum computers. As the transformative potential of quantum sensing technology has already been acknowledged in the defence security sector^{49,50}, we argue that law enforcement agencies and internal security institutions should take note of this. Some new capabilities are already achievable today, and it is likely that more technologies will be available soon. It is entirely possible that the first real transformative impact of the same quantum technologies underlying the development of qubits might first have a noticeable technological impact on the ground through generally enhanced measurement technology.

45 Krelina, M., 'Quantum technology for military applications', *EPJ Quantum Technology* (8), 2021, [accessed 22/06/2023], <https://link.springer.com/content/pdf/10.1140/epjqt/s40507-021-00113-y.pdf>.

46 Costanzo, H., Gooch, J., Frascione, N., 'Nanomaterials for optical biosensors in forensic analysis', *Talanta* (253), 2023, [accessed 22/06/2023], <https://www.sciencedirect.com/science/article/pii/S003991402200741X>.

47 Costanzo, H., Gooch, J., Frascione, N., 'Nanomaterials for optical biosensors in forensic analysis', *Talanta* (253), 2023, [accessed 22/06/2023], <https://www.sciencedirect.com/science/article/pii/S003991402200741X>.

48 Ganesan, M., Nagaraaj, P., 'Quantum dots as nanosensors for detection of toxics: a literature review', *Analytical Methods* (35), 2020, [accessed 22/06/2023], <https://pubs.rsc.org/en/content/articlelanding/2020/ay/d0ay01293a/unauth>.

49 Krelina, M., 'Quantum technology for military applications', *EPJ Quantum Technology* (8), 2021, [accessed 22/06/2023], <https://link.springer.com/content/pdf/10.1140/epjqt/s40507-021-00113-y.pdf>.

50 BAE Systems, 'What is Quantum Sensing', 2023, [accessed 22/06/2023], <https://www.baesystems.com/en-us/definition/what-is-quantum-sensing>.

This possibility should not be overlooked while focusing on the greater goal of a quantum computer.

While quantum sensing is still an emerging technology, it is considerably more mature than quantum computers.

Quantum machine learning will accelerate the use of AI and machine learning tools, but will not necessarily involve completely disrupting paradigm shifts in the near future. Some theoretical quantum algorithms could have an enormous impact on big data, search and large-scale data mining. Quantum sensors and quantum metrology hold substantial promise for law enforcement, offering the potential for transformative applications in the use of measurement devices in forensics, detection and decision making. New techniques may allow for the detection and analysis of clues and trace substances at a crime scene that would be undetectable to current technologies, including chemicals and fingerprint analysis. Quantum ghost imaging allows optical cameras to record images of object at extremely low levels of light or beyond the line-of-sight or blocked by other objects. Real-time data processing with quantum sensors could provide law enforcement officers with faster and more accurate decision-making in critical situations.

DEEP DIVE: QUANTUM SENSORS

Quantum sensors are devices that exploit quantum phenomena to measure physical quantities with increased performance, either by increasing sensitivity or accuracy compared to classical sensors or by opening entirely new channels of sensing, such as through materials or beyond the line-of-sight. As quantum computers, these sensors leverage the properties of quantum mechanics – such as superposition and entanglement – to achieve enhanced measurement sensitivity and resolution. Often, they are based on technology similar to that needed for qubits, such as quantum optics or solid-state advances for chemical sensors. The physical quantities that can be measured with quantum system-based sensors range from time, temperature, magnetic fields, gravity and motion to electromagnetic radiation, including optical light, and many more.

Conclusion

Quantum metrology is the scientific field that employs quantum mechanical principles to develop measurement standards and protocols that increase the precision and accuracy of measurements with quantum sensors beyond the limits set by classical physics.

Technology foresight plays a crucial role in ensuring better law enforcement preparedness for the future. The active monitoring of key emerging technological developments allows law enforcement to react more quickly and take the necessary steps to mitigate potential threats, as well as leverage the potential resulting from them. Only by identifying relevant emerging developments early on can the necessary actions be taken in time. While quantum computing and quantum technologies have been a field of interest for a while, the recent progress achieved requires a renewed, in-depth look at the resulting implications. This report provides an extensive assessment of this impact from the law enforcement perspective.

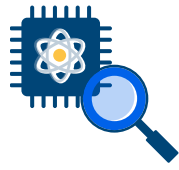
The advent of quantum computing promises to bring about transformative changes in various fields, with significant implications for law enforcement. One area in which this impact will be critical is cryptography. The potential ability of quantum computers to efficiently decrypt information will require a paradigm shift in how we approach data protection, urging law enforcement agencies to review their processes and transition to post-quantum cryptographic systems. At the same time, law enforcement agencies may also benefit from new possibilities in the field of decryption to fight against serious organised crime and terrorism.

As demonstrated in this report, however, the impact of quantum computing and quantum technologies extends far beyond cryptography. Quantum technologies carry enormous potential to facilitate the analysis of large and complex datasets, a challenge of increasing importance for law enforcement agencies. Similarly, improvements in machine learning and artificial intelligence may enable greater efficiency and innovative ways of solving complex problems. Finally, other uses of quantum technologies could facilitate the establishment of novel, secure communications systems, as well as improved reliability of evidence and the forensic detection of currently invisible traces.

Although there is uncertainty regarding the precise timeline for quantum computers becoming widely available, it is crucial that law enforcement agencies begin preparing now. This includes actively observing relevant developments, experimenting with the currently available technology, as well as liaising closely with subject matter experts. While these types of technological advancement offer significant potential benefit, they also pose risks for the rights of citizens, if not used responsibly. This means that any use of quantum technologies requires a thorough assessment of the potential fundamental rights impact they might generate, and the necessary steps must be taken to mitigate any negative consequences. In all of these areas, law enforcement must acquire

the required expertise to effectively harness the potential of this technology and adapt to the challenges it presents.

Key recommendations



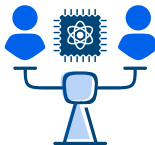
OBSERVE QUANTUM TRENDS



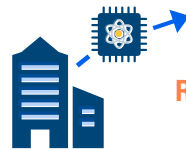
BUILD UP KNOWLEDGE AND START EXPERIMENTING



FOSTER RESEARCH & DEVELOPMENT PROJECTS



ASSESS THE IMPACT OF QUANTUM TECHNOLOGIES ON FUNDAMENTAL RIGHTS



REVIEW ORGANISATIONS TRANSITION PLANS

Despite rapid technological progress in the development of universal quantum computers, there is no certainty as to when this work is going to be completed. Key stakeholders engaged in this pursuit have published ambitious timelines envisaging the production of universal quantum computers in the early 2030s. While this might sound optimistic, experts nonetheless agree that this is bound to happen at some point in the near future, with predictions of up to 20 years and beyond in a recent JRC survey⁵¹. Until this goal is reached, however, a number of key challenges remain to be addressed, namely relating to improving the speed, scalability and accuracy of quantum computers. These are reflected in the key technological development stages, as listed above, that will need to be completed before quantum algorithms can be run efficiently.

Going forward, timelines will become clearer. Both public and private entities are actively working on achieving the development of universal quantum computers, which means that the rate of

⁵¹ Travagnin, M., Lewis, A.M., Ferigato, C., Florescu, E., 'The Impact of Quantum Technologies on the EU's Future Policies. Part 3, Perspectives for Quantum Computing.', JRC Sci. Tech. Res. Rep., Nov. 2018, 2018, [accessed 22/06/2023], <https://doi.org/10.2760/737170>.

progress is expected to continue at pace. With a growing focus on the potential impact of quantum computers in the near future, there will likely be an increase in investments into research and development, leading to further acceleration.

As the arrival of universal quantum computers draws nearer, it is critical to understand the impact this technology will have on various sectors. This report serves as the first in-depth exploration of the impact of quantum computing and quantum technologies from the perspective of law enforcement. In exploring this impact, this report emphasises the need for further work and research to fully comprehend and navigate the quantum era. By taking proactive steps today, the law enforcement community can ensure greater readiness to face the challenges and opportunities presented by this type of technology in the future.

Glossary

ALGORITHM: set of sequential instructions applied on specific input(s) to reach a predefined goal, ranging from the output of a basic mathematical function to more complex tasks.

BRUTE-FORCING: process of trying all possible combinations of characters from a defined alphabet until a targeted password is retrieved.

CRYPTOGRAPHY: the elaboration of secure protocols aiming at protecting information from unwanted third-party access, particularly ensuring its authenticity, integrity and confidentiality.

CRYPTOGRAPHIC KEY: a piece of information used to encrypt and decrypt information.

CRYPTOLOGY: the science of secrecy, aimed at ensuring the confidentiality, authenticity and integrity of the information exchanged between the sender and the receiver.

CRYPTANALYSIS: identification and analysis of potential vulnerabilities in cryptographic schemes.

DECOHERENCE: process in which quantum systems lose their inherent quantum traits, such as by interacting with their external environment.

DICTIONARY ATTACK: process of guessing a password by testing all candidates from a list of likely options.

ENTANGLEMENT: the quantum physical principle whereby composite physical systems such as several qubits are so closely related that by obtaining information about the state of one system, we automatically know the state of its companion – even if they are far apart.

FAULT INJECTION ATTACKS: the purposeful injection of faults into a system to get the system to malfunction. This malfunction can reveal sensitive information or weaken in-built security measures. Examples include introduction software glitches or physically tampering with the hardware.

HASH FUNCTIONS: take an input (i.e. a plaintext string) and return a unique string sequence of characters and numbers. This output is referred to as a hash.

KEY DERIVATION FUNCTION (KDF): process deriving a secure random cryptographic key from a less secure piece of information typically being a password or a passphrase mixed with random data.

NISQ: Noisy Intermediate-Scale Quantum (NISQ) devices are quantum devices that are an intermediate stage towards universal quantum computers. While they have not proven a speed-up over classical computers, NISQs are useful for further research and development.

ORACLE FUNCTION: an 'oracle function' in the context of decryption is a theoretical technique used in the formalisation of security proofs of cryptographic systems.

POST-QUANTUM CRYPTOGRAPHY (PQC): cryptographic algorithms designed to be secure against attacks from both classical as well as quantum computers.

QUANTUM ALGORITHMS: algorithms specifically designed to be run on quantum computers. They exploit specific quantum properties (such as superposition and entanglement) to solve specific problems more efficiently than classical algorithms.

QUANTUM CIRCUIT: sequence of quantum operations that are applied to qubits.

QUANTUM COMPUTERS: devices based on the laws of quantum mechanics that exploit the behaviour of quantum systems. By making use of qubits to execute certain algorithms, quantum computers significantly reduce the number of needed calculations compared to classical computers for specific problems. This unlocks a number of new possibilities in the development of algorithms.

QUANTUM KEY DISTRIBUTION (QKD): the process of exchanging a secret key between a receiver and a sender by means of quantum technology, which can later be used in a symmetric (classical) cryptographic encryption protocol.

QUANTUM MACHINE LEARNING: the application of quantum approaches, such as quantum computers and quantum algorithms, to machine-learning processes in order to improve performance.

QUANTUM SENSORS: devices that exploit quantum phenomena to measure physical quantities with increased performance, either in simply advancing sensitivities or accuracy with respect to classical sensors or by opening entirely new channels of sensing, such as through materials or for potential sensing of objects beyond the line-of-sight.

QUANTUM TECHNOLOGIES: technologies relying on the properties of quantum mechanics, including quantum computing, quantum sensors and quantum metrology, quantum communication, quantum imaging, among others.

QUBITS: whereas bits can only have two values (0 or 1), qubits can exist in a combination of both states simultaneously. Qubits offer different possibilities by exploiting quantum effects, such as superposition and entanglement.

SAT (SATISFIABILITY) SOLVERS: software that helps determine if a solution exists to complex logical formulas.

SEED: initial value from which a pseudorandom alphanumeric sequences is generated. Seeds are used, for instance, to create cryptographic keys.

SIDE-CHANNEL ATTACKS: allow forensic investigators to extract sensitive information from a system by examining a system's inputs and outputs. This side data can compromise the security infrastructure of the system and reveal information relating to encryption keys or other sensitive data. Examples include analysing the system's power consumption, time needed to perform certain operations, or electromagnetic emanation.

SUPERPOSITION: the ability of a qubit to be in more than one state at the same time until it is measured.



About the Europol Innovation Lab

Technology has a major impact on the nature of crime. Criminals quickly integrate new technologies into their modus operandi, or build brand-new business models around them. At the same time, emerging technologies create opportunities for law enforcement to counter these new criminal threats. Thanks to technological innovation, law enforcement authorities can now access an increased number of suitable tools to fight crime. When exploring these new tools, respect for fundamental rights must remain a key consideration.

In October 2019, the Ministers of the Justice and Home Affairs Council called for the creation of an Innovation Lab within Europol, which would develop a centralised capability for strategic foresight on disruptive technologies to inform EU policing strategies.

Strategic foresight and scenario methods offer a way to understand and prepare for the potential impact of new technologies on law enforcement. The Europol Innovation Lab's Observatory function monitors technological developments that are relevant for law enforcement and reports on the risks, threats and opportunities of these emerging technologies. To date, the Europol Innovation Lab has organised three strategic foresight activities with EU Member State law enforcement agencies and other experts.

www.europol.europa.eu

