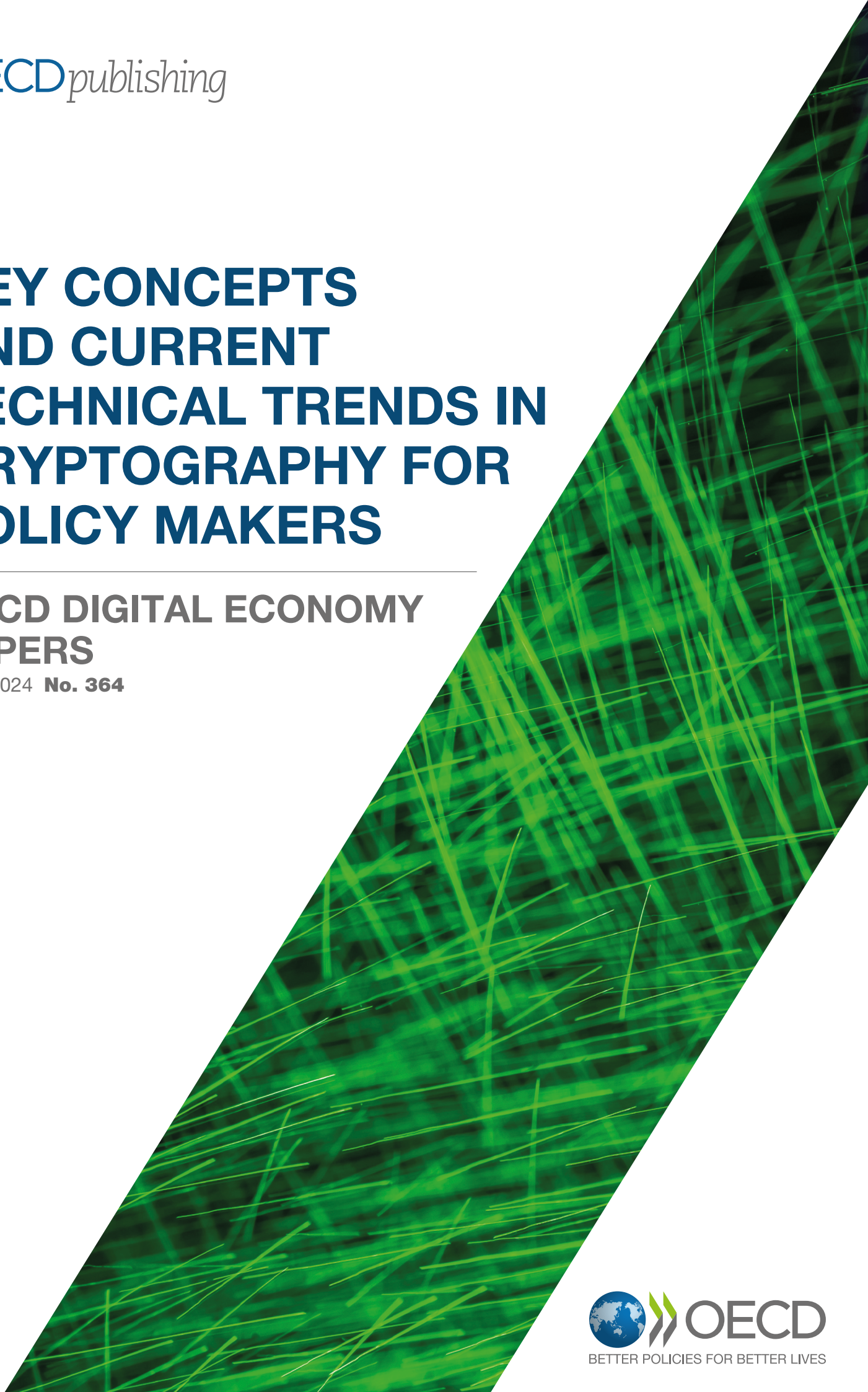
OECD publishing

KEY CONCEPTS AND CURRENT TECHNICAL TRENDS IN CRYPTOGRAPHY FOR POLICY MAKERS

OECD DIGITAL ECONOMY PAPERS
June 2024 **No. 364**



OECD
BETTER POLICIES FOR BETTER LIVES

Foreword

This report was prepared by the OECD Working Party on Digital Security (WPDS) of the Digital Policy Committee to support the fifth review of the 1997 OECD Recommendation concerning Guidelines on Cryptography Policy [OECD/LEGAL/0289] (hereafter the "Recommendation"). The conclusions of the review are presented in a separate document [DSTI/DPC/DS(2024)1/FINAL].

This report was drafted by Laurent Bernat, under the supervision of Jeremy West. It was approved and declassified by the Digital Policy Committee (DPC) on 5 April 2024 and prepared for publication by the OECD Secretariat.

Note to Delegations

This document is also available on O.N.E Members & Partners under the reference code:

DSTI/CDEP/SDE(2023)10/FINAL

Table of contents

FIGURES

TABLES

Executive summary

This report provides a basic introduction to cryptography for policy makers, including key concepts such as symmetric and asymmetric cryptography, public key infrastructure, end-to-end encryption, cryptanalysis, etc. The bulk of the report is a discussion of disruptive developments in homomorphic encryption and quantum-related cryptographic research. The following key points emerge from the research.

Cryptography is a fundamental digital security technology at the core of digital trust. Although most people rarely notice its use and barely understand how it works, it is the technical building block supporting user trust in their devices, software, and communications for personal, commercial, legal, business, governmental and other purposes. Cryptography supports the confidentiality and integrity of data in communication (in transit) and in storage (at rest). Digital signatures provide authenticity of information and prevent an involved party from denying its responsibility related to that information, such as authoring or sending it.

The implementation of any technology, cryptography included, can introduce weaknesses and technological developments such as homomorphic cryptography and quantum information technologies are creating new opportunities and challenges for cryptography.

Homomorphic encryption is an innovative cryptographic method that allows certain computations to be performed on encrypted data without the need to decrypt it first, and without requiring access to the secret key. Once mature, it could allow processing of financial, medical, location, and other confidential data without revealing their content or affecting privacy. Such data processing could take place in untrusted environments like public cloud infrastructures, reducing concerns such as data localisation and data breaches.

However, fully homomorphic encryption (FHE) is still just a promising area of research rather than a mature disruptive technology. It is often described as “the holy grail of cryptography”. Homomorphic encryption is available today, but only with algorithms that have significant performance, correctness, and usability limitations and weaknesses, restricting their potential use to niche applications. However, significant research and standardisation efforts to achieve FHE are underway and, according to some experts, today this technology is perhaps where machine learning was ten years ago.

Quantum technologies, which leverage physical properties of particles at the subatomic level, have the potential to threaten the foundations of public key cryptography and undermine our economies’ digital trust. In theory, a mature quantum computer would multiply processing power and speed by several orders of magnitude, allowing it to solve some of the most complex challenges of our time, for example in genetic, materials and climate sciences. However, a mature quantum computer could also easily break public key cryptography by solving the mathematical problems at its core that currently guarantee its robustness. This would have immense consequences because the vulnerability of these cryptosystems to a quantum attack would lead to the vulnerability of all security protocols that derive security from public key cryptography, and of any product or security system deriving security from these protocols. In brief, this would break the security of most, if not all, encrypted data in storage and in transit.

The race to develop more powerful quantum computers is accelerating, but current quantum computers are still several orders of magnitude away from threatening current cryptographic algorithms. Significant public and private research investments in OECD countries and beyond are boosting quantum computing research. However, design and engineering challenges are extremely significant and overcoming them in a short timeframe would require a concerted research programme of an Apollo or Manhattan project's scale. That makes estimating a realistic timeframe for the development of a quantum computer capable of breaking current cryptography very difficult.

Nevertheless, tomorrow's quantum computing impact on cryptography must be addressed today. There is evidence that some countries have already taken an "intercept and store now, decrypt later" approach, collecting high-value encrypted data today with the expectation to decrypt it later once a quantum computer is available to them (a "retroactive attack"). At that time, stakeholders will face a rapid collapse of their cryptographic architecture and will have little time to react. Long-term confidentiality protection is essential for the most sensitive encrypted data – from genetic, biometric, financial and other sensitive personal data to state secrets, long-term business development data and negotiation information. It is also critical for high-value, root-level public keys that are intended to have long operational lifetimes.

The solution to address this challenge is the progressive transition from current quantum vulnerable cryptographic algorithms to quantum resistant cryptography (QRC). Considering the significant and growing research investments in quantum technologies, experts are sounding the alarm and calling for a transition to QRC sooner rather than later. QRC, also known as post-quantum, quantum safe or quantum secure cryptography, is a family of new cryptographic algorithms that are immune to attacks leveraging both traditional and quantum computers, and that can be executed on traditional computers with traditional communication channels. Cybersecurity agencies from Australia, Canada, France, Germany, the United Kingdom, and the United States are encouraging stakeholders to start transitioning their products and information systems' security towards using QRC, a process that may take many years to complete. Several QRC algorithms have already been tested and selected through an international process carried out by the US National Institute for Standards and Technologies (NIST).

Quantum cryptography, also known as quantum key distribution (QKD), also carries an enormous potential for more secure communications, but is not yet ready for sensitive applications. It is a cryptography technology based on quantum communications that takes advantage of the laws of physics rather than mathematical complexity to ensure confidentiality. In theory, quantum cryptography, which is available today, can remain secure regardless of the amount of processing power and mathematical innovation an adversary uses to defeat it. However, it requires expensive, dedicated equipment with extremely low tolerance for error to leverage the quantum state of micro particles. This is the main reason many cybersecurity agencies discourage its use for sensitive applications at this point, and instead call for the adoption of QRC, which can run on existing computers.

1 Introduction

Cryptography is a fundamental digital security technology at the core of our economies' and societies' digital fabric. Although most people rarely notice its use and barely understand how it works, it is the technical building block that allows users to trust their devices, software, and communications for personal, commercial, legal, business, governmental and other purposes. The first section of this report provides a basic introduction to cryptography for policy makers, including key concepts such as symmetric and asymmetric cryptography, public key infrastructure, end-to-end encryption, and cryptanalysis. The second section includes a discussion of homomorphic encryption and quantum information technologies, two areas that could disrupt trust in our digitally dependent economy and societies. It also reviews approaches that some view as options to enable law enforcement to carry out their missions without undermining cryptography, such as lawful hacking, key escrow, and client-side scanning.

To put the sections exploring cryptography and its recent evolutions into the context of this report's purpose, which is to help gauge the continuing relevance of the 1997 OECD Recommendation concerning Guidelines on Cryptography Policy [OECD/LEGAL/0289], this introduction:

- explains the main cryptography policy challenge, namely the need to foster its use as a driver of trust in the digital era without jeopardising public safety and briefly introduces the OECD policy principles adopted in 1997 to guide public policy making in this area; and
- provides a short history of the subsequent debates, the so-called "crypto wars".

Fostering trust without jeopardising public safety

Cryptography is a vital enabling technology for trust in the digital environment and has become a commodity technology, used by everyone, although often unknowingly. However, the wide availability of cryptography can turn into a challenge when criminals and other malicious actors use it to protect their nefarious activities from investigations by law enforcement and national security agencies.

This challenge is not new. Before the beginning of the Internet era in the mid-1990s, cryptography was regulated in many countries to prevent its use by offensive actors. Robust cryptographic methods, called "strong cryptography", were limited to some well-known use cases such as military and diplomatic communications, as well as high-end commercial and contractual negotiations. Furthermore, many governments also regulated the exportation of cryptographic devices and programmes, including through the 1996 Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-use Goods and Technologies.

The Internet changed that situation, as cryptography rapidly became the missing part in the engine that would turn the "information superhighways" into a driver for new sources of economic growth and deep societal change. Businesses wanted cryptography to enable secure business-to-business, business-to-consumer and business-to-government interactions, including electronic commerce and the provision of innovative services; individuals wanted it to strengthen privacy in their personal, commercial, and official internet communications; and governments needed it to enable electronic government services, as well as to secure their own government-to-government interactions, with all the associated benefits in terms of cost reduction, service improvement, etc.

Furthermore, existing exportation or usage restrictions became simply unenforceable in practice because the Internet removed practical barriers to accessing cryptographic software. Anyone with the right skills and knowledge could code a cryptographic algorithm into a programme and share it with the entire world without restrictions, thanks to the new Internet-enabled "borderless world". The most well-known example was Phil Zimmerman's Pretty-Good-Privacy (PGP), an asymmetric cryptography programme famously uploaded on the Internet in 1991 (Zimmermann, 2021[1]).

In sum, cryptography regulation, where it existed, became an obstacle to Internet-driven economic and social benefits, and its implementation became impracticable. However, the prospect of deregulation in this area sparked intense debates on how law enforcement, public safety and national security agencies would be able to continue to exercise lawful access to plaintext data at rest and in transit for investigations and other purposes if cryptography became widely available. This initial period was often referred to as the "crypto war", a cycle of battles between supporters and opponents of deregulation, which extended over time to "crypto wars".

In 1997, the OECD Council adopted the Recommendation concerning Guidelines on Cryptography Policy, which includes a set of high-level policy principles in its annex (the "Guidelines") on how to promote cryptography to foster trust in the use of digital technologies to support economic and social objectives without unduly jeopardising public safety, law enforcement, and national security. Box 1 provides an overview of the Guidelines. Following the adoption of the Recommendation, OECD Members deregulated cryptography and the Internet evolved from the "information superhighways" of the early 1990s to today's backbone for digital transformation.

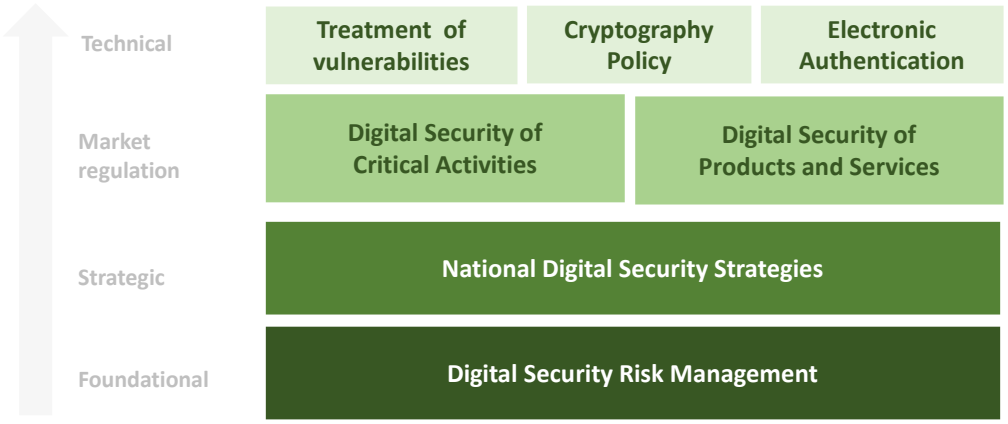
The Recommendation is part of the technical layer of the *OECD Digital Security Policy Framework: Cybersecurity for Prosperity*, illustrated in Figure 1, which charts the economic and social dimension of cybersecurity, highlights the OECD approach to digital security policy and equips policymakers to use OECD digital security Recommendations (OECD, 2022[2]). Table 1 provides a list of other OECD standards related to the Guidelines. In addition, the Guidelines are also related to the 2022 Declaration on Government Access to Personal Data Held by Private Sector Entities, which reflect OECD Members' agreement on common approaches to safeguard privacy and other human rights and freedoms when accessing personal data for national security and law enforcement purposes.

Box 1. Overview of the Guidelines

1. **Trust in cryptographic methods:** cryptographic methods should be trustworthy in order to generate confidence in the use of information and communications systems. Market forces should serve to build trust. Government regulation, licensing and use of cryptographic methods may also encourage user trust. The evaluation of cryptographic methods, especially against market-accepted criteria, could also generate user trust.
2. **Choice of Cryptographic Methods:** users should have a right to choose any cryptographic method, subject to applicable law.
3. **Market Driven Development of Cryptographic Methods:** cryptographic methods should be developed in response to the needs, demands and responsibilities of individuals, businesses and governments.
4. **Standards for Cryptographic Methods:** Technical standards, criteria and protocols for cryptographic methods should be developed and promulgated at the national and international level.
5. **Protection of Privacy and Personal Data:** The fundamental rights of individuals to privacy, including secrecy of communications and protection of personal data, should be respected in national cryptography policies and in the implementation and use of cryptographic methods.
6. **Lawful Access:** National cryptography policies may allow lawful access to plaintext, or cryptographic keys, of encrypted data. These policies must respect the other principles contained in the Guidelines to the greatest extent possible.
7. **Liability:** whether established by contract or legislation, the liability of individuals and entities that offer cryptographic services or hold or access cryptographic keys should be clearly stated.
8. **International Co-operation:** Governments should co-operate to co-ordinate cryptography policies. As part of this effort, governments should remove, or avoid creating in the name of cryptography policy, unjustified obstacles to trade.

Note: This overview does not reproduce the full text of the Guidelines. For the full text see: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0289
Source: OECD.

Figure 1. OECD Policy Framework on Digital Security



Source: OECD (2022), *OECD Policy Framework on Digital Security: Cybersecurity for Prosperity*, OECD Publishing, Paris, https://doi.org/10.1787/a69df866-en.

Table 1. OECD standards related to the Guidelines

Year	OECD Standards	Reference
2023	Recommendation on the Governance of Digital Identity	[OECD/LEGAL/0491]
2022	Recommendation on Digital Security Risk Management *	[OECD/LEGAL/0479]
2022	Recommendation on National Digital Security Strategies *	[OECD/LEGAL/0480]
2022	Recommendation on the Digital Security of Products and Services *	[OECD/LEGAL/0481]
2022	Recommendation on the Treatment of Digital Security Vulnerabilities *	[OECD/LEGAL/0482]
2022	Recommendation on Blockchain and other Distributed Ledger Technologies	[OECD/LEGAL/0470]
2021	Recommendation on Enhancing Access and Sharing of Data	[OECD/LEGAL/0463]
2019	Recommendation on Artificial Intelligence	[OECD/LEGAL/0449]
2016	Declaration on the Digital Economy: Innovation, Growth and Social Prosperity (Cancún Declaration)	[OECD/LEGAL/0426]
2007	Recommendation on Electronic Authentication *	[OECD/LEGAL/0353]
1980	Recommendation concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (revised in 2013)	[OECD/LEGAL/0188]

* These Recommendations are introduced in the OECD Policy Framework on Digital Security: Cybersecurity for Prosperity (OECD, 2022[2])

A brief overview of the "crypto wars"

Following the adoption of the Guidelines, the crypto war continued, particularly in the United States and to a certain extent in the European Union. The crypto war did not take place between countries but rather between communities supporting and opposing the regulation of cryptography. It was fought in courts and legislative assemblies, as well as through countless reports, communiqués and statements by politicians, government officials, former officials, technical security and policy experts, civil society and business groups, and in numerous conferences and meetings over the last three decades[1]. A comprehensive account of arguments raised by the many stakeholders involved in the hundreds of initiatives and publications on this issue would require an entire study. For the sake of brevity, this section provides only an overview of the three main phases since the mid-1990s during which an increased demand for and adoption of cryptography was followed by a reaction from law enforcement agencies asking for more control over cryptography, which was resisted by various stakeholders such as business and a large coalition of civil society groups.

- *Phase 1: The Clipper chip against the backdrop of global Internet adoption*

In the mid-1990s, governments considered the need to foster the use of strong cryptography to encourage the adoption of Internet technologies for economic and social activities such as e-commerce and e-government. The Clipper chip was proposed by the US Government as a technical requirement to ensure access to encrypted information by law enforcement and national security agencies. The Clipper Chip was a cryptographic microchip featuring a special cryptographic algorithm and a key escrow system, allowing government agencies to access encrypted communications by holding and combining unique parts of a decryption key. Following intense debates, the proposal was abandoned and cryptography was deregulated in the United States and other countries, fostering greater trust in, and therefore the growth of, the global Internet and its economic and social uses. The policy debates about access by law enforcement and national security agencies to encrypted information became relatively quiet and remained that way for more than 15 years.

- *Phase 2: Backdoors for not "going dark" against a backdrop of surveillance and terrorism*

In 2013, the revelations of the surveillance programs conducted by the NSA and its partners generated a public outcry. In response to increased demand for stronger privacy and security online from businesses, individuals and governments, major ICT industry players decided to implement cryptography more systematically in their products and services, in transit and at rest. The Federal Bureau of Investigation

(FBI) claimed that with such measures, law enforcement agencies would lack the technical ability to intercept and access communications and information pursuant to court orders despite having the legal authority to do so (Comey, 2014[3]). To prevent the agencies from "going dark", the FBI Director called for technology companies to provide law enforcement with means to access encrypted data, a request many experts interpreted as a call for law enforcement backdoors in products and services, and firmly rejected as such.

This triggered an intense "going dark" debate, with statements calling cryptography an obstacle to law enforcement's efforts against terrorists (who had attacked several countries during the same period), and numerous voices arguing against any form of backdoors. These debates spanned across several years and took place in many countries. A few examples are provided in this section to illustrate their intensity.

Speaking one week after the 2015 Paris terrorist attacks and a few months before national elections, the UK Prime Minister David Cameron called for new legislation to ensure that "we do not allow terrorists safe space to communicate with each other" (Watt, Traynor and Mason, 2015[4]). The same year, the Manhattan district attorney Cyrus R. Vance Jr., Paris chief prosecutor François Molins, the commissioner of the City of London Police Adrian Leppard, and chief prosecutor of the High Court of Spain Javier Zaragoza blamed "the new encryption policies of Apple and Google [for making] it harder to protect people from crime" and called on "regulators and lawmakers to find an appropriate balance between the marginal benefits of full-disk encryption and the need for local law enforcement to solve and prosecute crimes" (Vance Jr et al., 2015[5]). A similar message was sent by Europol's Director, who called the decision of companies such as Apple to allow customers to encrypt their smartphones "disappointing" and "only adding to our problems in getting to the communications of the most dangerous people that are abusing the internet" (BBC, 2015[6]). A technical and legal battle between the FBI and Apple over unlocking an iPhone used by the perpetrator of the San Bernardino shooting in 2015 further fuelled the "going dark" debate.

The business and academic communities, and numerous civil society organisations, strongly opposed these arguments. For example, trade associations representing the US ICT sector called the White House to express its opposition "to any policy actions or measures that would undermine encryption as an available and effective tool" and urged the President "not to pursue any policy or proposal that would require or encourage companies to weaken these technologies, including the weakening of encryption or creating encryption *work-arounds*" (ITIC and SIIA, 2015[7]). A group of nearly 150 civil society groups, major companies, and security experts urged the President to oppose mandatory backdoors in cryptography (Open Technology Institute, 2015[8]). Fourteen world-renowned cryptography experts and security technologists opposed initiatives "mandating insecurity by requiring government access to all data and communications", emphasising that "the damage that could be caused by law enforcement exceptional access requirements [to encrypted data] would be even greater today than it would have been 20 years ago" (Abelson et al., 2015[9]). In 2015 and 2016, the US-based NGO Access Now organised a "crypto summit" to foster discussions among various policy, legal and technical experts in this area. A petition launched in 2016 by the Open Technology Institute to urge the White House to issue a statement in support of strong cryptography had received over 100 000 signatures (McLaughlin, 2015[10]).

Interestingly, not all voices in the national security establishment were aligned with proponents of the going dark narrative. For example, the former directors of key US intelligence, homeland security and defence agencies argued that "the greater public good is a secure communications infrastructure protected by ubiquitous encryption at the device, server and enterprise levels without building in means for government monitoring". They noted that "if law enforcement and intelligence organisations face a future without assured access to encrypted communications, they will develop technologies and techniques to meet their legitimate mission goals" (McConnell, Chertoff and Lynn, 2015[11]).

In 2018, the Australian Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (TOLA Act) was the first legislation passed in an OECD Member country since the adoption of the Guidelines that introduced some degree of regulation over cryptography.

- *Phase 3: content scanning against child sexual exploitation and abuse material.*

To a certain extent, the going dark debate against a terrorism backdrop continues to unfold today, and law enforcement's push for the regulation of cryptography has never stopped[2]. However, an additional thread was added more recently with the fight against child sexual exploitation and abuse material. Several draft laws have been proposed to address issues related to such illegal content, particularly child sexual exploitation and abuse (CSEA) material online. They include the US *Eliminating Abusive and Rampant Neglect of Interactive Technologies* Act (EARN IT), introduced in 2020, 2022 and 2023 (US Congress, 2023[12]), the UK's *Online Safety Bill* (UK Parliament, 2022[13]), and the European Union's *Regulation laying down rules to prevent and combat child sexual abuse* (European Parliament, 2023[14]). These draft laws have in common *i)* the establishment of some form of obligation by online service providers to use technology to identify CSEA material on public or private parts of their service, including user devices; and *ii)* very strong negative reactions from many business, civil society, and technical community stakeholders on the ground that such technical solutions would break end-to-end encryption with wide consequences for users' privacy and security, the functioning of the Internet, and national security (CDT, 2023[15]; Campbell et al., 2022[16]; Save Online Speech Coalition, n.d.[17]; Global Encryption Coalition, 2022[18]; Global Encryption Coalition, 2022[19]). As an illustration, Box 2 summarises the goal of the EARN-IT Act and the main arguments from its non-governmental opponents.

Box 2. The US EARN-IT Act and its detractors

The EARN-IT Act is a draft law put before the US Congress in 2020, 2022 and 2023. It would establish a National Commission on Online Child Sexual Exploitation Prevention, which would develop best practices for interactive online services providers (e.g., Facebook and Twitter) to prevent, reduce, and respond to the online sexual exploitation of children. Additionally, the bill would limit the liability protections currently enjoyed by interactive online service providers with respect to claims alleging violations of child sexual exploitation and abuse laws.

According to a coalition of 132 civil society organisations led by the Centre for Democracy and Technology (CDT), the Act "would make it harder for law enforcement to protect children and result in online censorship that will disproportionately impact marginalized communities. It will also jeopardise access to encrypted services, undermining a critical foundation of security, confidentiality, and safety on the internet".

In a joint analysis of the potential impact of the bill, the Internet Society and CDT warned that the Act would threaten companies' ability to use and offer end-to-end encryption by putting their liability immunity at risk if they do not proactively monitor and filter for illegal user content. It would directly threaten entities that supply or support encrypted services, such as online service providers and Internet intermediaries, who would have to choose to weaken security by providing a backdoor or "exceptional access" to end-to-end encrypted content for governments; or bypass end-to-end encryption entirely by allowing access to and surveillance of content before or after the encryption process, through methods such as client-side scanning or storing a copy of every message sent; or not offering end-to-end encrypted services at all.

Furthermore, it would also create risks for Internet infrastructure intermediaries – such as Internet Service Providers and others who could be made civilly liable for delivering illegal traffic even without any knowledge about the contents of the traffic, and any direct involvement in providing encrypted services.

According to this analysis, the Act poses an "existential threat to the Internet" by interfering with critical properties the Internet needs to exist, and undermines most enablers that the Internet needs to thrive as an open, globally connected, secure and trustworthy resource for all. Instead of tackling nefarious

actors who would continue to encrypt their communications on their own even if the communication service they use does not do it for them, the Act would undermine security and confidentiality online, putting billions of people worldwide at greater risk of harm from those seeking to exploit private data for harm, and jeopardising national security and virtually every sector of the economy that relies on a strong Internet. As of September 2023, an online petition against the Act had collected over 624 000 signatures[3].

Sources : Campbell, N. et al. (2022), *How the US EARN IT Act Threatens Security, Confidentiality, and Safety Online*, www.internetsociety.org/resources/2022/internet-impact-brief-how-the-us-earn-it-act-threatens-security-confidentiality-and-safety-online; CDT (2023), CDT Leads Broad Civil Society Coalition Urging Senate to Drop EARN IT Act, https://cdt.org/insights/cdt-leads-broad-civil-society-coalition-urging-senate-to-drop-earn-it-act/; US Congress (2023), S. 1207 - A Bill to establish a National Commission on Online Child Sexual Exploitation, www.congress.gov/118/bills/s1207/BILLS-118s1207is.pdf.

2 What is cryptography?

This section provides basic information about cryptography for policy makers. Depending on the algorithm, cryptography can provide confidentiality, integrity, authenticity, and non-repudiation. The two most widespread cryptosystems are symmetric and asymmetric cryptography. Even if we do not notice it, cryptography is literally everywhere in the digital era. End-to-end cryptography is becoming the norm for certain types of communication such as instant messaging. Lastly, cryptography is not magic: it is possible to break it, in particular when it is not sufficiently well implemented.

Cryptography provides confidentiality, integrity, authenticity and non-repudiation

From antiquity to modern times, diplomats, soldiers, spies, and traders have used cryptographic techniques to protect written secrets and to communicate in a way that replicates the confidentiality they would have enjoyed if they had been speaking face to face. Such cryptographic techniques transform written information into a form that unauthorised parties cannot understand. This is still what cryptography is well-known for today, a means to ensure the confidentiality of information, i.e. keeping information secret, or concealing it from prying eyes, during a communication ("in transit") and when the information is stored, archived or filed ("at rest"). The Greek etymology of the term cryptography, literally "secret writing" (*kryptos*, secret or hidden, and *graphia*, writing), reflects this initial usage.

However, with the emergence of information technologies and the digitisation of data after the second world war, cryptography has also evolved to:

- Ensure the *integrity* of data, i.e. prevent data from being modified or altered in an unauthorised manner without such modifications or alterations being detected;
- *Authenticate* an identity attached to data (e.g. sender, author);
- Enable *non-repudiation*, i.e. prevent an individual or entity from denying its involvement with data, such as being its author or sender.

In other words, *cryptography* refers to practices, means, methods, and techniques that transform data to provide confidentiality, integrity, authentication, and non-repudiation, or a mix of those. In contrast, *cryptology* is the broader science of secret messages, encompassing both cryptography and other disciplines such as the science of breaking cryptography, also known as *cryptanalysis*. Cryptography encompasses *encryption* and *decryption*. Encryption is the implementation of a cryptographic algorithm (*cipher*[4]) to transform intelligible data (*plaintext*) into unintelligible data (*ciphertext*). Decryption is the algorithm that reverts it to its intelligible form. In cryptographic jargon: a cryptographic method uses a cipher to turn plaintext into ciphertext, and vice-versa.

Symmetric and asymmetric cryptography are the two main cryptosystems

There is a wide variety of cryptographic methods, also known as *cryptosystems*, with different strengths and weaknesses. This diversity allows users to choose the most appropriate method for their needs, context, resources, and other constraints.

Cryptographic methods involve techniques rooted in mathematics. This section briefly introduces the two most common families of cryptographic methods, symmetric and asymmetric cryptography. Other methods include homomorphic cryptography, introduced below, as well as zero-knowledge proofs, secure-multi-party computation (SMPC), lattice-based cryptography, secret sharing, obfuscation, etc.

Both symmetric and asymmetric cryptography use a simple string of bits (zeros and ones) called a cryptographic *key,* as an input variable provided to a cryptographic algorithm to transform data in a unique manner. The size and security of the key are critical conditions for the security of the entire cryptographic process, although not the only ones.

With *symmetric cryptography*, the data is encrypted and decrypted using the same secret key, just like the same key can both lock and unlock the same door. Symmetric cryptography is reversible: decrypting ciphertext simply requires reversing the encryption process using a copy of the same key. The secret key is sometimes called a shared secret because the sending and receiving parties in a communication have to share it. Symmetric encryption ensures the confidentiality of information in transit or at rest but does not ensure its integrity, authenticity and non-repudiation. Symmetric cryptography is also called secret key cryptography. It has been used since antiquity in many parts of the world.

With *asymmetric cryptography*, a pair of keys mathematically related ensures the confidentiality, integrity, authenticity and non-repudiation of information in transit or at rest. One key is “public”, i.e. not secret, and the other is private, i.e. must be kept secret. Asymmetric cryptography is also called public key cryptography. It was proposed as a concept in 1976 by Whitfield Diffie and Martin Hellman prior to Ronald Rivest, Adi Shamir and Len Adleman further developing it into the well-known and widely used RSA algorithm the following year. However, a similar system was developed secretly in 1973 by the British signals intelligence agency and declassified in 1997.[5]

Symmetric and asymmetric cryptography are complementary and generally serve different purposes in different contexts. Among their differences, asymmetric cryptography is more complex technically, organisationally, and operationally than symmetric cryptography. To provide confidentiality, the data is encrypted by the sender with the receiver’s public key and decrypted by the receiver with her private key. To provide authenticity and integrity of data such as a message or file, the sender (or owner if the data is at rest) generates a *digital signature* by encrypting with her private key a mathematically generated unique digital code based on the message and appending the results, called a hash[6] value, to the message before sending it to the recipient(s)[7]. The recipient(s) can then decrypt the digital signature with the sender’s public key. If the public key decrypts the digital signature, they can trust the integrity and authenticity of the data. Otherwise, it is a proof that the authenticity and integrity are broken. The digital signature also ensures that the sending party cannot deny having “signed” the message (i.e. non-repudiation) because the encryption process to digitally sign the data provides a very high level of assurance that it was really performed by whomever holds the private key. The confidence stems from the mathematical properties of the key pair and encryption/decryption algorithms, which make it quasi-impossible to tamper with if there are no exploitable weaknesses in the implementation of the cryptosystem.

There is no 100% risk-free cryptographic method. All cryptographic methods come with pros and cons, and when a method seems to eliminate a weakness compared to another one, it often shifts the risk elsewhere. It is therefore essential to analyse and understand the risk related to the use of a particular cryptographic method in each use case prior to choosing a cryptographic method, and to treat the risk associated with the chosen method to reduce it to an acceptable level (OECD, 2022[2]).

For example, with symmetric cryptography, two parties wishing to exchange a confidential message need to first exchange the secret key, a process through which the secret key could be intercepted by a third party. This is a weakness if the two parties do not have a sufficiently secure channel to exchange the secret key. In contrast, with asymmetric cryptography, the receiver does not need to share the private key with anyone, eliminating the risk of it being intercepted. However, the higher complexity of asymmetric

cryptography can introduce new weaknesses and therefore opportunities for potential adversaries (or, in other words, increase the "attack surface").

A good example of such additional complexity is the need for a *Public Key Infrastructure* (PKI) to support asymmetric cryptography. To send an encrypted message to Alice, Bob first needs to access Alice's public key, which is easy because that public key is not secret. But how can Bob be certain that Alice's public key has not been generated by somebody else pretending to be Alice? The solution is to require a *digital certificate* from Alice, i.e. a file that contains her public key digitally (cryptographically), signed by one or more trusted third party(ies), thereby confirming that the public key is really bound to Alice[8]. While this may sound easy in principle, in practice it involves many additional components that all have to be trusted by participants, such as a *registration authority* to verify Alice's identity, a *certification authority* to generate the certificate, a *repository* to store digital certificates, a *certificate revocation list* to ensure that revoked certificates are not used to sign or encrypt messages, etc. Regardless of the theoretical perfection of the cryptographic technique, adversaries will have as many opportunities for exploitation as there are implementation weaknesses in any of the PKI components. Therefore, ensuring the appropriate level of security for all the technologies, people and processes required by these components is significantly more complex and expensive than implementing symmetric cryptography.

Therefore, a systematic and comprehensive risk analysis of both the cryptographic technique and how it would be implemented in each case is essential to choose the most appropriate one, and the implementation of a systematic and comprehensive risk management cycle is also crucial when cryptography is deployed and operated in practice. Naturally, participants also need to consider other factors such as cost, usability, and technical feasibility.

Asymmetric cryptography is well-suited for encrypting small amounts of data because its performance drops in proportion to the amount of data. This is why symmetric and asymmetric cryptography are often used in combination, typically in the key establishment (or agreement) process whereby two parties use asymmetric cryptography to agree on a symmetric key that they will then use during their communication. This is typically the case with hybrid protocols such as Transport Layer Security (TLS). Key establishment is further discussed below.

These two families of cryptosystems can use a variety of techniques and algorithms, overall offering users a large choice of how cryptographic methods can be implemented. Techniques include encryption standards such as Data Encryption Standard (DES) and Advanced Encryption Standard (AES); hash functions algorithms (see above) such as MD5 and SHA-2; cryptographic protocols to define the rules and procedures for secure communications such as SSL/TLS (for internet communications), IPsec (for IP network layer security), S/MIME (for email), PGP (for email and files), and SSH (for remote access and file transfer); digital signatures algorithms such as RSA, DSA, and ECDSA; and several types of random number generators. While many of these algorithms are in the public domain, some others are not.

While some cryptosystem implementations can be entirely based on software, others can include hardware devices or components. For example, Hardware Security Modules (HSMs) provide tamper resistant storage for cryptographic keys, accelerated cryptographic computation and other features; Trusted Platform Modules (TPMs) provide secure cryptographic functions embedded in a dedicated chip; smart cards can embed cryptographic capabilities and be used for secure storage and processing of keys. Lastly, some cryptosystems use a combination of software and hardware components.

Cryptography is a vital foundation of the digital world

Before the advent of modern communication technologies, cryptography was primarily used to communicate confidential diplomatic, intelligence, military, and other State secrets. A market for cryptography started to emerge with the invention of wired and wireless communications in the 19th century.

Businesses and governments increasingly used radio and wired technologies to support their activities and needed to address the growing risk of interception by adversaries or competitors. The market expanded further after World War II as computer technologies multiplied the possibilities to store and communicate confidential information. With the rise of the Internet in the 1990s, the availability of sufficiently robust cryptography became a key enabler for electronic commerce and electronic government, as well as for businesses, governments and individuals to use the network for private (i.e. confidential) communications. Furthermore, cryptography was also at the core of electronic authentication, for example to protect the confidentiality of passwords and other credentials, but also to authenticate people and documents through digital signature. After its deregulation (see Introduction), cryptography became a foundational security technology for digital communications, storage, and authentication, enabling the migration of offline economic and social activities online, and considerable innovation in the digital realm.

Whether users realise it or not, cryptography is everywhere in the digital world, and it is an enabler for all valuable uses of digital technologies. It provides a fundamental building block for the digital security of business, governmental and individual uses of digital technologies, as well as for the protection of fundamental rights, including privacy and data protection. Cryptography allows stakeholders to exercise in remote communications the right to confidential exchanges that is granted to them in face-to-face communications.

Cryptography is one of the essential components of secure digital systems, from the smallest (i.e. a person's smartphone) to the largest ones (i.e. a government network or a business's global communication infrastructure). It is critical for security and privacy at all levels of the implementation of digital technologies: hardware, software, networks, and data. It is used at all levels of digital infrastructures: application (e.g. users' programmes), operating system (e.g. Windows, Android, iOS, Linux), network (e.g. network security protocols rely on cryptography), and hardware levels (e.g. in microprocessors). For example, it is key to:

- Web security, with the browser padlock showing that cryptographic protocols are in use;
- Authentication processes of persons and entities, e.g. for password communication and storage, regardless of the application they support and their technology (e.g. smartcard); as well as authentication of documents, with digital signature and time stamping techniques;
- The privacy and security of instant messaging through end-to-end cryptographic techniques used by popular applications such as WhatsApp, Signal, Telegram, and Threema;
- Wireless communications such as Wi-Fi, Bluetooth, etc;
- Secure storage in local (i.e. hard drive, flash memory, SD cards) and remote (e.g. cloud) drives and in databases;
- Virtual private networks (VPNs), which enable teleworking and other remote applications; and
- Smart cards, wherever they are used, such as sim cards in phones and payment cards.

Cryptography is also at the core of distributed ledger technologies (e.g. blockchain applications).

End-to-end encryption

In the early days of instant messaging, data was typically not protected seamlessly from one end of the communication to the other. Instead, cryptography protected it in transit between the source machine and the intermediary server hosted by the instant messaging service provider, where it was decrypted and stored in plaintext, prior to being re-encrypted and sent to the destination where the recipient machine would decrypt it. In some implementations, the service provider kept the data encrypted also when at rest on its servers. However, in both cases, the service provider would generate and therefore know the secret keys. The communicating parties had to trust that this intermediary would keep the keys secret (i.e. prevent leakage), respecting the confidentiality and integrity of the data in all circumstances (i.e. not access

plaintext for purposes other than delivering the service), and implement sufficiently robust security on its system to prevent unauthorised parties such as malicious actors from accessing the keys or the plaintext.

Following controversies over the roles and responsibilities of intermediaries (see Introduction), some of the major providers of instant messaging as well as audio and video communications services adopted end-to-end encryption (E2EE) to provide confidentiality, integrity, and authenticity between ends.

The term E2EE is somewhat incomplete because it does not simply mean that the communication is encrypted from end to end, but also that "confidentiality is broken if content *can be* decrypted at any intermediate point" (Knodel et al., 2023[20]). In an instant messaging context, E2EE "conceals communications between one user's instant messaging application through any intermediate devices and servers all the way to the recipient's instant messaging application" (Gillmor, ACLU and Oever, 2015[21]) in a manner that prevents any intermediate device from breaching the confidentiality of the data. In practice, it means that the secret keys are generated and can be accessed only by the communicating parties. This ensures that the data can be decrypted only at its destination and prevents service providers and other third parties from decrypting the data during its journey, including when at rest on the providers' servers. Services that process the information exchanged by users for marketing, profiling, ad targeting, and other purposes cannot implement real E2EE without breaking their business model. In most cases, however, they can still use metadata, such as who is communicating with whom, when and for how long, for profiling purposes.

In cloud storage scenarios such as network drive services (e.g. Dropbox, Microsoft OneDrive or Google Drive), the data is typically protected by cryptographic protocols when transiting to and from the cloud, but depending on the offer, it may not be encrypted while at rest on the provider's storage system, or if it is, the cloud service provider often owns the secret key. E2EE can address the security issues in this context, too.

Although many communication and storage providers claim to offer E2EE, it is often incomplete end-to-end encryption because the service provider has access to the secret keys. However, with increased security and privacy awareness among users, communication and social media platforms such as Facebook are adding end-to-end encrypted features on top of their incompletely encrypted end-to-end encrypted existing services (Meta, 2021[22]).

E2EE introduces more complexity, in particular in contexts where several users are involved. That is the case, for example, in group communications or when files stored in network drives can be shared with multiple users.

As explained below, homomorphic cryptography has the potential to extend the definition of E2EE.

Breaking cryptography

The easiest and often underestimated way to break cryptography is by exploiting weaknesses in users' behavior, typically deceiving users into revealing their key or behaving in a manner that creates a vulnerability in the system. In addition to such social engineering techniques, there are several other approaches to breaking cryptography:

- *Brute-force attack*: trying every possible key until the correct one is found. This approach requires a combination of computing power and time: the more power, the less time is needed to break the key. It can be countered by increasing the length of the key, forcing the attacker to consume more power and spend more time. For example, a 256-bit AES key would require testing 2^{128} possibilities (assuming half the number of possible keys would have to be tested in average), i.e. 3.402×10^{38}, that is, 3.4 followed by 38 zeros. This is a rather difficult number to comprehend. Assuming one

possessed the capacity to test 10 billion keys per second, it would take 539 514 153 540 301 000 000 years to do it[9].

- *Cryptanalysis*: analysing the encryption algorithm to identify weaknesses that can be exploited to decrypt the data, either to attack it or to assess its robustness against potential attackers. Cryptanalysis requires extensive knowledge in mathematics and computer science.
- *Side-channel attack*: exploiting information leaked from a physical cryptosystem. Characteristics that could be exploited in a side-channel attack include timing, power consumption, as well as electromagnetic and acoustic emissions (Grassi, Garcia and Fenton, 2017[23]). This type of attack attempts to gather information from measuring or exploiting the indirect effects of a system instead of targeting the computer code (programme) directly. For example, the attacker would observe the power and electromagnetic variations of a cryptographic system during operation to learn enough information to break the cryptosystem.

As suggested above, effective implementation of cryptography is difficult. Cryptography is a complex science and its implementation in practice requires a very strict and systematic approach with acute attention to details. Potential attackers will look for and try to exploit weaknesses in the design and/or in the implementation of a cryptographic system, including with respect to technical (e.g. bugs, misconfigurations), organisational, and human aspects involved in the entire cryptosystem. In response, defenders need a comprehensive and systematic risk management approach to choosing a cryptographic method and implementing it, taking into account dependencies upon underlying technical components (e.g. operating system, applications, libraries, etc.) as well as people and processes (cf. below).

Furthermore, instead of spending significant resources on breaking robust cryptography, attackers can choose among a variety of attack techniques to breach parts of the cryptosystem other than its encryption component, such as by gaining access to secret keys without directly tampering with encryption *per se*. This could be done, for example, by exploiting vulnerabilities in the information system where the secret keys are stored and processed, or by using social engineering techniques. For example, in 2011, attackers successfully targeted RSA, the well-known security firm founded by the co-inventors of asymmetric cryptography. Some RSA employees opened a malicious email attachment containing malware that allowed the attackers to gain a foothold in the company's information system and explore it to eventually access the cryptographic keys used to generate RSA's SecureID token values for the company's two-factor authentication product. The incident eroded the company's reputation, generated business and financial losses, and had a wide impact on the security of its customers who could no longer trust their SecureID tokens.

In addition, attackers could compromise one or more components of the infrastructure required to support the cryptographic method, typically the public key infrastructure. For example, malicious actors can compromise a certificate authority to generate valid certificates with which they would intercept encrypted traffic or digitally sign malware code that will therefore be trusted by victims' machines, thereby avoiding detection by security software. For example, in 2011 attackers successfully compromised the Dutch DigiNotar certificate authority and issued dozens of fraudulent digital certificates, affecting the Dutch government as well as thousands of people outside the government. The company went bankrupt shortly after the event. Comodo, a US-based certificate authority, was also affected by an attack in 2011[10].

There is no doubt that all certificate authorities are under constant pressure from offensive actors attempting to compromise their systems and that some have weaknesses or insufficient security practices. Examples show that such weaknesses sometimes i) come from the company's mismanagement, as when fraudulent certificates for Google domain names issued by TurkTrust were found in 2013 (Fisher, 2013[24]); ii) are sometimes rapidly addressed, e.g. the security vulnerability detected in StartSSL's domain validation process that attackers could have abused to issue certificates for domains they did not own in 2016 (Security Week, 2016[25]); iii) are detected by the company itself when carrying out a security audit, as GoDaddy did in 2018 when, in less than three days, it detected and fixed a code vulnerability that could

have allowed an attacker to bypass its validation controls (Tayer, 2018[26]). In other cases, incidents have created enough suspicion for key actors to stop trusting the authority's digital certificates, as Microsoft did with StartCom/woSign certificates in 2017 (Microsoft, 2017[27]). Lastly, there are numerous reports of sophisticated attacks targeting certificate authorities, although their names are often not revealed, such as the Billbug attack detected by Symantec in 2022 that compromised an Asian certificate authority as part of a broader campaign targeting multiple Asian countries (Symantec, 2022[28]). Compromising the digital certificate of a supply chain actor can be extremely fruitful for attackers as it can allow the exploitation of their customers' systems. For example, malicious actors behind the infamous SolarWinds attack in 2021 accessed the cloud-based email management company Mimecast's production environment as well as a Mimecast-issued certificate used by some Mimecast customers to authenticate various Microsoft 365 Exchange web services (Goodin, 2021[29]).

Lastly, attackers could also compromise the endpoints to intercept the information before its encryption or after its decryption, for example by planting software that automatically captures and sends out users' screenshots when the confidential document or conversation is displayed on the user's screen. In such cases, the confidential information is compromised but the core cryptographic method is not.

These examples show that trust in a cryptographic method needs to encompass the core cryptographic algorithms as well as all the other components upon which their implementation relies, such as the cryptographic infrastructure (e.g. PKI), the operating system, applications, time source, random number generator, hardware and network components, etc. The security of each component of this broader cryptosystem includes aspects related to people, processes, and technologies. Lastly, the trustworthiness, integrity and verifiability of each component's supply chain is also of utmost importance.

3 Key trends in cryptography: towards future disruptions?

Throughout history, cryptographers have continuously researched new cryptographic methods and techniques to improve on the cryptographic *status quo* of their time and to respond to new threats. The last disruptive cryptographic innovation was probably the discovery of asymmetric cryptography in the 1970s, widely adopted 25 years later with the advent of the Internet. This section discusses two areas of research that could disrupt current cryptography with tremendous potential economic and social consequences: homomorphic encryption and quantum information technologies. It also includes an overview of approaches and techniques proposed to overcome the law enforcement challenge created by the wide adoption of cryptography.

Homomorphic Encryption: the "Holy Grail" of cryptography?

What is homomorphic encryption?

It is not possible to process encrypted data without decrypting it first with the secret key. While this protects the confidentiality of the data, it can also be viewed as a limitation. For example, a company that outsources the storage of encrypted data in an untrusted cloud environment is currently deterred from also outsourcing computation in that environment. To process the data, the company would have to decrypt the data first, either by sharing the secret key with the untrusted cloud system and increasing the risk of confidentiality breach, or by copying the data to a trusted environment (typically on-premises) prior to decrypting and processing it, thereby increasing the time, complexity, and cost, as well as the risk of exposure when the data is no longer encrypted. Even when using E2EE, the data is protected in transit and storage but still needs to be decrypted to be processed, potentially exposing it to prying eyes at that moment.

Homomorphic encryption (HE) overcomes this issue, opening a whole new range of possibilities. It is a cryptographic method allowing certain computations to be performed on encrypted data without the need to decrypt it first, and without requiring access to the secret key. The result of such computations remains in encrypted form and can at a later point be revealed by the owner of the secret key (Homomorphic Encryption Standardization, n.d.[30]).

Encryption can be partially homomorphic (PHE), somewhat homomorphic (SHE) or fully homomorphic (FHE), with some variations in between. The difference between these types of HE is in the extent to which additions and multiplications, which are at the core of computer processing, can be executed over the encrypted data. PHE enables only a single type of operation on the ciphertext, addition or multiplication, but for an unlimited number of times. SHE enables both addition and multiplication operations, but only for a limited number of times (Munjal and Bhatia, 2022[31]). Importantly, the available operations are predetermined by the way the data is encrypted, which means that if PHE or SHE is implemented to perform one set of operations on a dataset, it is not possible to request other operations from the same dataset (ISOC, 2023[32]). Lastly, FHE aims to enable any operations to be applied to encrypted data in unconstrained combinations. This means that with FHE, programs can run directly on encrypted data,

eliminating risk of data leakage during or after computation, as the final output is only decrypted when it returns to the user's device (Gorantala, Springer and Gipson, 2023[33]).

What could FHE be used for?

In principle, FHE has a wide variety of potential applications. For example, both storage and computation of sensitive data could take place in an untrusted environment, typically a cloud platform, significantly reducing the risk of data breach, as malicious actors attacking the cloud provider's system would be as blind as the provider itself with respect to the homomorphically encrypted data and processing outputs. Furthermore, with FHE, the cloud platform's location would no longer be a relevant criterion for choosing a cloud provider because the risk of governments or other actors leveraging cloud providers under their jurisdiction for monitoring purposes would be significantly reduced (Paillier, 2020[34]), at least as long as no additional obligations are imposed on cloud providers such as the custody of FHE keys.

With FHE, third parties could perform analytics without threatening the confidentiality of sensitive data in areas such as health care (e.g. applying machine learning to genome data for medical research), finance (e.g. analysing transaction records), and law enforcement (e.g. detecting tax evasion, preventing crime, carrying out investigations) (Koerner, 2021[35]). They could also query if specific data exists in a data store without revealing information about the contents of the query or the data store (Creeger, 2022[36]). FHE could enable data sharing for machine learning purposes in areas such as finance that were once considered impossible or highly undesirable due to a lack of trust, including with respect to the possibility of data breaches (Masters and Hunt, 2019[37]). Participants could use FHE to analyse confidential data from multiple organisations without these organisations having to share the data and the results from the computations among themselves or anybody else (see for example the SCRAM platform developed at the Massachusetts Institute of Technology (MIT) for a multi-user application oriented towards cybersecurity (MIT, 2021[38])).

FHE can be viewed as a powerful privacy-enhancing technology (PET) (OECD, 2023[39]). It could bring a considerable amount of privacy protection to everyday applications such as GPS navigation, biometric identification, or voice assistants. With FHE, users would not have to share any personal data with the providers of location, identification, voice assistant or other services but could still benefit from their services (Zama, n.d.[40]). HE enthusiasts even envision a next generation FHE-enabled HTTP where everything, including data processing, is encrypted by default (Zama, n.d.[40]).

FHE could also be viewed as a building block for a Zero Trust environment, as it allows computation even if the environment is known to be compromised by an attacker (IBM, 2021[41]). Some stakeholders argue that the reason data is still being compromised by attackers despite encryption being used in transit is that it is not encrypted during processing (Zama, n.d.[40]).

The implementation of FHE would raise wide-ranging potential legal questions. For example, should homomorphically encrypted personal data be considered anonymous, pseudonymous or personal and, depending on the response, what would the consequences with respect to data controllers' regulatory requirements be when using HE? For example, would a data subject's consent still be required prior to FHE processing of their data (Koerner, 2021[42])? While some stakeholders view HE as a means to reduce compliance requirements or the risk of non-compliance, more work needs to be done to confirm whether this is really the case and, if so, under which conditions.

The enormous potential for new applications explains in part why experts have called FHE the "Holy Grail of cryptography" (Tourky, ElKawkagy and Keshk, 2016[43]) and "a technology that will change the world" (Paillier, 2020[34]).

What are the main challenges and limitations of FHE?

At this point however, the HE Holy Grail remains more of a dream than a reality. This is because HE and FHE have several important limitations.

While HE has made considerable progress over the last four decades, it is still evolving and FHE is not yet a fully mature technology. The basic concept for HE was first proposed in 1978 by Ron Rivest, Len Adleman, and Michael Dertouzos. It took 30 years for the first fully homomorphic encryption scheme to be developed by Craig Gentry at IBM in 2008. Since then, four generations of improved FHE schemes have been developed, each with their pros and cons in terms of efficiency and security (van den Nieuwenhoff, 2021[44]).

First, HE is very computationally intensive. It is slower, less efficient, and more energy-consuming than processing the same data without encryption (i.e. "in clear"), with variations depending on the technique used. FHE requires enormous computation time to perform even simple operations. A computation that would take a millisecond to complete on a standard laptop would take weeks to compute on a conventional server running FHE today, according to the FHE programme manager at the US Defense Advanced Research Project Agency (DARPA) (DARPA, 2021[45]). Current FHE processing can be from 1 000 to 1 million times slower than the equivalent plaintext processing (Mattsson, 2021[46]). With an overhead latency of several orders of magnitude, it can be suitable in certain business scenarios but not for real-time computation needs. However, some companies are investing in FHE-designed acceleration chips to overcome this issue (Arghire, 2022[47]) and the DPRIVE DARPA project, developed with Intel and Microsoft, aims at developing a hardware accelerator for FHE that could be implemented in Microsoft's cloud ecosystem (Intel, 2021[48]; DARPA, 2021[45]). While such innovation would improve performance, its impact on the cost of an FHE solution is yet to be determined.

HE is also limited in multi-user environments such as outsourced processing. HE is designed for a single user because HE schemes involve a single secret key. This means that additional users would need to share the secret key, which may not be suitable in certain scenarios, such as when different users come from different organisations, or when the secret key needs to be strictly controlled. Multi-user HE has been developed to address this issue but, because it uses several keys, the ciphertext size grows according to the number of users, which results in increasing both computation and communication cost in proportion to the number of users (Park, 2021[49]). This limitation reduces the potential for some scenarios, such as government analysis of financial data for detecting tax evasion.

Second, FHE can raise correctness challenges because it generates noise that can accumulate over time and distort the results. Sophisticated or repeated uses of FHE on the same data may require advanced mathematical computations of the ciphertext that may affect the accuracy of the results (Yang et al., 2023[50]). More generally, correctness challenges related to noise generation are the main difficulty of moving from PHE to FHE, where FHE requires additional techniques to manage the noise, increasing the efficiency challenge. Furthermore, implementing FHE or other HE computations in a cloud environment does not provide guarantees for clients regarding the accuracy of computations carried out (Fernàndez-València, 2022[51]). In other words, they cannot easily verify that the output is correct.

Third, FHE is potentially vulnerable to many types of attacks ranging from side-channel to key recovery attacks (Yang et al., 2023[50]). For example, the use of FHE in a cloud environment is currently vulnerable to an attack that would substitute a given ciphertext with another valid ciphertext or a given computation query with another valid query (Awadallah, Samsudin and Almazrooie, 2021[52]).

Fourth, while an increasing number of HE software libraries and tools are available and being developed by key industry and research players, HE is still neither beginner friendly, nor user-friendly for programmers and is very difficult to understand for a person who is not a cryptographer (van den Nieuwenhoff, 2021[44]). Some stakeholders are working to improve HE usability, such as Intel which developed a Homomorphic Encryption Toolkit to accelerate HE adoption (Intel, n.d.[53]).

Lastly, even for a cryptographic method initially formulated four decades ago, it is fair to say that HE standardisation is on its way but still at an early stage. The availability of technical standards related to a cryptographic method generally provides a fair reflection of that method's maturity. Standards increase confidence, provide interoperability and allow stakeholders to develop tools that foster adoption. A cryptographic method without a widely recognised standard is unlikely to affect the technology landscape. In 2019 the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC) published a standard addressing some mechanisms for homomorphic encryption and including a "general model" for HE (ISO/IEC, 2049[54]). The US National Institute of Standards and Technology (NIST) addresses HE as part of its Privacy-Enhancing Cryptography project (NIST, 2023[55]). FHE is also the subject of a draft Technical Report on "FHE-based data collaboration in machine learning" under development in ITU-T Study Group 17 on security (ITU, 2023[56]; ITU, 2022[57]). On the industry side, an open consortium of industry, government and academia called HomomorphicEncryption.org has been working to standardise HE since 2017, released a standard in 2018 (Albrecht et al., 2018[58]), and holds regular workshops on this issue.

Overall, HE and FHE hold promise for significant change in the security landscape with important economic repercussions across all sectors. However, while some HE applications are already in place, FHE does not seem to be ready for wide adoption yet. According to well-known cryptographer Pascal Pallier, "fully homomorphic encryption is today where deep learning was 10 years ago" (Paillier, 2020[34]). However, we do not know how much time will be necessary for FHE to reach the inflexion point after which wide and rapid adoption would follow.

Quantum information technologies: a disruptive innovation that presents both opportunities and dangers

Mature quantum information technologies will have disruptive potential in many areas (Barker, Polk and Souppaya, 2021[59]). A key issue is that, at least in theory, a mature quantum computer could easily break some encryption methods that are widely used today. However, recent progress in quantum computing research is stimulating cryptographic research and innovation, particularly the development of algorithms that could resist attacks powered by a quantum computer. Furthermore, research on quantum technologies creates opportunities for new cryptographic approaches based on the laws of quantum physics ("quantum cryptography" and "quantum key distribution") rather than mathematics. This section introduces quantum information technologies, discusses how they challenge current cryptosystems, introduces approaches to address these challenges ("quantum resistant cryptography"), and explores the opportunities that quantum computing raises for cryptography.

What is quantum computing?

This section introduces quantum computing, which is expected to allow complex computations on a massive scale that is beyond the reach of traditional computing. It also briefly introduces quantum communication[11].

Quantum technologies are based upon quantum mechanics, the subfield of physics that describes the behavior of very small particles. Among the quantum technologies is quantum computing, which is a new computing paradigm (Grumbling and Horowitz, 2019[60]). Quantum computing and more broadly quantum information technologies aim to use the properties of nature at atomic scales to accomplish tasks that are not achievable with existing technologies (US Government Accountability Office, 2021[61]). Initially proposed in 1982 by Nobel Laureate Richard Feynman as a tool to simulate quantum systems, quantum computing has become an established interdisciplinary research area between physics, computer science and engineering involving universities, research centres and companies worldwide (BSI, 2021[62]).

In traditional computers, an intangible binary digit (*bit*) reflects the state of a tangible (i.e. physical) transistor similar to a tiny on-off switch. Therefore, the information is binary, i.e. either a 0 or a 1 for each transistor. In quantum computers, information is encoded in *qubits* instead of *bits*. A qubit represents a property called "spin," which is the intrinsic angular momentum of an electron, akin to a tiny compass needle that points either up or down. When they manipulate that needle to encode information into the electrons, researchers can leverage the possibility of quantum systems to exist in two or more states simultaneously (superposition) to encode the information as 0, 1, or a combination of 0 and 1 at the same time (Nellis, 2022[63])[12]. Quantum computers leverage superposition to multiply processing power. They also leverage the possibility to intrinsically link qubits (entanglement) so that when one qubit is acted upon, such as through measurement, it can reveal information about the other linked qubits regardless of distance. Leveraging entanglement allows quantum computers to perform parallel computations on entangled qubits (US Government Accountability Office, 2021[61]).

Quantum computers are expected to demonstrate a gigantic extension of both processing power and speed. A traditional computer with N bits will be able to represent 2^N states. For example, a 1-bit computer can represent 2^1 states (0 or 1), a 2-bit computer can represent 2^2 states (00, 11, 01, 10), and so on. A quantum computer with N qubits will be able to represent 2^N quantum states *simultaneously*. While the number of possible states in a traditional computer doubles with each additional bit and therefore scales linearly with the number of bits, the number of possible states in a quantum computer increases exponentially with the addition of each qubit (Congressional Research Service, 2022[64]). Therefore, in theory, quantum computers' processing power could outperform the power of traditional computers by several orders of magnitude and make it possible to solve certain problems much faster, even problems that traditional computers cannot solve within a reasonable timeframe. This is the so-called "quantum supremacy" or "quantum advantage" (Preskill, 2012[65]). As an illustration of the processing power difference between the two technologies, it would take about 18 quadrillion bits (i.e. 2^{54} bits) of traditional memory to model a quantum computer with just 54 qubits. Only one traditional supercomputer on the planet, the IBM *Summit*, had such a capacity as of 2019. Modelling a 72-qubit quantum computer would require 2^{72} bits, which would require stacking 262 000 Summit-type supercomputers! Modelling a 100-qubit quantum computer would require more bits than there are atoms on our planet, and a 280-qubit computer would require more bits than there are atoms in the known universe (Sedik, Malaika and Gorban, 2021[66]).

With entirely new quantum algorithms leveraging quantum properties, quantum computers can also considerably reduce the time needed to perform specific tasks. For example, the best-known quantum algorithms (Grover and Shor) yield a polynomial speedup and an exponential speedup. A polynomial speedup is when a quantum computer solves a problem in time T (say, 1 000 steps) while a traditional computer needs time T^2 (i.e. 1 000 000 steps) to solve the same problem. An exponential speedup is when a quantum computer takes time T (say 100) while a traditional computer takes time 2^T (i.e. 2^{100}), which is a 31 digit number (Sedik, Malaika and Gorban, 2021[66]).

Such figures are purely theoretical, though, because building a quantum computer with sufficient computing power to perform useful tasks is extremely complex. Consequently, despite enthusiastic announcements and optimistic forecasts by some stakeholders, few independent experts even predict a timeframe for the maturity of quantum computing. Design and engineering challenges account for a very significant part of the complexity. For example, researchers and engineers must figure out how a quantum computer can be completely isolated from the world around it to protect the fragile state of the qubits, while at the same time allowing interactions with the qubits to control them (Institute for Quantum Computing, n.d.[67]; BSI, 2021[62]). The loss of information due to environmental noise, called quantum decoherence, increases with the number of qubits and requires maintaining current quantum computers at temperatures close to absolute zero (−273,15 °C, −459,67 °F). Quantum error correction techniques can be implemented to address decoherence, but they require additional qubits. Public announcements of major progress in quantum computing engineering reported only through an out-of-context number of qubits must therefore

be viewed with scepticism. While it is an active area of research, no one is willing to predict how long it will take researchers to master error correction (Cho, 2020[68]).

In addition to hardware and engineering challenges, totally new kinds of algorithm design principles leveraging quantum features will need to be invented, and an entirely new software stack will need to be developed (Grumbling and Horowitz, 2019[60]). , Quantum algorithms are much more difficult to design than algorithms for traditional computers. According to some experts, as of 2019, only a few dozen quantum algorithms had been developed (Vardi, 2019[69]). Mature quantum computers are not expected to be used like today's computers or smartphones, but rather like super calculators capable of handling certain problems or algorithms better than traditional computers (SQT, 2021[70]).

According to a 2019 "consensus study report" of the US National Academies of Sciences, Engineering, and Medicine, "the progress required to bridge the current [technological] gap makes it impossible to project the timeframe for a large error-corrected quantum computer, and while significant progress in these areas continues, there is no guarantee that all these challenges will be overcome. The process of bridging this gap might expose unanticipated challenges, require techniques that are not yet invented, or shift owing to new results of foundational scientific research that change our understanding of the quantum world" (Grumbling and Horowitz, 2019[60]). In fact, some researchers have even expressed scepticism over the feasibility of ever building a mature quantum computer capable of achieving useful tasks (Kalai, 2011[71]; Dyakonov, 2018[72]).

The German Federal Office for Information Security (BSI) reviewed the status of quantum computer development from the perspective of its digital security implications in 2017, with updates in 2019 and 2020. According to BSI, the point where quantum computers can no longer be simulated by current traditional supercomputers was reached in 2019, with design limitations preventing impact on current cryptography's robustness. Quantum processors are still several orders of magnitude away from being able to carry out effective cryptography attacks. Currently, an enormous effort would be needed to scale up quantum computing technologies to a cryptographically relevant level. According to BSI, with an optimistic view of near-term progress, a quantum computer capable of cryptographic attacks would be a major piece of infrastructure that could be the size of a football field and would require a concerted research programme with an industrialised nations pooling major research and development resources, similar to the Apollo and Manhattan projects. However, progress has been accelerating recently with the involvement of strong industrial players and large research programs, and commercial applications could further boost progress. All of this makes estimating a realistic timeframe for cryptographically relevant quantum computers difficult (BSI, 2021[62]).

Quantum communication is another potentially disruptive type of quantum information technology currently under research. Quantum communication makes use of the laws of quantum physics to transmit information via quantum particles, such as single photons of light through optical fibre or free space (Kristjánsson, Gardner and Chiri, 2021[73]). Superposition can be exploited to allow quantum particles to travel along multiple lines of communication simultaneously, making the information less susceptible to errors during transmission. Entanglement allows the transfer of quantum information across large distances, whereby the sender holds half of the entangled photons and the receiver holds the other half. Quantum information is transferred by using a combination of entanglement and traditional communication. Information is encoded in controllable parameters of the photons, such as their polarisation. To control the property of individual photons, the sender and receiver use specialised generation and detection devices requiring specific engineering conditions such as cryogenic temperatures (below -153°C, -243°F). Importantly, quantum computing is necessary, albeit on a simple level, for quantum communication (OFCOM, 2021[74]).

Quantum communication could enable a major advance in cryptography through the development of quantum key distribution (further discussed below). It would also offer ultra-secure communication because the fragile state of qubits in transit would guarantee the confidentiality of the communication. Should an

eavesdropper observe a qubit, its quantum state would immediately "collapse" to either 0 or 1, leaving behind a telltale sign of the observation (Giles, 2019[75]). Quantum communication could also, in theory, enable the development of a quantum Internet that joins up quantum computers to pool their capacity. However, the very notion of a quantum Internet is subject to debate (BSI, 2021[62]). The Quantum Internet Research Group of the Internet Research Task Force discusses how to design and build quantum networks (IRTF QIRG, n.d.[76])

Nevertheless, it is fair to say that the quantum computing race has started. The considerable potential benefits that quantum information technologies could bring in areas such as materials science, pharmaceuticals, energy and finance (US White House, 2022[77]) are attracting public and private stakeholders' attention and investments. According to McKinsey, private investors poured USD 2.35 billion into quantum technology start-ups in 2022 (2023[78]). Furthermore, many OECD governments are adopting national quantum strategies and allocating significant research budgets, as illustrated in Table 2.

Table 2. Public sector research investments in quantum technologies in select countries

Country / region	Strategy, policy instrument	Budget	Timeframe
Canada	National Quantum Strategy (2023)	USD 760 million (CAD 1 billion) USD 272 million (CAD 360 million)	2012 – 2023 2023
European Union	Quantum Technologies Flagship (2017)	EUR 1 billion	2018-2027
France	Stratégie Nationale Quantique (2021)	EUR 1 billion	2021-2025
Germany	Research funding Quantum Technologies Action Concept (2023)	EUR 650 million EUR 2.18 billon	2018-2022 2023-2026
India	National Quantum Mission (2023)	USD 732.8 million (INR 60 billion)	2023-2031
Japan	Quantum technology strategy review Quantum technology strategy review	USD 170 million (JPY 23.7 billion) USD 570 million (JPY 80 billion)	2021 2022
Korea	National Quantum Technologies Development Roadmap (2023)	USD 2.6 billion	2023-2035
Netherlands	Quantum Delta Netherlands (2021)	EUR 615 million	
United Kingdom	National Quantum Strategy (2023)	GBP 2.5 billion	2023-2033
United States	National Quantum Initiative (2018)	USD 449 million USD 672 million USD 855 million USD 918 million USD 844 million	2019 2020 2021 2022 2023

Note: these amounts cover funding allocated to research in quantum technologies, not necessarily limited to quantum computing and communications. The People's Republic of China is widely reported as being among the global leaders in terms of quantum research funding, but there is no reliable information on the amount of investment.

Sources: Quantum Flagship (n.d.), *Introduction to the quantum flagship*, https://qt.eu/about-quantum-flagship/; Government of Canada (2023), *Government of Canada launches National Quantum Strategy to create jobs and advance quantum technologies*, www.canada.ca/en/innovation-science-economic-development/news/2023/01/government-of-canada-launches-national-quantum-strategy-to-create-jobs-and-advance-quantum-technologies.html; Gouvernement Français (2023), *France 2030: des résultats concrets pour les 2 ans de la stratégie quantique*, www.info.gouv.fr/actualite/france-2030-des-resultats-concrets-pour-les-2-ans-de-la-strategie-quantique; Government of The Netherlands (2021), *Innovative projects given additional €1.35 billion boost due to funding from National Growth Fund*, www.government.nl/latest/news/2021/04/21/innovative-projects-given-additional-%E2%82%AC1.35-billion-boost-due-to-funding-from-national-growth-fund; Euractiv (2023), *Germany strives to catch up with US, China in quantum tech race*, www.euractiv.com/section/digital/news/germany-strives-catch-up-with-us-china-in-quantum-tech-race/; Kim, J. (2023), *S. Korea to invest $2.6 bn in quantum technology by 2035*, www.kedglobal.com/tech,-media-telecom/newsView/ked202305110016; Government of India (2023), *Cabinet approves National Quantum Mission to scale-up scientific & industrial R&D for quantum technologies*, https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1917888; UK NCSC (2023), *Next steps in preparing for post-quantum cryptography,* www.ncsc.gov.uk/whitepaper/next-steps-preparing-for-post-quantum-cryptography; US National Science and Technology Council (2023), *National Quantum Initiative Supplement to the President's FY 2023 Budget*, www.quantum.gov/wp-content/uploads/2023/01/NQI-Annual-Report-FY2023.pdf.

The potential for quantum computing to break cryptography in the future is a major challenge for today

Current symmetric cryptographic methods such as AES are not significantly affected by quantum computing if used with suitable key sizes (UK NCSC, 2020[79]; ANSSI, 2022[80]; ENISA et al., 2022[81]; ETSI, 2015[82]; BSI, 2021[62]; BSI, 2021[83]; UK NCSC, 2023[84]).

However, this is not the case with public key cryptography algorithms. Therefore, quantum computing directly threatens the continued robustness of public key cryptography, which is widely used for digital signature and key agreement between parties, i.e. the determination by remote parties of the symmetric keys they intend to use in a communication, introduced above (UK NCSC, 2020[79]; ANSSI, 2022[80]; US Government Accountability Office, 2021[61]).

The consequences are immense because the vulnerability of these cryptosystems to a quantum attack leads to the vulnerability of all security protocols that derive security from their public key ciphers, and of any product or security system deriving security from these protocols (ETSI, 2015[82]). While the quantum computers currently available are not a threat to public key cryptography, a future large general-purpose quantum computer, called a Cryptographically Relevant Quantum Computer (CRQC), could easily solve the mathematical problems at the core of public key cryptography (UK NCSC, 2020[79]). As noted by the US National Institute for Standards and Technologies (NIST), the availability of a CRQC to an adversary will break the security of nearly all modern public-key cryptographic systems. Consequently, all secret symmetric keys and private asymmetric keys that are now protected using current public-key algorithms, as well as the information protected under those keys, will be subject to exposure. This includes all recorded communications and other stored information protected by those public-key algorithms, because nothing can protect the confidentiality of encrypted material that was previously stored by an adversary if this adversary gains access to a CRQC at some point. Any such information still considered to be private or otherwise sensitive will be vulnerable to exposure and undetected modification (Barker, Polk and Souppaya, 2021[59]).

It will take some time for a CRQC to be available, but it is impossible to predict when, if ever, this will happen. If it happens sooner rather than later, stakeholders will face rapid a collapse of their cryptographic architecture and will have little time to react. Furthermore, some threat actors could carry out a “retroactive attack”, collecting today both high-value encrypted data and the data used for key agreement in view of decrypting it later with a CRQC. There is evidence that such an “intercept and store now, decrypt later” approach has been taken by some nation states (ENISA et al., 2022[81]). In addition, a threat actor could use a CRQC in the future to forge digital signatures and impersonate the legitimate private key owner, or tamper with information whose authenticity is protected by a digital signature. While this threat will be real when a CRQC is available, it needs to be taken into consideration today for high-value, root-level public keys that are intended to have long operational lifetimes (UK NCSC, 2020[79]; ANSSI, 2022[80]; BSI, 2021[83]). Furthermore, a national security agency may operate the first fully functional large quantum computer long before any public announcement is made about it so as to gain a significant intelligence advantage over competing nation states (ENISA et al., 2022[81]). The US National Security Agency issued an urgent warning in 2015 about the imminent threat to current public key cryptography posed by the development of quantum computers (BSI, 2021[62]; ANSSI, 2022[80]).

Considering the significant and growing research investments in quantum information technologies, several cybersecurity agencies warned that it is necessary to address today the anticipated collapse of the current cryptographic infrastructure resulting from tomorrow’s expected advent of quantum computing, and to start the transition to quantum resistant cryptography now (Chen et al., 2016[85]; ANSSI, 2022[80]; BSI, 2021[83]; UK NCSC, 2020[79]). In doing so, at least three factors should be considered, namely how long (ETSI, 2015[82]):

- the information needs to stay secure, a duration which depends on the information considered, e.g. a credit card payment information has a limited confidentiality time span, some State and military secrets may require secrecy during several decades;
- it will take to update the infrastructure to reach quantum safety, recognising that new cryptographic methods take a very long time to be widely accepted by the security community, and most information systems are not designed to facilitate rapid adaptation of new cryptographic methods without making significant changes to the system's infrastructure (according to NIST, algorithm replacement can be extremely disruptive and often takes decades to complete (Barker, Polk and Souppaya, 2021[59])); and
- it will take to build a CRQC. If this last timeframe is shorter than the shorter of the two others, secrets may be compromised by an adversary.

Furthermore, even if a functional CRQC could never be built, as quantum sceptics argue, the development of a new cryptographic paradigm would nevertheless offer a most welcome alternative to the widely used public key cryptography, should the discovery of a potential weakness jeopardise its utility, which can never be excluded (ANSSI, 2022[80]).

Quantum Resistant Cryptography: the solution for cryptography in the future quantum computing era

The solution to the challenge of quantum computing breaking traditional cryptography is to develop a family of new cryptographic algorithms that are immune to attacks leveraging both traditional and quantum computers. This new family of algorithm is called "quantum resistant cryptography" (QRC). These algorithms include key establishment and digital signatures and can be executed on traditional computers with traditional communication channels (ANSSI, 2022[80]). Once developed, they could be deployed in anticipation of a CRQC to address the "intercept and store now, decrypt later" challenge. QRC is also interchangeably called post-quantum, quantum safe, or quantum secure cryptography.

Since 2006, a large international community of researchers has been working on QRC, including through publicly funded research projects in the European Union and Japan (Chen et al., 2016[85]).

As usual in cryptography, trust in new cryptosystems is generally associated with the standardisation of algorithms by internationally recognised institutions such as ETSI, ISO, and NIST. In 2016, NIST initiated a QRC standardisation effort through the specification of evaluation criteria for quantum-resistant public key cryptography standards, and started to accept proposals of quantum-resistant public key encryption, digital signature, and key exchange algorithms, with the objective of selecting at least one candidate algorithm for each of these functionalities through a consensus procedure (Chen et al., 2016[85]). After a thorough three-round evaluation process, in 2022 NIST selected one quantum-resistant algorithm for key establishment and three for digital signatures out of a total of 82 proposals from international teams of researchers, and at the time of this writing continues the evaluation of four additional candidates for possible future inclusion in the standard (Alagic et al., 2022[86]; US NIST, 2022[87]; UK NCSC, 2023[84]). Many cyber security agencies welcomed the NIST process (BSI, 2021[83]; ANSSI, 2022[80]; UK NCSC, 2020[79]), which acted as a catalyst for strong involvement of the international cryptography research community and stimulated initiatives to co-ordinate domestic players such as the French "Risq" project (ANSSI, 2022[80]). During NIST's standardisation process, these cybersecurity agencies have issued recommendations encouraging organisations to consider QRC. In parallel, the Internet Engineering Task Force has been working on updating Internet protocols to be resistant against a quantum computer and ETSI has been producing migration and deployment guidance (IETF, 2022[88]; IETF, 2022[88]; UK NCSC, 2023[84]).

The UK National Cyber Security Centre (NCSC) invited large organisations to factor the threat of quantum computer attacks into their long-term roadmaps, such as the evolution of major commercial products and

services to support QRC. The NCSC encouraged organisations that manage their own cryptographic infrastructure to factor post quantum transition into their long-term plans and identify which systems will be high priority for transition, such as those that process sensitive personal data, or the parts of the public-key infrastructure with certificate expiry dates far into the future. Because of potential security and business continuity risks, the British cybersecurity agency did not recommend early adoption of non-standardised QRC, but underlined the ongoing development of relevant guidance in this area by standards bodies such as NIST and ETSI. The agency also emphasised the need to continue support for conventional public key cryptography for the interim period during which organisations will be required to operate both conventional and quantum-safe cryptography, while working towards a QRC-only future end state (UK NCSC, 2020[79]; UK NCSC, 2023[84]).

The German Federal Office for Information Security (BSI) called for early consideration of the need for implementing QRC at an early stage within an appropriate risk management framework. In light of the current lack of knowledge regarding potential weaknesses in QRC, the German cybersecurity agency recommended "hybridation", i.e. the combination of traditional algorithms with QRC rather than QRC-only implementation (BSI, 2021[83]).

The French cybersecurity agency (ANSSI) also supported hybridation through a three-phase transition process: i) an immediate and voluntary hybridation phase where quantum resistant security aims to add post-quantum defence-in-depth to pre-quantum security assurance; ii) a second phase, to begin not earlier than 2025, providing quantum resistant security assurance while avoiding any pre-quantum security regression, and during which quantum resistance would be claimed as a security feature; and iii) a third phase, after 2030, with optional hybridation where the level of assurance provided by quantum resistant security would be equivalent to the current pre-quantum level (ANSSI, 2022[80]). ANSSI recognised that standardisation does not necessarily means maturity, with many aspects, such as the design of secure implementations of the algorithms, still being research topics that will lack cryptanalytical hindsight for some time. France encourages the development of future QRC and hybrid cryptographic products.

Both BSI and ANSSI recommended implementing "cryptoagility" for new products, that is, designing them with sufficient flexibility to be able to react to all conceivable developments, implement upcoming recommendations and standards and possibly replace algorithms that no longer guarantee the desired level of security in the future (ANSSI, 2022[80]; BSI, 2021[83]). According to ANSSI, a product is said to be "cryptoagile" if it includes the possibility to update its cryptographic algorithms without recalling it or substituting it with a new one. Cryptoagility is also defined as "a design feature that enables updates to future cryptographic algorithms and standards without the need to modify or replace the surrounding infrastructure" (US DHS, 2022[89]) and "best practice that enables cryptographic algorithms used in applications and protocols to be interchanged easily to ensure systems remain secure if new cryptographic vulnerabilities are discovered" (Canadian Centre for Cyber Security, 2022[90]).

The transition to QRC is one of the priorities of the US Department of Homeland Security (DHS)'s vision for cybersecurity and resilience (US DHS, 2022[91]). In partnership with NIST, DHS released a roadmap to help organisations protect their data and systems and to reduce risks related to the advancement of quantum computing technology. The US Cybersecurity and Infrastructure Security Agency (CISA) established a QRC Initiative in 2022 to unify and drive agency efforts to address threats posed by quantum computing, and to support critical infrastructure and government network owners and operators during the transition to quantum resistant cryptography. The initiative covers i) assessing the quantum computing risk across the US critical infrastructure (i.e. 55 National Critical Functions) to determine where QRC transition work is underway, where the greatest risk resides, and what may require federal support; ii) planning where CISA and its partners should focus resources and engagement with owners and operators across public and private sectors; iii) partnering to foster adoption and implementation of policies, standards, and requirements to improve the security of the Federal Civilian Executive Branch, state, local, tribal, and territorial (SLTT) entities; critical infrastructure; and the underlying technology that supports all of these entities; and iv) engaging stakeholders to develop mitigation plans and encourage implementation of

standards once they are available as well as to develop technical products to support these efforts (US CISA, 2022[92]). DHS also created a roadmap to help organisations prepare their transition to QRC, based on a scenario where a CRQC would be available in 2030 (US DHS, 2022[91]; US DHS, 2021[93]).

The Australian Signal Directorate (ASD) encouraged research, testing and practical trials of QRC algorithms while NIST finalises the standardisation process, and encourages Australian industry to continue research and development of quantum technologies (ACSC, 2023[94]). In planning for a quantum resistant computing environment, organisations are encouraged to: create a transition plan for the use of QRC algorithms within their environment, including the testing and adoption of new QRC algorithms as well as the decommissioning of legacy cryptographic algorithms, based on an inventory of their use of public key cryptography and on the value of all data within their environment that is currently protected by public key cryptography. The ASD also encouraged organisations to discuss anticipated QRC requirements with vendors or those involved in quantum resistant cryptographic research and to educate and train relevant areas of their organisation on the eventual transition to the use of QRC algorithms.

The Canadian Centre for Cyber Security invited organisations to develop and budget for a transition plan to deploy standardised QRC, prioritising sensitive information with a long lifespan such as intellectual property, tax data, and medical records, and to ask vendors about their plans to securely upgrade software and hardware to QRC. The Centre recommended several steps to plan for the transition (Canadian Centre for Cyber Security, 2021[95]).

Quantum Cryptography and Quantum Key Distribution

Traditional cryptography is based upon mathematical foundations, which means that the security of the cryptosystem depends upon the resources available to a potential adversary to break a mathematical challenge or attack the system with brute force. If such resources are not available today, an adversary can still “intercept and store now, and decrypt later”, as explained above. Quantum cryptography protects against these scenarios because it takes advantage of the laws of physics rather than mathematical complexity. In theory, quantum cryptography can remain secure regardless of the amount of processing power and mathematical innovation an adversary could use. This would be a major paradigm shift in cryptography.

It is easy to confuse quantum cryptography with QRC because, like QRC, quantum cryptography is robust against future algorithmic and computational advances, including the emergence of quantum computers. However, quantum cryptography is fundamentally different from QRC because it requires special equipment to leverage quantum physics and therefore cannot run on existing traditional computers. Quantum cryptography is a subset of quantum communication because it leverages the same quantum principles.

Despite being sometimes presented as synonymous with quantum cryptography, quantum key distribution (QKD) is rather a specific application of quantum cryptography[13]. QKD enables two remote parties to build a secret key through a dialogue taking place on public channels while ensuring that any observation of the secret in transit would be detected, a feature that traditional (i.e. non-quantum) cryptographic methods do not provide (US NSA, n.d.[96]; ANSSI, n.d.[97]; UK NCSC, 2020[98]; BSI, 2021[62]). In practice, encrypted data is sent as traditional bits over the network, while the secret key is transmitted (but not measured and retained) as quantum states of light (OFCOM, 2021[74]), through special equipment (e.g. single photon detectors) via a fibre or satellite link. Because information is encoded in quantum states, it would be impossible for an eavesdropper to observe the data stream without changing the value of some of the qubits and introducing errors, making the observation detectable by the sender and the recipient (ETSI, 2015[82]). Therefore, QKD provides confidentiality and integrity but not availability, as noted below (ANSSI, n.d.[97]). Furthermore, the eavesdropper would not be able to copy the qubits transmitted in an unknown state, a consequence of the quantum physics “no-cloning” principle (BSI, 2021[62]; ETSI, 2015[82]). This means that any attempt to exploit a flaw in an implementation of transmitters or receivers would have to

be carried out in real time as there is no way to save the information for later decryption by more powerful technologies (ETSI, 2015[82]).

QKD could also be used without symmetric cryptography, to provide communication security regardless of an adversary's computational power. In this case, however, the data rate is typically between 1 000 and 1 000 000 times lower than when using symmetric encryption, which eliminates this option for most applications (ANSSI, n.d.[97]).

Unlike quantum computing, QKD is feasible with technology available today (BSI, 2021[62]). Several fibre-based and free space based QKD networks have been deployed or are under construction worldwide. A review of recent and ongoing large-scale deployment of QKD networks identified projects in Canada, People's Republic of China (hereafter "China"), Europe, India, Italy, Japan, Korea, Spain, the Russian Federation, the United Kingdom, and the United States, as well as standardisation efforts by CEN-CENELEC, ETSI, IEEE, ITU-T, ISO/IEC JCT-1, the China Communications Standards Association (CCSA), and the UK British Standards Institute (BSI). Together, these organisations had published 22 standards as of 2022 and were developing 20 more (Stanley et al., 2022[99]).

Nevertheless, several cybersecurity agencies have expressed strong reservations regarding the potential of QKD and quantum computing to match security expectations and compete with QRC algorithms. The main argument is that the engineering required to balance communication needs and security requirements has extremely low tolerance for error, making the security of QKD and quantum computing highly implementation-dependent rather than assured by laws of physics (US NSA, n.d.[96]). In theory, the security of QKD is based on laws of physics, but in practice, it is based on the degree of perfection with which it is technically implemented, namely the degree to which potential adversaries can exploit possible deviations of real life quantum cryptography systems from the theoretical requirements, for example in the transmitters or receivers (ETSI et al., 2018[100]). Evaluations by cybersecurity agencies are pointing out that achieving such a degree of perfection is far from easy and cheap, considerably reducing the number of potential use cases.

Cybersecurity agencies such as the US National Security Agency (NSA), the UK NCSC, the French ANSSI and the German BSI have highlighted the following additional issues:

- *QKD is a partial solution.* It does not provide a means to authenticate the QKD transmission source (US NSA, n.d.[96]). The lack of authentication makes QKD vulnerable to physical man-in-the-middle attacks in which an adversary can agree individual shared secret keys with two parties who believe they are communicated with each other (UK NCSC, 2020[98]). Parties must therefore use asymmetric cryptography or preplaced keys to provide authentication (US NSA, n.d.[96]). However, the interactions between the QKD system and asymmetric authentication mechanism raise additional issues, and preplacing keys increases the cost of QKD networks (BSI, 2021[62]).
- *The security benefit of QKD can be provided by less expensive and better understood QRC*, which do not require special hardware and can provide authentication (US NSA, n.d.[96]; UK NCSC, 2020[98]);
- *QKD requires special purpose equipment*, such as a dedicated fibre connection or physically managed free-space transmitter, and it cannot be easily integrated into existing network equipment. Furthermore, hardware-based QKD equipment lacks flexibility for upgrades or security patches (US NSA, n.d.[96]), is expensive and raises digital sovereignty issues in countries or regions where no manufacturers exists, such as the European Union (BSI, 2021[62]).
- *Fibre-based QKD has a limited range. Longer ranges increase infrastructure costs and insider threat risks, and they do not offer end-to-end security*. When using fibre, QKD requires direct point-to-point links as it cannot tolerate active devices such as switches, routers, and optical amplifiers, thereby reducing the range of the communication. The maximum distance of the communication depends on the level of losses, which grows exponentially as a function of distance. Currently, fibre-based QKD is limited to about 100 kilometers (ANSSI, n.d.[97]; BSI, 2021[62]). Trusted relays

could increase the range, but also the costs and risk (US NSA, n.d.[96]). Quantum repeaters based on quantum entanglement would resolve this challenge, but they are unlikely to be available in the near future (BSI, 2021[62]). Greater distances are possible with satellite links (ANSSI, n.d.[97]), which are both costly and more exposed to availability attacks (BSI, 2021[62]).

- *QKD increases the risk of denial-of-service attacks*. The sensitivity to interception, which guarantees the confidentiality of the transmission, also increases the risk of denial of service (US NSA, n.d.[96]).
- *Side channel attacks are not yet fully understood*. Numerous side-channel attacks on QKD systems have been demonstrated over the years. QKD devices are highly technical, and it is therefore imperative to prevent all known side-channel attacks, thoroughly investigate devices for their resistance to these attacks, and continue research on unknown side-channel attacks (BSI, 2021[62]). In fact, QKD equipment has not been thoroughly analysed following standardized methodologies such as Common Criteria (ANSSI, n.d.[97]), although BSI has started to work in this area in partnership with ETSI (BSI, 2021[62]).

More generally, the actual security of QKD is based on the limited security of the hardware and engineering design required to operate QKD rather than on the unconditional security derived from underlying laws of physics (US NSA, n.d.[96]). As it is very difficult to perfectly implement QKD, an attacker could cause abnormal behavior in the equipment that would compromise security (ANSSI, n.d.[97]). The gap between the theoretical security offered by the laws of quantum physics and real-life implementations is very wide. Several attacks on commercial QKD systems leveraging hardware vulnerabilities have been published (ANSSI, n.d.[97]; US NSA, n.d.[96]).

In summary, the NSA views QRC as a more cost effective and easily maintained solution than QKD, does not support the usage of QKD or quantum computing to protect communications in US national security systems, and does not anticipate certifying or approving any QKD or quantum computing security products for usage by national security systems' customers unless current limitations are overcome (US NSA, n.d.[96]). Similarly, while welcoming the ongoing research and assurance work currently underway in this area, the UK NCSC does not endorse the use of QKD for any government or military applications, and cautions against sole reliance on QKD for business-critical networks, especially in critical national infrastructure sectors. The NCSC encourages the adoption of QRC against the quantum threat rather than QKD (UK NCSC, 2020[98]). For ANSSI, QKD is an interesting research area that deserves further research but is not yet sufficiently mature to be fully implemented for operational purposes. It is currently at a distinct disadvantage in all cases where cryptography is implemented in software. Its most reasonable use is in combination with symmetric encryption to provide communication security between fixed locations that are sufficiently close to each other and connected by an optical fibre (ANSSI, n.d.[97]). The French authorities currently do not recommend allocating operational budget to QKD. BSI recognises that QKD can represent an alternative, should QRC be broken in the future by algorithmic advances, and the agency also welcomes research in the technologies underlying QRC such as quantum networking. However, for BSI, there are still numerous issues to be clarified and limitations to be addressed before QKD can be recommended as a security-critical technology for practical applications. The use of QKD is currently conceivable mainly in the context of experiments for restricted use cases where practical limitations are less significant, in hybrid mode as an add-on in conjunction with traditional and quantum resistant key agreement techniques (BSI, 2021[62]). The Australian Signal Directorate also underlines the practical limitations of QKD and does not support its use for secure communications as of 2023 (ACSC, 2023[94]). The Canadian Cyber Centre noted in 2021 that QKD is not a replacement for current applications of cryptography, but it could be a way of securely communicating in the future (Canadian Centre for Cyber Security, 2021[95]).

Technical and other responses to the law enforcement challenge: a trend towards more targeted approaches?

To carry out their mission in a world where communications are increasingly end-to-end encrypted, law enforcement and national security agencies use various means and methods, such as metadata analysis and "lawful hacking", in combination with more traditional investigation techniques.

In many cases, E2EE communications encrypt the content of the communication from end to end, but not the associated metadata, which therefore can technically be intercepted, stored and analysed for law enforcement and national security purposes. Metadata typically includes the identifier of the endpoints, as well as the time, date and duration of the exchanges. It can reveal considerable information about the suspected activities of a targeted individual.

Lawful hacking is the exploitation of vulnerabilities in the devices of suspected individuals to access their content and monitor their activities. In addition to the San Bernardino attack mentioned above, lawful hacking has been successfully used in high profile investigations on the darknet, specifically regarding crimes of child sexual exploitation and trafficking of drugs and weapons (Finklea, 2017[101]). Recent large scale examples of lawful hacking include the FBI's ANOM program (Baker and Klehm, 2021[102]) and the French-Dutch EncroChat operation (Europol, 2023[103]). In the case of ANOM, the FBI set up a company selling secure communications services to criminals that led to 800 arrests, seizures of more than 8 tons of cocaine, 250 firearms, and more than USD 48 million. In the case of EncroChat, French and Dutch police infiltrated a European-based communication company (EncroChat) to monitor suspected criminals and ultimately arrested 6 558 individuals and seized close to EUR 900 million, over 100 tons of cocaine, 3.3 tons of heroin as well as hundreds of vehicles, boats, homes, and weapons. For this operation, the police intercepted, shared and analysed over 115 million criminal conversations of approximately 60 000 EncroChat users.

Metadata analysis and lawful hacking are not without privacy and security concerns. For example, while the targeted collection and analysis of metadata respecting human rights does not raise concerns, privacy and human rights advocates have stressed that metadata analysis can be as revealing as content, especially when it is collected in bulk, a practice viewed as a form of general and indiscriminate surveillance that is inherently disproportionate (Privacy International, 2022[104]).

While lawful hacking is used to access content before encryption or after decryption, it can also be used to manipulate data and devices' functionalities, such as activating the microphone, camera, or GPS location. Lawful hacking has raised questions, for example with respect to potential disincentives to patching, negative effects on innovation, and participation of governments in grey and black vulnerability markets where some sellers and buyers are criminals themselves (Bellovin et al., 2014[105]; OECD, 2021[106]). According to some researchers, there is a need to develop a more robust legal framework for lawful hacking that would address issues such as its definition and scope, prerequisites for deployment, the development and acquisition of tools, potential interference with the public disclosure of vulnerabilities, as well as jurisdictional issues (Liguori, 2020[107]).

The list below includes some of the key technical proposals that have been put forward for how public policy could address the lawful access dilemma. Most of these proposals have been widely debated, rejected as "backdoors" by numerous security and privacy experts, and are not mandated through legislation or regulation in OECD countries.

For such experts, a backdoor is defined as a category of methods that ultimately decrypt communications for an actor other than the sender and intended recipients, allowing third-party access to communications without the sender's or recipient's knowledge or permission (Privacy International, 2022[104]). It is also defined as an intentionally built-in mechanism used to bypass a system's security measures to gain access to that system or its data (EDRI, 2022[108]). Privacy and security experts argue that backdoors increase

security and privacy risk by introducing a security vulnerability that can be discovered and exploited by cybercriminals and other offensive actors. This is the main reason the experts reject any form of backdoor established for lawful access.

- Downgrading cryptography

Before the "crypto war", cryptography regulation typically restricted the use of strong cryptography to specific categories of users, who generally had to register and justify its use. Other users were left with weaker cryptography that the government could break when appropriate. In today's deregulated environment, some privacy and security experts consider that forcing users to adopt weaker encryption would be a "downgrade attack" (Privacy International, 2022[104]). Chinese cryptography regulation has been reported as imposing such limitations on the use, as well as import and export of strong cryptography[14].

- Key escrow

Key escrow, also known as key recovery, was one of the first technical solutions proposed to enable lawful access to encrypted data. The basic idea is that an official organisation such as a government agency or a trusted third party acts as an escrow agent, holding a copy of the decryption key to enable authorised access to encrypted data under certain circumstances. If the data owner or user is unable or unwilling to provide the encryption key, the escrow agent can release the stored key to the authorised party, allowing them to decrypt and access the data. The above-mentioned Clipper Chip proposal was one type of technical implementation of such a key escrow mechanism. Key escrow mechanisms are still being discussed in countries such as India (Ray, 2021[109]).

- Ghost Protocol

This proposal, also known as "silent listener", formulated by the UK GCHQ aims to implement the digital equivalent of the old-style physical crocodile clip hooked on a telephone line by asking the service provider to silently add an invisible and silent law enforcement participant to end-to-end encrypted group call or chat communications. According to its authors, this technique would not undermine or affect E2EE and would only require suppressing a notification on a target's device and possibly those they communicate with (Levy and Robinson, 2018[110]). However, as explained above, E2EE means that the communication is encrypted from end to end, and that "confidentiality is broken if content *can be* decrypted at any intermediate point", which this technique would do by adding a stealthy listener and creating a situation where the participants do not control who the endpoints are. A broad coalition of tech and trade business groups, civil society, and human rights organisations as well as security and privacy experts opposed the proposal, noting that it would create digital security risks by undermining authentication systems, introducing potential unintentional vulnerabilities, and creating new risks of abuse or misuse of systems. It would also break user trust and transparency (Bradford Franklin and Wilson Thompson, 2019[111]).

- Message hash escrow

This technique, proposed by the Indian government, aims to prevent harm resulting from viral messages circulating in large communication platforms such as Whatsapp. The idea is to hold individuals responsible for the consequences of what they post on such platforms, which would require the ability to bind responsibility for a message that caused harm after becoming viral to the initial author. The platform would have to apply a hash function to each message a person composes, attach it to the message together with the encoded identity of the author, and ensure that this information remains attached to the message even when it is forwarded. This would allow the authorities to track authors of viral messages falling under content control regulations. The proposal was criticised by Privacy International as potentially undermining E2EE (Privacy International, 2022[104]) and as easy to circumvent and likely to be ineffective (Ray, 2021[109]).

- Client-side scanning

To detect and take relevant action with respect to illegal user content such as CSEA, communication platforms typically use automated content moderation tools based on AI and techniques that compare hash values of user files transiting on their servers with hash values of known illegal content. In the absence of mature and cost effective FHE, platforms that adopt E2EE are prevented from using such automated tools (OECD, 2023[112]).

Some stakeholders contend that existing content moderation tools can work in end-to-end encrypted environments if they are deployed on the client side instead of the server side (OECD, 2023[112]). In principle, the process is similar to an antivirus scan. The platform's application on the user's device downloads the database of known illegal content's hash values, performs the comparison, and triggers specific actions when a match is found. In August 2021, Apple announced such a measure for the uploading of photos to its iCloud service. A client-side hashing technology called NeuralHash would analyse images on the user's device for matches against a database of known CSEA images provided by the US National Centre for Missing and Exploited Children (NMEC). If an on-device match was found, and crossed a threshold of known CSEA content, Apple would be notified. Apple would then manually review the report to confirm the match, disable the user's account, and send a report to NCMEC. The proposal received criticism from a range of privacy experts and as of December 2022 it was withdrawn (OECD, 2023[112]).

Because the scanning takes place before encryption or after decryption, the proponents of client-side scanning claim that it does not break E2EE. For a group of well-known technical security, privacy and cryptography experts, "client-side scanning by its nature creates serious security and privacy risks for all society while the assistance it can provide for law enforcement is at best problematic. There are multiple ways in which client-side scanning can fail, can be evaded, and can be abused" (Abelson et al., 2021[113]). They argue that the technique does break E2EE because it reveals the content of E2EE communication and defeats the purpose of E2EE encryption communications, which are meant to stay private and secure (Privacy International, 2022[104]; Abelson et al., 2021[113]) Furthermore, it is viewed as disproportionate to scan all the material being sent over an E2EE service, from all users, to identify the small amount deemed problematic (Privacy International, 2022[104]).

According to the UN High Commissioner for Human Rights this "paradigm shift [would] raise a host of serious problems with potentially dire consequences for the enjoyment of the right to privacy and other rights". For example, client-side scanning will inevitably expose false positives to third parties, and "is likely to have a significant chilling effect on free expression and association, with people limiting the ways they communicate and interact with others and engaging in self-censorship", a view shared by many technical security and privacy experts (Abelson et al., 2021[113]). Furthermore, client-side scanning could be repurposed as a mass-surveillance tool (Abelson et al., 2021[113]) or extended to other purposes ("function creep"), widening the scope of the targeted content, for example to suppress political debate or to target opposition figures, journalists and human rights defenders (Office of the United Nations High Commissioner for Human Rights, 2022[114]). For the Internet Society, client-side scanning is simply lacking effectiveness as it would be easy for criminals to modify the objectionable content to evade detection (ISOC, 2022[115]). Lastly, security and privacy experts view the scanning taking place on the user's device as a source of weakness rather than as a security feature, because it can potentially be abused by many adversaries, including criminals and hostile states actors with limited ability for users to verify its scope of action on their device (Abelson et al., 2021[113]). More generally, like server-side scanning, client-side scanning is unlikely to detect previously unknown CSEA content, and to detect grooming activities.

The discussion on the merits and dangers of client-side scanning is ongoing. For example, in a detailed analysis, two UK GCHQ technical directors underlined the multifaceted complexity of the challenges faced by law enforcement when countering child sexual abuse online. They found no reason why these techniques cannot be implemented safely in many of the situations one will encounter, recognised that

more work may be needed, and concluded that “there are clear paths to implementation that would seem to have the requisite effectiveness, privacy and security properties” (Levy and Robinson, 2022[116]). Their analysis was subsequently rebutted by academics (Anderson, 2022[117]) and evaluated by the UK National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online (REPHRAIN) (Peersman et al., 2023[118]).

4 Conclusion

Cryptography serves as the cornerstone of digital trust, ensuring the security of online interactions and data exchanges. It guarantees the integrity and confidentiality of information both in transit and at rest, with digital signatures verifying the origin and integrity of data. Despite its theoretical strength, practical implementation can introduce vulnerabilities, while emerging technologies like homomorphic encryption and quantum computing create both opportunities and challenges. Homomorphic encryption, in its nascent stage, shows promise for secure data processing in untrusted environments, while quantum computing presents a potential threat to traditional cryptographic systems, necessitating a gradual transition to quantum-resistant cryptography (QRC). These technologies are still relatively far from maturity, and it is not currently possible to accurately assess how soon they will reach it. However, when this time approaches, it might become necessary to better understand their potential impact on cryptographic policies.

References

Abelson, H. et al. (2021), *Bugs in our Pockets: the Risks of Client-Side Scanning*, https://arxiv.org/pdf/2110.07450.pdf. [113]

Abelson, H. et al. (2015), *Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications*, https://mitpress.mit.edu/keys-under-doormats-security-report/ (accessed on 24 July 2023). [9]

ACSC (2023), *Planning for Post-Quantum Cryptography*, https://www.cyber.gov.au/resources-business-and-government/governance-and-user-education/governance/planning-post-quantum-cryptography (accessed on 10 July 2023). [94]

Alagic, G. et al. (2022), *Status report on the third round of the NIST Post-Quantum Cryptography Standardization process*, National Institute of Standards and Technology (US), Gaithersburg, MD, https://doi.org/10.6028/nist.ir.8413-upd1. [86]

Albrecht, M. et al. (2018), *Homomorphic Encryption Standard*, https://homomorphicencryption.org/standard/. [58]

Anderson, R. (2022), *Chat Control or Child Protection?*, https://doi.org/10.48550/arXiv.2210.08958 (accessed on 21 December 2023). [117]

ANSSI (2022), *ANSSI views on the Post-Quantum Cryptography transition*, https://www.ssi.gouv.fr/uploads/2022/01/anssi-technical_position_papers-post_quantum_cryptography_transition.pdf. [80]

ANSSI (n.d.), *Should Quantum Key Distribution be Used for Secure Communications? Technical Position Paper: QKD v2.1*, https://www.ssi.gouv.fr/uploads/2020/05/anssi-technical_position_papers-qkd.pdf. [97]

Arghire, I. (2022), *Cornami Raises $68 Million for Quantum Secure Computing on Encrypted Data*, https://www.securityweek.com/cornami-raises-68-million-quantum-secure-computing-encrypted-data/. [47]

Awadallah, R., A. Samsudin and M. Almazrooie (2021), "Verifiable Homomorphic Encrypted Computations for Cloud Computing", *International Journal of Advanced Computer Science and Applications*, Vol. 12/10, https://doi.org/10.14569/ijacsa.2021.0121089. [52]

Baker, S. and B. Klehm (2021), *Legal Tetris and the FBI's ANOM Program*, https://www.lawfaremedia.org/article/legal-tetris-and-fbis-anom-program (accessed on 27 July 2023). [102]

Barker, W., W. Polk and M. Souppaya (2021), *Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms*, National Institute of Standards and Technology, https://doi.org/10.6028/nist.cswp.04282021. [59]

BBC (2015), *Europol chief warns on computer encryption*, https://www.bbc.com/news/technology-32087919 (accessed on 24 July 2023). [6]

Bellovin, S. et al. (2014), *Lawful hacking: using existing vulnerabilities for wiretapping on the Internet*, https://scholarlycommons.law.northwestern.edu/njtip/vol12/iss1/1 (accessed on 28 July 2023). [105]

Bradford Franklin, S. and A. Wilson Thompson (2019), *Open Letter to GCHQ on the Threats Posed by the Ghost Proposal*, https://www.lawfaremedia.org/article/open-letter-gchq-threats-posed-ghost-proposal (accessed on 25 July 2023). [111]

BSI (2021), *Migration to Post Quantum Cryptography*, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/Migration_to_Post_Quantum_Cryptography.pdf?__blob=publicationFile&v=2. [83]

BSI (2021), *Quantum safe cryptography - fundamentals, current developments, and recommendations*, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Brochure/quantum-safe-cryptography.pdf. [62]

Campbell, N. et al. (2022), *How the US EARN IT Act Threatens Security, Confidentiality, and Safety Online*, https://www.internetsociety.org/resources/2022/internet-impact-brief-how-the-us-earn-it-act-threatens-security-confidentiality-and-safety-online/#_ftn1. [16]

Canadian Centre for Cyber Security (2022), *Guidance on becoming cryptographically agile - ITSAP.40.018*, https://www.cyber.gc.ca/en/guidance/guidance-becoming-cryptographically-agile-itsap40018 (accessed on 22 December 2023). [90]

Canadian Centre for Cyber Security (2021), *Preparing your organization for the quantum threat to cryptography - ITSAP.00.017*, https://www.cyber.gc.ca/en/guidance/preparing-your-organization-quantum-threat-cryptography-itsap00017 (accessed on 10 July 2023). [95]

CDT (2023), *CDT Leads Broad Civil Society Coalition Urging Senate to Drop EARN IT Act*, https://cdt.org/insights/cdt-leads-broad-civil-society-coalition-urging-senate-to-drop-earn-it-act/ (accessed on 18 July 2023). [15]

Chen, L. et al. (2016), *Report on Post-Quantum Cryptography*, National Institute of Standards and Technology, https://doi.org/10.6028/nist.ir.8105. [85]

Cho, A. (2020), "No room for error", *Science*, https://www.science.org/content/article/biggest-flipping-challenge-quantum-computing. [68]

Comey, J. (2014), *Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?*, https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course (accessed on 18 July 2023). [3]

Congressional Research Service (2022), *Defense Primer: Quantum Technology*, https://crsreports.congress.gov/product/pdf/IF/IF11836. [64]

Creeger, M. (2022), "The Rise of Fully Homomorphic Encryption", *Queue*, Vol. 20/4, pp. 39-60, https://doi.org/10.1145/3561800. [36]

DARPA (2021), *DARPA Selects Researchers to Accelerate Use of Fully Homomorphic Encryption*, https://www.darpa.mil/news-events/2021-03-08. [45]

Dyakonov, M. (2018), *The Case Against Quantum Computing*, IEEE Spectrum, https://spectrum.ieee.org/the-case-against-quantum-computing. [72]

EDRI (2022), *State access to encrypted data. A digital rights perspective*, https://edri.org/wp-content/uploads/2022/10/Position-Paper-State-access-to-encrypted-data.pdf (accessed on 25 July 2023). [108]

ENISA (n.d.), *Public Key Infrastructure (PKI)*, https://www.enisa.europa.eu/topics/incident-response/glossary/public-key-infrastructure-pki. [119]

ENISA, J. et al. (2022), *Post-Quantum Cryptography: Current state and quantum mitigation*, Publications Office of the European Union, https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation. [81]

ETSI (2015), *Quantum Safe Cryptography. An introduction, benefits, enablers and challenges*, https://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf. [82]

ETSI (n.d.), *Quantum-Safe Cryptography (QSC)*, https://www.etsi.org/technologies/quantum-safe-cryptography (accessed on 3 January 2024). [133]

ETSI, M. et al. (2018), *Implementation Security of Quantum Cryptography. Introduction, challenges, solutions*, ETSI White Paper No. 27. [100]

Euractiv (2023), *Germany strives to catch up with US, China in quantum tech race*, https://www.euractiv.com/section/digital/news/germany-strives-catch-up-with-us-china-in-quantum-tech-race/. [129]

European Parliament (2023), *Combating child sexual abuse online - 2022/0155(COD)*, https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2022/0155(COD)&l=en (accessed on 18 July 2023). [14]

European Union (2014), *Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC*, http://data.europa.eu/eli/reg/2014/910/oj. [120]

Europol (2023), *Dismantling encrypted criminal EncroChat communications leads to over 6 500 arrests and close to EUR 900 million seized*, https://www.europol.europa.eu/media-press/newsroom/news/dismantling-encrypted-criminal-encrochat-communications-leads-to-over-6-500-arrests-and-close-to-eur-900-million-seized (accessed on 27 July 2023). [103]

Fernàndez-València, R. (2022), *Verifiable Homomorphic Encryption*, https://medium.com/iovlabs-innovation-stories/verifiable-homomorphic-encryption-7de41e39c20. [51]

Finklea, K. (2017), *Law Enforcement Using and Disclosing and Disclosing Technology Vulnerabilities*, https://sgp.fas.org/crs/misc/R44827.pdf. [101]

Fisher, D. (2013), *TURKTRUST Officials Say No Evidence of Malice in Certificate Incident*, https://threatpost.com/turktrust-officials-say-no-evidence-malice-certificate-incident-010713/77369/. [24]

Giles, M. (2019), *Explainer: What is quantum communication?*, https://www.technologyreview.com/2019/02/14/103409/what-is-quantum-communications/ (accessed on 28 June 2023). [75]

Gillmor, D., ACLU and N. Oever (2015), *Human Rights Protocol Considerations Glossary. draft-dkg-hrpc-glossary-00*, IETF, https://datatracker.ietf.org/doc/html/draft-dkg-hrpc-glossary-00. [21]

Global Encryption Coalition (2022), *70 organizations, cyber security experts, and elected officials sign open letter expressing dangers of the UK's Online Safety Bill*, https://www.globalencryption.org/2022/11/70-organizations-cyber-security-experts-and-elected-officials-sign-open-letter-expressing-dangers-of-the-uks-online-safety-bill/ (accessed on 19 July 2023). [18]

Global Encryption Coalition (2022), *Joint statement on the dangers of the EU's proposed regulation for fighting child sexual abuse online*, https://www.globalencryption.org/2022/05/joint-statement-on-the-dangers-of-the-eus-proposed-regulation-for-fighting-child-sexual-abuse-online/ (accessed on 19 July 2023). [19]

Goodin, D. (2021), *Mimecast says SolarWinds hackers breached its network and spied on customers*, https://arstechnica.com/gadgets/2021/03/mimecast-says-solarwinds-hackers-breached-its-network-and-spied-on-customers/. [29]

Gorantala, S., R. Springer and B. Gipson (2023), "Unlocking the Potential of Fully Homomorphic Encryption", *Communications of the ACM*, Vol. 66/5, pp. 72-81, https://doi.org/10.1145/3572832. [33]

Gouvernement Français (2023), *France 2030: des résultats concrets pour les 2 ans de la stratégie quantique*, https://www.gouvernement.fr/sites/default/files/contenu/piece-jointe/2023/03/20230330_france2030_dp_deux_ans_de_la_strategie_nationale_quantique_vdef2_clean.pdf. [127]

Government of Canada (2023), *Government of Canada launches National Quantum Strategy to create jobs and advance quantum technologies*, https://www.canada.ca/en/innovation-science-economic-development/news/2023/01/government-of-canada-launches-national-quantum-strategy-to-create-jobs-and-advance-quantum-technologies.html. [126]

Government of India (2023), *Cabinet approves National Quantum Mission to scale-up scientific & industrial R&D for quantum technologies*, https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1917888. [131]

Government of The Netherlands (2021), *Innovative projects given additional €1.35 billion boost due to funding from National Growth Fund*, https://www.government.nl/latest/news/2021/04/21/innovative-projects-given-additional-%E2%82%AC1.35-billion-boost-due-to-funding-from-national-growth-fund. [128]

Grassi, P., M. Garcia and J. Fenton (2017), *Digital identity guidelines: revision 3*, National Institute of Standards and Technology, Gaithersburg, MD, https://doi.org/10.6028/nist.sp.800-63-3. [23]

Grumbling, E. and M. Horowitz (eds.) (2019), *Quantum Computing*, National Academies Press, Washington, D.C., https://doi.org/10.17226/25196. [60]

Homomorphic Encryption Standardization (n.d.), *Basics of homomorphic encryption*, https://homomorphicencryption.org/introduction/. [30]

IBM (2021), *The next step in homomorphic encryption for Linux on IBM Z and LinuxONE*, https://www.ibm.com/blog/the-next-step-in-homomorphic-encryption-for-linux-on-ibm-z/. [41]

IETF (2022), *Post-Quantum Cryptography*, https://wiki.ietf.org/group/sec/PQCAgility (accessed on 3 January 2024). [88]

Institute for Quantum Computing (n.d.), *Quantum Computing*, https://uwaterloo.ca/institute-for-quantum-computing/quantum-101/quantum-information-science-and-technology/quantum-computing. [67]

Intel (2021), *Intel to Collaborate with Microsoft on DARPA Program*, https://www.intel.com/content/www/us/en/newsroom/news/intel-collaborate-microsoft-darpa-program.html#gs.yo43kd. [48]

Intel (n.d.), *Intel Homomorphic Encryption Toolkit*, https://www.intel.com/content/www/us/en/developer/tools/homomorphic-encryption/overview.html. [53]

IRTF QIRG (n.d.), *Quantum Internet Research Group QIRG*, https://www.irtf.org/qirg.html (accessed on 21 December 2023). [76]

ISO/IEC (2049), *ISO/IEC 18033-6:2019 - IT Security techniques — Encryption algorithms — Part 6: Homomorphic encryption*, https://www.iso.org/standard/67740.html. [54]

ISOC (2023), *Homomorphic Encryption: What Is It, and Why Does It Matter?*, https://www.internetsociety.org/resources/doc/2023/homomorphic-encryption/. [32]

ISOC (2022), *Fact Sheet: Client-Side Scanning*, https://www.internetsociety.org/resources/doc/2020/fact-sheet-client-side-scanning/ (accessed on 26 July 2023). [115]

ITIC and SIIA (2015), *Letter to President Obama*, https://www.itic.org/dotAsset/58fbf8de-cd86-47a0-a114-43a55776d2e6.pdf (accessed on 24 July 2023). [7]

ITU (2023), *Technical Report: FHE-based data collaboration in machine learning*, https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=17999. [56]

ITU (2022), *The case for standardizing homomorphic encryption*, https://www.itu.int/hub/2022/12/the-case-for-standardizing-homomorphic-encryption/. [57]

Jarvis, C. (2021), *Crypto Wars. The Fight for Privacy in the Digital Age: A Political History of Digital Encryption*, CRC Press. [123]

Kalai, G. (2011), *How Quantum Computers Fail: Quantum Codes, Correlations in Physical Systems, and Noise Accumulation*, https://arxiv.org/abs/1106.0485. [71]

Kim, J. (2023), *S.Korea to invest $2.6 bn in quantum technology by 2035*, https://www.kedglobal.com/tech,-media-telecom/newsView/ked202305110016. [130]

Knodel, M. et al. (2023), *Definition of End-to-end Encryption*, Internet Engineering Task Force, https://datatracker.ietf.org/doc/draft-knodel-e2ee-definition/. [20]

Koerner, K. (2021), *Introduction to Homomorphic Encryption*, https://medium.com/golden-data/introduction-to-homomorphic-encryption-d903d02d4ce0. [35]

Koerner, K. (2021), *Legal perspectives on PETs: Homomorphic encryption*, https://medium.com/golden-data/legal-perspectives-on-pets-homomorphic-encryption-9ccfb9a334f. [42]

Kristjánsson, H., R. Gardner and G. Chiri (2021), *Quantum Communications: new potential for the future of communications*, https://www.ofcom.org.uk/research-and-data/technology/general/quantum-communications. [73]

Levy, I. and C. Robinson (2022), *Thoughts on child safety on commodity platforms*, https://arxiv.org/abs/2207.09506. [116]

Levy, I. and C. Robinson (2018), *Principles for a More Informed Exceptional Access Debate*, https://www.lawfaremedia.org/article/principles-more-informed-exceptional-access-debate (accessed on 25 July 2023). [110]

Levy, S. (2001), *Crypto: how the code rebels beat the government- Saving Privacy in the Digital Age*, Viking Press. [121]

Liguori, C. (2020), *Exploring Lawful Hacking as a Possible Answer to the "Going Dark" Debate*, https://repository.law.umich.edu/mtlr/vol26/iss2/5. [107]

Masters, O. and H. Hunt (2019), *Towards a Homomorphic Machine Learning Big Data Pipeline for the Financial Services Sector*, Cryptology ePrint Archive, https://eprint.iacr.org/2019/1113. [37]

Mattsson, U. (2021), *Security and Performance of Homomorphic Encryption*, https://www.globalsecuritymag.com/Security-and-Performance-of,20210601,112333.html. [46]

McConnell, M., M. Chertoff and W. Lynn (2015), *Why the fear over ubiquitous data encryption is overblown*, https://www.washingtonpost.com/opinions/the-need-for-ubiquitous-data-encryption/2015/07/28/3d145952-324e-11e5-8353-1215475949f4_story.html (accessed on 24 July 2023). [11]

McKinsey (2023), *Quantum technology sees record investments, progress on talent gap*, https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/quantum-technology-sees-record-investments-progress-on-talent-gap. [78]

McLaughlin, J. (2015), *Tech Companies and Civil Liberties Groups Force Obama To Weigh In On Encryption Debate*, https://theintercept.com/2015/10/27/tech-companies-and-civil-liberties-groups-force-obama-to-weigh-in-on-encryption-debate/ (accessed on 24 July 2023). [10]

Meta (2021), *A Privacy-Focused Vision for Social Networking*, https://www.facebook.com/notes/2420600258234172/. [22]

Microsoft (2017), *Microsoft to remove WoSign and StartCom certificates in Windows 10*, https://www.microsoft.com/en-us/security/blog/2017/08/08/microsoft-to-remove-wosign-and-startcom-certificates-in-windows-10/. [27]

MIT (2021), *SCRAM*, https://scram.mit.edu/ (accessed on 9 October 2023). [38]

Munjal, K. and R. Bhatia (2022), "A systematic review of homomorphic encryption and its contributions in healthcare industry", *Complex & Intelligent Systems*, https://doi.org/10.1007/s40747-022-00756-z. [31]

Nellis, A. (2022), *The quantum internet, explained*, https://news.uchicago.edu/explainer/quantum-internet-explained. [63]

NIST (2023), *Privacy-Enhancing Cryptography*, https://csrc.nist.gov/Projects/pec. [55]

OECD (2023), "Emerging privacy-enhancing technologies: Current regulatory and policy approaches", *OECD Digital Economy Papers*, No. 351, OECD Publishing, Paris, https://doi.org/10.1787/bf121be4-en. [39]

OECD (2023), *Transparency Reporting on Child Sexual Exploitation and Abuse Material Online by the Global Top-50 Content Sharing Services [report DSTI/CDEP(2022)16/REV3]*. [112]

OECD (2022), *OECD Policy Framework on Digital Security: Cybersecurity for Prosperity*, OECD Publishing, Paris, https://doi.org/10.1787/a69df866-en. [2]

OECD (2021), *Encouraging vulnerability treatment: background report - Responsible management, handling and disclosure of vulnerabilities*, https://one.oecd.org/document/DSTI/CDEP/SDE(2020)3/FINAL/en/pdf. [106]

OFCOM (2021), *Quantum Communications: new potential. Executive summary*, https://www.ofcom.org.uk/__data/assets/pdf_file/0013/222601/Executive-Summary.pdf. [74]

Office of the United Nations High Commissioner for Human Rights (2022), *The right to privacy in the digital age*, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G22/442/29/PDF/G2244229.pdf?OpenElement. [114]

Open Technology Institute (2015), *Massive Coalition of Security Experts, Tech Companies and Privacy Advocates Presses Obama to Oppose Surveillance Backdoors*, https://www.newamerica.org/oti/press-releases/massive-coalition-of-security-experts-tech-companies-and-privacy-advocates-presses-obama-to-oppose-surveillance-backdoors/ (accessed on 24 July 2023). [8]

Paillier, P. (2020), *Introduction to FHE*, https://fhe.org/meetups/001-introduction-to-fhe. [34]

Park, J. (2021), *Homomorphic Encryption for Multiple Users with Less Communications*, https://eprint.iacr.org/2021/1085. [49]

Peersman, C. et al. (2023), *REPHRAIN : Towards a Framework for Evaluating CSAM Prevention and Detection Tools in the Context of End-to-End Encryption Environments : a Case Study*, https://www.rephrain.ac.uk/safety-tech-challenge-fund/ (accessed on 21 December 2023). [118]

Preskill, J. (2012), *Quantum computing and the entanglement frontier*, https://arxiv.org/abs/1203.5813. [65]

Privacy International (2022), *Securing Privacy : Privacy International on End-to-End Encryption*, https://privacyinternational.org/sites/default/files/2022-09/SECURING%20PRIVACY%20-%20PI%20on%20End-to-End%20Encryption.pdf (accessed on 25 July 2023). [104]

Quantum Flagship (n.d.), *Introduction to the quantum flagship*, https://qt.eu/about-quantum-flagship/. [125]

Ray, T. (2021), *The Encryption Debate in India: 2021 Update*, https://carnegieendowment.org/2021/03/31/encryption-debate-in-india-2021-update-pub-84215 (accessed on 25 July 2023). [109]

Save Online Speech Coalition (n.d.), *#SaveOnlineSpeech*, https://saveonlinespeech.org/ (accessed on 19 July 2023). [17]

Security Week (2016), *StartSSL Flaw Allowed Attackers to Obtain SSL Cert for Any Domain*, https://www.securityweek.com/startssl-flaw-allowed-attackers-obtain-ssl-cert-any-domain/. [25]

Sedik, T., M. Malaika and M. Gorban (2021), *Quantum Computing's Possibilities and Perils*, https://www.imf.org/en/Publications/fandd/issues/2021/09/quantum-computings-possibilitiesand-perils-deodoro. [66]

Singh, S. (2000), *The Code Book : The Secret History of Codes and Code-breaking*, Fourth Estate. [122]

SQT (2021), *Quantum communications : a primmer*, https://www.kratosdefense.com/-/media/k/co/quantum-communications-primer_2021-march-10.pdf. [70]

Stanley, M. et al. (2022), "Recent Progress in Quantum Key Distribution Network Deployments and Standards", *Journal of Physics: Conference Series*, Vol. 2416/1, p. 012001, https://doi.org/10.1088/1742-6596/2416/1/012001. [99]

Symantec (2022), *Billbug: State-sponsored Actor Targets Cert Authority, Government Agencies in Multiple Asian Countries*, https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/espionage-asia-governments-cert-authority. [28]

Tayer, W. (2018), *GoDaddy: Random Value Vulnerability in Domain Validation*, https://bugzilla.mozilla.org/show_bug.cgi?id=1484766. [26]

Tourky, D., M. ElKawkagy and A. Keshk (2016), "Homomorphic encryption the "Holy Grail" of cryptography", *2016 2nd IEEE International Conference on Computer and Communications (ICCC)*, https://doi.org/10.1109/compcomm.2016.7924692. [43]

UK DSIT (2023), *National quantum strategy*, https://www.gov.uk/government/publications/national-quantum-strategy. [124]

UK NCSC (2023), *Next steps in preparing for post-quantum cryptography*, https://www.ncsc.gov.uk/whitepaper/next-steps-preparing-for-post-quantum-cryptography (accessed on 4 January 2024). [84]

UK NCSC (2020), *Preparing for Quantum-Safe Cryptography*, https://www.ncsc.gov.uk/whitepaper/preparing-for-quantum-safe-cryptography. [79]

UK NCSC (2020), *Quantum security technologies. V1.0*, https://www.ncsc.gov.uk/whitepaper/quantum-security-technologies. [98]

UK Parliament (2022), *Online Safety Bill*, https://bills.parliament.uk/bills/3137. [13]

US CISA (2022), *Post-Quantum Cryptography Initiative*, https://www.cisa.gov/quantum (accessed on 10 July 2023). [92]

US Congress (2023), *S. 1207 - A Bill to establish a National Commission on Online Child Sexual Exploitation*, https://www.congress.gov/118/bills/s1207/BILLS-118s1207is.pdf. [12]

US DHS (2022), *Cryptographic Agility Infographic*, https://www.dhs.gov/publication/cryptographic-agility-infographic (accessed on 22 December 2023). [89]

US DHS (2022), *Post-Quantum Cryptography*, https://www.dhs.gov/quantum (accessed on 10 July 2023). [91]

US DHS (2021), *Preparing for Post-Quantum Cryptography: Infographic*, https://www.dhs.gov/publication/preparing-post-quantum-cryptography-infographic (accessed on 10 July 2023). [93]

US Government Accountability Office (2021), *Quantum Computing and Communications. Status and Prospects*, https://www.gao.gov/assets/gao-22-104422.pdf. [61]

US National Science and Technology Council (2023), *National Quantum Initiative Supplement to the President's FY 2023 Budget*, https://www.quantum.gov/wp-content/uploads/2023/01/NQI-Annual-Report-FY2023.pdf. [132]

US NIST (2022), *NIST Announces First Four Quantum-Resistant Cryptographic Algorithms*, https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms (accessed on 28 August 2023). [87]

US NSA (n.d.), *Quantum Key Distribution (QKD) and Quantum Cryptography (QC)*, https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/ (accessed on 20 June 2023). [96]

US White House (2022), *National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems*, https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/. [77]

van den Nieuwenhoff, T. (2021), *Fully Homomorphic Encryption: the history*, https://tvdn.me/fhe/2021-05-27-homomorphic-encryption-history. [44]

Vance Jr, C. et al. (2015), *When Phone Encryption Blocks Justice*, https://www.nytimes.com/2015/08/12/opinion/apple-google-when-phone-encryption-blocks-justice.html. [5]

Vardi, M. (2019), "Quantum hype and quantum skepticism", *Communications of the ACM*, Vol. 62/5, pp. 7-7, https://doi.org/10.1145/3322092. [69]

Watt, N., I. Traynor and R. Mason (2015), *David Cameron pledges anti-terror law for internet after Paris attacks*, https://www.theguardian.com/uk-news/2015/jan/12/david-cameron-pledges-anti-terror-law-internet-paris-attacks-nick-clegg (accessed on 24 July 2023). [4]

Yang, W. et al. (2023), "A Review of Homomorphic Encryption for Privacy-Preserving Biometrics", *Sensors*, Vol. 23/7, p. 3566, https://doi.org/10.3390/s23073566. [50]

Zama (n.d.), *A 6 minute introduction to homomorphic encryption*, https://6min.zama.ai/. [40]

Zimmermann, P. (2021), *PGP Marks 30th Anniversary*, https://philzimmermann.com/EN/essays/PGP_30th/. [1]

Notes

1 For a chronology, see for example (Jarvis, 2021[123]).

2 For a review of related events across countries, see for example https://carnegieendowment.org/programs/technology/cyber/encryption.

3 www.noearnitact.org

4 The English term cipher comes from the Arabic word “sifr”, meaning “zero”. The same Arabic word became “chiffre” in French, which means both “digit” and “cipher” in English.

5 For a general history of cryptography, see (Singh, 2000[122]) and for an account of the discovery of cryptography, see (Levy, 2001[121]).

6 A hash value is the result of a hash function. While symmetric and asymmetric cryptography involve an encryption and a decryption process, a hash function is a one-way encryption algorithm that encrypts data in a manner that i) generates a fixed-sized result (hash values of a given hash function always have the same number of bits regardless of the size of the input value), ii) makes it quasi-impossible to recover the initial data in its intelligible form from the hash value, iii) makes it unique, in the sense that it is extraordinarily unlikely that for a given hash function, two different set of data would generate the same hash.

7 In the European Union, the terms electronic signature and digital signature carry different legal meaning. Under the eIDAS Regulation, an electronic signature is any data in electronic form which is attached to or logically associated with other data in electronic form and which is used to sign the data. This includes for example a scanned signature or even a typed name. However, a digital signature is a specific type of electronic signature that meets technical requirements for security and authenticity, such as a digital certificate that meets certain technical and legal requirements for security and authenticity called a qualified certificate (European Union, 2014[120]).

8 For more details about PKI, see for example (ENISA, n.d.[119]).

9 For estimates with other computing power capacity, see https://asecuritysite.com/principles/key?keys=10000000000. For a visual demonstration of such large numbers, see www.youtube.com/watch?v=S9JGmA5_unY.

[10] www.infoworld.com/article/2623829/weaknesses-in-ssl-certification-exposed-by-comodo-security-breach.html

[11] Quantum technologies include other areas such as quantum sensing and metrology, as well as quantum simulation, which are beyond the scope of this report. For examples of other applications, see the US National Quantum Initiative (www.quantum.gov) and the EU Quantum Flagship (https://qt.eu).

[12] For a more sophisticated description, see (Dyakonov, 2018[72]).

[13] Quantum cryptography research also includes quantum cryptographic protocols, quantum authentication, quantum randomness (the generation of truly random numbers), etc.

[14] www.gp-digital.org/world-map-of-encryption/