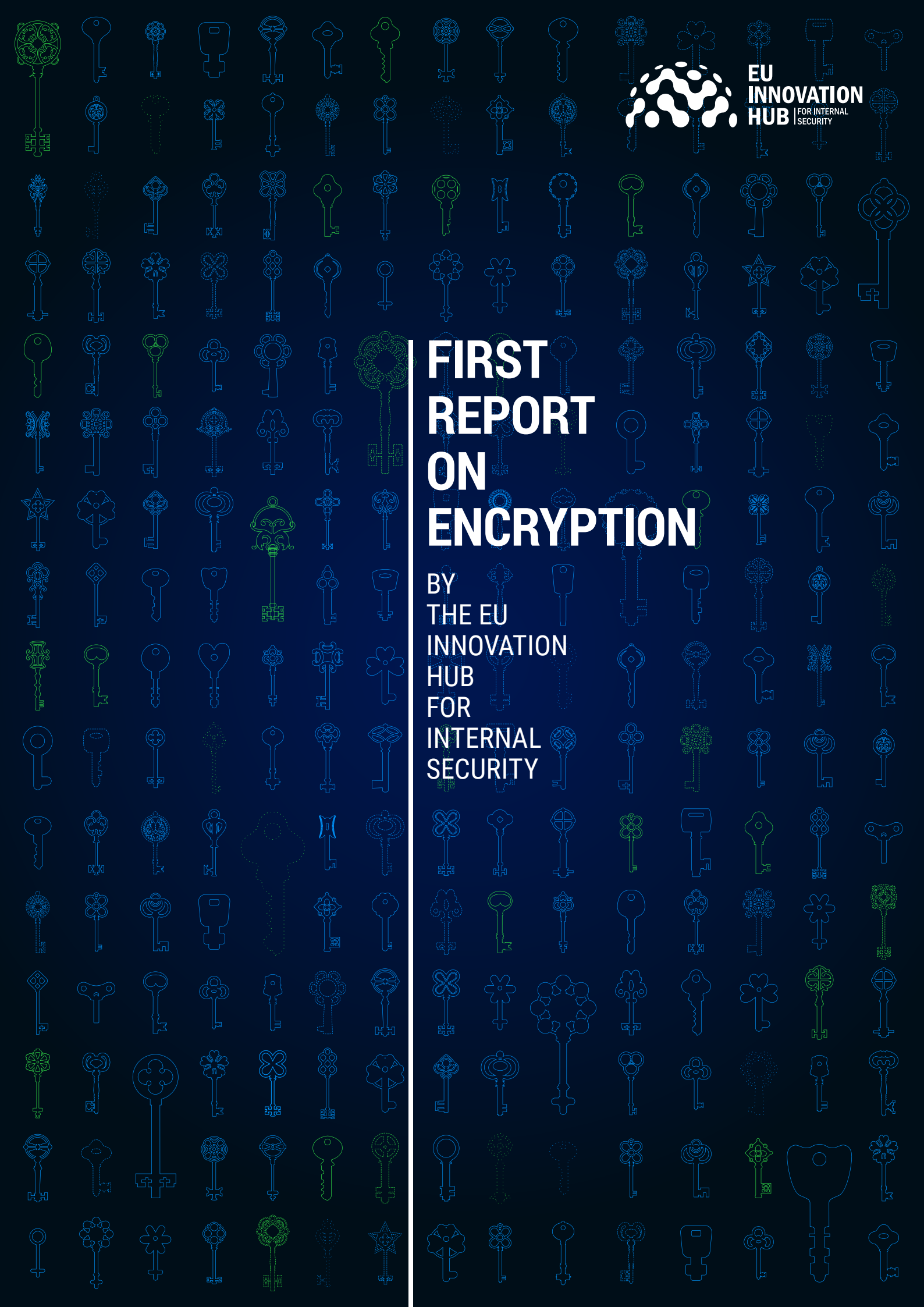

EU INNOVATION HUB FOR INTERNAL SECURITY

FIRST REPORT ON ENCRYPTION

BY THE EU INNOVATION HUB FOR INTERNAL SECURITY

Acknowledgements

This report was produced by the following EU Innovation Hub for Internal Security members: Europol, Eurojust, European Commission's Directorate-General for Migration and Home Affairs (DG HOME), European Commission's Joint Research Center (JRC), European Council's Counter-Terrorism Coordinator, European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (EU-LISA).

PDF | ISBN 978-92-95236-26-4 | DOI: 10.2813/437117 | QL-09-24-220-EN-N

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

Luxembourg: Publications Office of the European Union, 2024

Cite this publication: EU Innovation Hub (2024), First Report on Encryption by the EU Innovation Hub for Internal Security, Publications Office of the European Union, Luxembourg.

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

www.europol.europa.eu

Contents

Executive summary

The first report on encryption created by the EU Innovation Hub for Internal Security presents an analysis on the topic of encryption from a legislative, technical and developmental viewpoint. It also touches upon certain specific judicial process and court rulings about overcoming encryption in cases where it represents an obstacle for criminal investigations, especially in relation to evidence admissibility.

In the last few years, the debate between data privacy and lawful interception (LI) has evolved into a more constructive discussion. While police and judicial authorities acting within their power can be prevented from accessing digital evidence by modern privacy-enhancing technologies like end-to-end encryption (E2EE) and Rich Communication Services (RCS) systems, different international initiatives are calling for a balanced approach, where LI can coexist with encryption without undermining cybersecurity and/or privacy. At the same time, a framework to access encrypted communications is steadily taking shape in the EU. As technology advances, finding a balance between individual privacy and collective security remains an ongoing challenge. The key to success is to foster dialogue, cooperation and innovation to ensure that fundamental rights (including protection of personal data), as well as the security and integrity of the person, are equally respected.

The newly adopted e-evidence package can be seen as a step in the right direction for enhancing law enforcement access to electronic evidence. However, the package does not specifically address the challenges related to encryption outlined in this report because the regulation does not include obligations for service providers to make data in the clear available.

The admissibility of evidence gathered from encrypted communication channels has been legally questioned in a number of countries. However, several courts have dismissed such challenges, thereby setting precedents in favour of using evidence gathered in this manner (for instance, the French Court of Cassation accepts the use of evidence from the EncroChat cryptophone service). Court rulings in Germany, Italy and the Netherlands have also established that evidence gathered through authorised interception by other nations (e.g. France, Canada) is valid and usable in domestic criminal proceedings. In other words, courts in these countries have concluded, in several instances, that data gathered in this manner is obtained lawfully and in a proportional manner. In its ruling of 30 April 2024, the Court of Justice of the European Union clarified conditions under which intercepted data from encrypted communication channels can be requested and transmitted between EU Member States, and used in criminal proceedings as evidence.

Technologies using encryption present many challenges but also opportunities for law enforcement and security practitioners. In this paper, we will look at encryption challenges and opportunities in relation to various technologies, i.e.: quantum computing, cryptocurrencies, biometric data, the Domain Name System (DNS), telecommunication technologies, artificial intelligence (AI) and large language models (LLMs).

For example, cryptocurrencies are widely used for laundering criminal proceeds and there are concerns that tracing funds will become more complicated if zero-knowledge proofs and layer 2 applications are more widely deployed in the blockchain. On the other hand, the use of custodial wallets, where the user does

not hold their own private key, create opportunities for cooperation between law enforcement authorities, exchanges and service providers to seize crypto assets that are suspected to be of criminal nature.

In the realm of DNS encryption, two competing approaches have surfaced, DoT/DoQ and DoH/DoHTTP3. In both cases, the content of the DNS messages is encrypted, hindering the lawful access to suspects' DNS traffic contents. In practice, it means that law enforcement will become more dependant of DNS service providers' cooperation.

Similarly, the use of encryption in 4G (VoLTE) and 5G (Standalone 5G) telecommunication technologies complicates law enforcement and judicial authorities' ability to carry out investigations. These standards introduce end-to-end encryption (E2EE) for voice calls over the network, which complicates lawful interception of criminal communications in roaming scenarios. For this reason, it is important for the communication service providers to disable privacy-enhancing technologies in home routing scenarios. Looking into the future, it is vital that law enforcement needs are taken into account when designing standards for the next generation telecommunication services (e.g. 6G) and that the architecture introduced has innate features that enable law enforcement to carry out their criminal investigations.

The use of biometric recognition is predicated on being able to safely store and use biometric data, which can be enabled by biometric template protection (BTP) technologies. These technologies enable citizens to, for example, use national ID cards, passports or conduct banking transactions through biometric verification, while recognition comparison operations take place in the encrypted domain. The security and privacy of current biometric recognition systems still need to be enhanced before they become fully deployable in public services.

Artificial intelligence (AI) and large language models (LLMs) continue to play an important role in cryptography. These technologies can be used for both strengthening encryption algorithms as well as for analysing cryptographic security systems, which in some cases helps break the encryption by scrutinising its mathematical properties.

The same goes for the advancements that are being made in the field of quantum computing, which can be used for breaking cryptographic protocols in the future. This ties in with the well-known concept of 'store now, decrypt later' that could create opportunities for law enforcement to decrypt stored criminal communications, but also creates risks as malicious actors might also be gathering encrypted data with the same prospect in mind. In addition, quantum computing will likely also support the creation of new digital forensic techniques that help with the retrieval of electronic evidence in investigations.

The main future research areas relevant for policymakers in the areas of law enforcement and justice will most likely be the use of "user-controlled" encryption (and its effect on digital forensics and decryption capabilities), the development of quantum computing, and the use of encrypted data for development of machine learning (ML) algorithms. The EU has different funding schemes that can be leveraged to develop research projects to address the challenges related to these technologies.

Introduction

Encryption refers to the process of transforming information into a secure format to protect it from unwanted access or modifications by third parties, typically referred to as the confidentiality and integrity of data. Having originally been used to prevent intercepted handwritten messages from being read, encryption has evolved over the last decades to protect digital data and is now a well-established field of research and development, closely connected with computer science and mathematics. As EU citizens spend more and more of their daily lives online, expectations about digital security to safeguard our activities there have increased in parallel.

Although encryption on its own does not solve the challenge of providing effective security for data and systems, it is at the heart of digital security. It makes encryption an integral part of daily life and contributes to developments in this area of technology, as well as others relying on it. At the same time, the wider and increased usage of encryption technology continues to be exploited by criminals, both as part of their modus operandi and/or as a means to enable secret communication and illegal activities by remaining out of reach of law enforcement and judicial authorities.

Besides the well-known EncroChat and SkyECC cases, EU agencies Europol and Eurojust have both dealt with several other cases in which organised crime groups were suspected of using encryption tools and methods. The use of encryption continues to pose significant challenges to law enforcement and judicial authorities to intercept (criminal) communications, and to successfully collect and use digital evidence in court proceedings. These cases concern not only cyber-enabled and cyber-dependent crimes, but also other crime areas such as drug trafficking, aggravated fraud schemes, and money laundering. Solutions found to collect encrypted digital evidence go hand-in-hand with ensuring the protection of fundamental rights and alignment with established principles of proportionality and necessity. Legal answers to this challenge continue being multi-faceted and complex.

This report was produced by the following EU Innovation Hub for Internal Security members:

- Europol,
- Eurojust,
- European Commission's Directorate-General for Migration and Home Affairs (DG HOME),
- European Commission's Joint Research Center (JRC),
- European Council's Counter-Terrorism Coordinator,
- European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (EU-LISA).

The report aims to provide an update on the topic of encryption from a legislative perspective, but also focus more heavily on a technical and developmental viewpoint. This report will touch upon certain specific legislative developments and court rulings about attacking encryption, especially in relation to evidence admissibility. Some of these have been reported in the

eighth edition of the Cybercrime Judicial Monitor[1], recently published in June 2023. In 2024, members of the European Judicial Cybercrime Network (EJCN) will be requested to provide an update about new or amended legal provisions concerning bypassing or attacking encryption at national level.

The report will also provide an update on recent policy developments, including those in regard to the High-Level Group on access to data for effective law enforcement (ADELE) (also known as the Expert Group on Going Dark, co-led by the Commission and the rotating Presidency of the Council).

Policy overview

In our increasingly digital and interconnected world, the need to strike a balance between individual privacy and public security has become a paramount topic of discussion. The fundamental right of personal data protection should go hand in hand with the fundamental rights of security and integrity of the person. One of the most contentious issues in this context is the tension between encryption and lawful access to data, as the problems arising from law enforcement agencies' inability to access electronic evidence is an increasing concern.

Commercial device manufacturers are increasingly implementing encryption methods that grant access to the content exclusively to device users, a concept known as "user-only-access" device encryption. Similarly, a growing number of communications service providers (CSPs) are structuring their platforms and applications to guarantee that only the communicating parties can decrypt and access the content, a practice commonly referred to as end-to-end encryption (E2EE). Both "user-only-access" and "end-to-end" encryption technologies guarantee the highly secure nature of user data, rendering it inaccessible to third parties - including the technology companies implementing these measures. Such technologies therefore increasingly restrict law enforcement's capacity to access crucial evidence and information, even when equipped with a warrant or court order, creating a challenge often referred to as the 'going dark' problem.

Law enforcement agencies (LEAs) argue that technology companies should modify their secure systems to provide lawful access mechanisms that would allow them to decrypt criminal communications. In response, technology companies and civil society groups contend that implementing such mechanisms could jeopardise system security and may not significantly enhance crime prevention. They also express concerns that lawful access mechanisms might be exploited by malicious actors, and criminals could turn to alternative non-compliant solutions to evade surveillance.

The 3rd Observatory Function Report on Encryption bore witness to the intensity of this debate and showcased European, American, and Australian policy initiatives, each bringing their respective contributions to the discussion. Two years later, tangible advances appear limited at first sight. However, it is interesting to note that the debate surrounding encryption and lawful access to data has moved to a more mature and constructive path.

NEW TECHNOLOGIES

Firstly, the situation concerning the deployment of warrant-proof encryption technologies has evolved. The concept of end-to-end encryption for Meta's Messenger, which faced substantial technological challenges in 2021, has materialised. The technology is now available for some users and Meta announced the roll-out at scale at the end of 2023[2]. Consequently, millions of messages containing ***inter alia*** child sexual abuse material (CSAM) will no longer be automatically detected by Meta and reported to the National Center for Missing & Exploited Children (NCMEC). Similarly, Apple Private Relay, a service provided by Apple offering anonymity through encryption to its iCloud users, is now up and running. The service is designed in a manner that Apple,

even when required to by the judiciary, is not in position to link web browsing activity with a specific user.

Another significant change is brought by the implementation and deployment of Rich Communication Systems (RCS) protocol by several major communication operators. From a user perspective, RCS is as an evolution of Short Message Service (SMS) as the protocol allows the exchange of group chats, video, audio, and high-resolution images in an encrypted manner. From a law enforcement perspective RCS is a new challenge as, depending on its implementation, lawful interception features (including decryption capabilities) may not be available. Finally, 5G standalone systems are slowly but steadily being rolled out, bringing long foreseen challenges (*see chapter on ''Telecommunication technologies''*).

INTERNATIONAL RESPONSE

Secondly, international initiatives of like-minded countries tend to address the issue of encryption in a more comprehensive manner, building on fundamental principles that can bring consensus. Notably, expanding on the 2020 EU Council Resolution on Encryption[3] and the G7 Interior and Security Ministerial Commitments 2021[4], G7 members called for an approach involving technology companies in fostering a safety-centric mind-set, and prioritising the concept of safety by design. This approach should encompass the integration of lawful access mechanisms without undermining cybersecurity or privacy, emphasising the concept of designed-in exceptional access.

At EU level, the Commission and the Presidency of the Council of the European Union launched the High-Level Group (HLG) on access to data for effective law enforcement[5], in June 2023. The HLG aims to provide a strategic vision on how to address current and anticipated challenges against the background of technological developments to ensure access to data for law enforcement and judicial authorities. It is set up as a collaborative and inclusive platform for stakeholders from all relevant sectors, including law enforcement, judicial authorities, data protection experts, private sector operators, NGOs, and academia, to work towards commonly accepted solutions. It is important to note that the HLG does not focus specifically on encryption, but more broadly on the challenge for law enforcement and judicial authorities in accessing data. This initiative will propose recommendations by mid-2024 for the further development of Union policies on lawful access to data at rest, data in providers' systems, and data in transit.

POLICY DEVELOPMENTS

Thirdly, rules pertaining to access to encrypted communications are significantly impacted by the broader framework of data protection and privacy, electronic communication, and cross-border access to electronic evidence, which is steadily taking shape in the EU. The framework constitutes a prerequisite to advance the encryption debate on solid grounds.

In particular, the European Electronic Communications Code (EECC)[6] harmonised the telecommunications regulatory framework across the EU, governing a range of legal obligations imposed upon telecommunications providers, including enabling lawful interception (LI) by competent national authorities in compliance with the ePrivacy Directive[7] and the General Data Protection Regulation[8]. No further details are given in the EECC, providing

Member States with discretionary powers to frame national rules on the implementation of LI capabilities, creating room for fragmentation across the EU. However, over-the-top (OTT) service providers must comply with the same obligations regarding their cooperation with public investigations and other public security authorities as traditional telecommunications service providers. This pertains to, for example, the storage of client data and its transfer to the authorities responsible for lawful interception[a].

In addition, from a more operational perspective, a list of non-technical requirements on (real time) access to data was put forward by the Swedish Presidency of the Council of the European Union. The requirements were compiled by security officials and are publicly available in a document named "Law Enforcement Operational Needs" (LEON). The document also describes the specific needs regarding encryption in the context of lawful interception[9]. Defining these security requirements is an important prerequisite for the development of international standards that provide a balance between the need for privacy, cybersecurity and lawful access in justified cases.

The tension between encryption and lawful access is a complex issue that requires careful consideration and nuance. As technology continues to advance, striking a balance between individual privacy and collective security remains an ongoing challenge. The key is to foster dialogue, cooperation and innovation to ensure that both data protection rights and the need for lawful interception are respected. In this evolving landscape, the above-mentioned initiatives can help move forward the policy debate on encryption towards solutions that respect the core values of democracy while safeguarding society.

a The EECC has significantly extended the definition of telecommunications services adding new categories of ECS, that were previously unregulated, such as number-based and number-independent interpersonal communications, however when it comes to requirements to implement LI capabilities some EU Member States still differentiate between number-independent interpersonal services and other telecommunications services while others, such as France or Belgium, don't.

Legislation

This chapter builds on the findings laid out in the Third Observatory Function report on encryption, published July 2021[10]. As concluded in the third Observatory Function report, based on an overview of legal provisions applied by nineteen different EU Member States plus Switzerland, the majority of countries applied general legal provisions related to overcoming encryption between 2018 and 2020. It was found that an important distinction can be made between provisions permitting directly accessing encrypted content, and those allowing for the use of tools to gain access to data before it is encrypted, or after it has been decrypted.

In June 2023, Eurojust published the eighth edition of the Cybercrime Judicial Monitor (CJM)[11], an annual report distributed to judicial and law enforcement authorities active in the field of combating cybercrime and cyber-enabled crimes. It covers legislative developments in these areas, nationally and internationally, as well as legislative developments concerning electronic evidence in general. Adopted EU legislation such as the Digital Services Act (DSA), in addition to ongoing European legal developments (e.g. Artificial Intelligence Act), are also touched upon. Relevant court rulings are presented and briefly analysed, for example, regarding the use of captured encrypted communication data. The CJM has a dedicated section on electronic evidence, linked to the topic of encryption.

NATIONAL LEGISLATION

The most recent CJM highlights that certain EU Member States reportedly introduced changes to existing national legislation, mainly in the area of (extended) remote search capabilities in information systems. It appears that this development can be seen in relation to bypassing encryption, as the CJM observes *'these new or adapted pieces of legislation might offer additional opportunities to capture and use (encrypted) data.'*

The Netherlands is one of the few European countries with specific legal provisions concerning encrypted data that entered into force on 1 October 2022. Article 558 of the Dutch Criminal Procedure Code[b] has created the possibility to use proportionate coercion to have a suspect unlock a seized device, with no approval of a supervisory judge being required. This is a temporary legal provision that will be reviewed after two years.

On 31 August 2023, the Research and Documentation Centre of the Netherlands, a centre of knowledge active in the field of justice and security, published its report 'Police hacking regulation abroad'[12]. The report contains a comparative analysis of 'legal regulations and safeguards' concerning law enforcement authorities' ability to ***'to intrude into computer systems … and investigate them'***, with findings relevant for the discussion of bypassing encryption.

Besides the Netherlands, the authors of the report have studied the situation in countries such as Belgium, Germany, France, Sweden, and the non-EU Member State Switzerland in more depth. They report on 20 countries having included

b The full provisions are detailed (in Dutch) at https://zoek.officielebekendmakingen.nl/stb-2022-276.html.

safeguards in their laws regarding the storage of data collected through targeted lawful access to a suspect's device. 13 countries have included a notification obligation in their laws. In half of these countries, notification can be deferred, or sometimes even omitted, if the investigation may be compromised.

From the report it can be concluded that the majority of EU Member States have direct or indirect capabilities for targeted lawful access to suspect's device. It is clear that accessing computer systems does not necessarily mean that authorities will encounter encrypted data, but bypassing technical security measures is sometimes necessary to capture digital evidence, encrypted or not.

EUROPEAN AND INTERNATIONAL LEGISLATION

On 17 November 2021, the Committee of Ministers of the Council of Europe adopted the Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence[c]. This Protocol supplements the Convention on Cybercrime and its First Protocol, aiming to further enhance the ability of criminal justice authorities to obtain electronic evidence from another jurisdiction for the purpose of criminal investigations or proceedings. On 14 February 2023, the Council of the European Union adopted a decision authorising EU Member States to ratify the Second Additional Protocol[13]. The recently adopted EU e-evidence package will be elaborated on further below.

In December 2020, the European Commission presented the Digital Services Act package, consisting of the Digital Services Act (DSA) and the Digital Markets Act (DMA). These new rules govern the digital space and digital services, including social media platforms. The DSA aims to create a safer online environment for users and companies protecting fundamental rights in the digital space. It provides a set of responsibilities and a clear accountability and transparency framework for providers of intermediary services, regardless of the location of these providers, within or outside the European Union. On 4 October 2022, the Council of the European Union adopted the DSA and on 19 October 2022, the Regulation (EU) 2022/2065 was adopted[14] and came into force on 16 November 2022, becoming directly applicable across the EU. Article 94 of the Regulation stipulates that the new rules shall apply from 17 February 2024 onwards.

On 10 September 2020, the European Commission presented a first legislative proposal containing an interim regulation allowing certain interpersonal communication services to derogate from established privacy rules to enable them to continue detecting and reporting child sexual abuse material (CSAM) online on a voluntary basis. Regulation (EU) 2021/1232 of the European Parliament and of the Council of 14 July 2021 entered into force on 2 August 2021[15]. The European Commission aimed to replace abovementioned interim regulation by proposing a new regulation on 11 May 2022[16], introducing mandatory measures to detect and report CSAM. A few months later, the European Data Protection Board and the European Data Protection Supervisor adopted a Joint Opinion on the proposed regulation, considering risks posed by it. On 12 October 2022, the Czech Presidency of the Council of the European Union presented a new compromise text on the proposed regulation:

c https://www.coe.int/en/web/cybercrime/second-additional-protocol

''A main concern raised against this legislative proposal is that companies could consider so-called client-side scanning as a solution to comply with the new legislation. Some law enforcement authorities favour this method, as it makes (obfuscation by) encryption of criminal content and communication less effective, but privacy advocates claim that it would almost be impossible to preserve and guarantee privacy.''

In order to ensure legal certainty and continuity while the legislative procedure on the proposed Regulation is ongoing, the Commission proposed an extension of the interim regulation until 2026 on
30 November 2023.

On 28 July 2023, the so-called EU electronic evidence package was adopted. The legislative package consists of two key components: the first is the Regulation on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal procedures. The second component is the Directive laying down harmonised rules on designating establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings. This legislation entered into force on 17 August 2023 and will be applicable on 17 August 2026 for the Regulation[17], and 17 February 2026 for the Directive (i.e. to be transposed in national legislation by then).

According to the European Commission, more than half of all criminal investigations today include a cross-border request to access electronic evidence such as texts, e-mails or messaging apps[20]. That is why several actions were proposed to make it easier and faster for police and judicial authorities to access electronic evidence they need in investigations to arrest and prosecute criminals. From the perspective of encryption, the creation of so-called European Production Orders and European Preservation Orders will allow judicial authorities to obtain e-evidence directly from a service provider or its legal representative in another EU Member State, and in less time than foreseen in the existing European Investigation Order or Mutual Legal Assistance procedure. As already concluded in the eighth edition of Eurojust's Cybercrime Judicial Monitor:

''…the adoption of the legislative package on e-evidence marks a significant advancement in the access to digital information in cross-border criminal investigations and prosecutions.''

By expediting and simplifying the process of obtaining electronic evidence from the service providers providing their services in the EU, this comprehensive legal framework aims to enhance the efficacy of law enforcement and judicial authorities in combating crime in the digital age.

It has to be noted that it is explicitly mentioned in the Regulation that its application should not affect the use of encryption by service providers or their users. Data requested by means of a European Production Order or a European Preservation Order should be provided or preserved regardless of whether they are encrypted or not: ''*The Regulation should not lay down any obligation for service providers to decrypt data*''. From this perspective, the

freshly adopted e-evidence package does not seem to assist law enforcement and judicial authorities with the problem that encryption poses for their criminal investigations.

SELECTED COURT RULINGS

On 30 April 2024, the Court of Justice of the European Union (CJEU) issued its judgment in case C-670/22 - *M.N. (EncroChat)*[18], following questions referred to the CJEU by the German Court (Landgericht Berlin). The questions mainly related to the lawfulness of the European Investigation Orders (EIO) which were issued by the German public prosecutor's office towards France, in view of obtaining EncroChat data, gathered by France, and using it in criminal proceedings in Germany.

In its ruling, the CJEU has interpreted several Articles of Directive 2014/41/EU regarding the European Investigation Order in criminal matters. The CJEU does not rule on the dispute itself (i.e., the national criminal case against the accused), which is the sole competence of the national courts.

First, the Court took a closer look at the competent authority to issue the EIO. The issuance of an order to transmit evidence that has already been gathered, is subject to the same conditions that apply in a domestic situation. In Germany, contrary to an order to intercept data (requiring issuance by a judge), an order for the transmission of already gathered data can be issued by a public prosecutor. The Court therefore replied that a public prosecutor can issue an EIO to request the transmission of (EncroChat) data that had already been gathered by the executing State (in this case the French authorities).

Secondly, concerning the substantive conditions for issuing an EIO for the transmission of evidence, the CJEU states that the same conditions apply as for the transmission of similar evidence in a purely domestic situation. It does not need to satisfy the same substantive conditions as those that apply to the collection of evidence. However, the CJEU clarifies that a court before which an action against an EIO is brought, must be able to review compliance with the fundamental rights of the persons concerned.

The Court further clarifies that 'interception of telecommunications' –within the meaning of Article 31 of Directive 2014/41- covers a measure entailing the infiltration of terminal devices for the purpose of gathering traffic, location and communication data from an internet-based communication service. This is in fact the interception measure which was performed by the French authorities on German territory in the EncroChat case. When carried out, such a measure should be notified, in good time, to the authority designated for that purpose by the Member State (or to any other authority if this specific one is not known) on whose territory the subject of the interception is located (i.e., Germany). In case the measure would not be allowed in a similar domestic case, this notification enables the competent authority of the notified State to indicate that the interception may not be carried out or needs to be terminated or, where appropriate, that any material already intercepted may not be used, or may only be used under conditions which it is to specify. This not only guarantees respect for the sovereignty of the notified Member State, but also protects the rights of the persons affected by the interception.

Finally, the Court states that the need to disregard information and evidence obtained in breach of the requirements of EU law exists only if a court comes to

the conclusion that an EIO has been unlawful. In any case, the Court reiterates that, in principle, the rules relating to admissibility of evidence and assessment of information and evidence in criminal proceedings is a matter of national law, but also that the rights of the defense and the right to a fair trial should be guaranteed: if a defendant cannot review or comment on important information or evidence, obtained through the EIO, and the said information and evidence are likely to have a preponderant influence on the findings of fact, these should be excluded from the criminal proceedings by the national criminal courts.

At national level, many cases have been and are still being brought to courts throughout Europe, where the admissibility of the evidence, obtained via interception of encrypted communication platforms, is being challenged. Below you will find some examples, taken from Eurojust's Cybercrime Judicial Monitor referenced previously.

In Germany, the Federal Court of Justice dismissed the appeal lodged following a judgment passed by the Hamburg Regional Court on 15 July 2021 (sentence for offences of drug trafficking). The Court ruled that the EncroChat data forwarded by France could be used as evidence if it served the purpose of investigating serious criminal offences.

In France, the Court upheld the provisions of Article 706-102-1 of the French Criminal Code to authorise and execute the capture of data. Additionally, the Court decided that the capturing technique could be secret for reasons of national security. This ruling followed an earlier favourable decision by the French Constitutional Court on 8 April 2022.

In Italy, the Supreme Court of Cassation dealt with a referral from the lower tribunal of Rome, which denied a defendant's request to disclose information about the police methods used to acquire and decrypt SkyECC data. It was argued that since the material was acquired by Europol and foreign judicial authorities based on a European Investigation Order, the information could be used without any further scrutiny based on the presumption that the interception was legally carried out.

On the contrary, the Supreme Court of Cassation ruled that the encrypted messages obtained by Europol and foreign authorities could not be used in a pre-trial hearing unless prosecutors explained how such evidence was obtained. The Supreme Court explained that the principle of cross-examination implies a dialectical procedure, not only with regard to the screening of the acquired material, but also to the manner of acquisition of said material. According to the Supreme Court, a defendant should be able to question not only the content, but also the acquisition and investigation procedure of this material, in order to give full rights to the defence and in order to assess the relevance, reliability and demonstrative value of the evidence.

In addition to the above, in 2023 there appeared to be several other rulings by the Italian Supreme Court of Cassation concerning encrypted communication platforms like SkyECC and EncroChat, upholding the earlier positive decisions about validity and usability of acquired data in court proceedings.

In the Netherlands, the Supreme Court was asked for the first time to decide on the legality of the use of data from encrypted telephone communications. The Court ruled that the data transferred by Canadian authorities was legitimately used as evidence in a criminal proceeding. This decision concerned the hacking of the Antwerp Euroterminal in Belgium in 2020. Suspects were involved

in the large-scale import and trading of cocaine. The investigation started based on intercepted messages coming from EncroChat and SkyECC. The defence contested the legitimacy of the operations regarding these encrypted communication services. The Court found that these operations were legitimate and that they were carried out in accordance with national law.

In non-EU Member State Norway, the Supreme Court ruled in favour of an earlier decision by the Oslo District Court that material from an encrypted communication service (i.e. EncroChat) was allowed as evidence in a criminal case of drug trafficking. This decision was first upheld by the Norwegian Court of Appeal. The premise for the Supreme Court's conclusion was that the evidence had been legally acquired under French law.

These rulings can be seen as favourable for using captured encrypted data in court. This is also positive considering that law enforcement authorities in Germany and the Netherlands, supported by Europol and Eurojust, were able to dismantle an additional encrypted communication service used by criminals in February 2023[19].

Technologies

Quantum computing (QC)

This chapter aims to provide an overview of recent developments and to examine the potential impact of this field in the context of encryption. A more detailed analysis is available in Europol's Observatory report titled *'The Second Quantum Revolution: The Impact of Quantum Computing and Quantum Technologies on Law Enforcement'*[20].

STATE-OF-PLAY

The development of a universal quantum computer has progressed significantly recently. The past three years in particular have brought a substantial amount of research and innovation activity, and consequentially a number of new achievements and milestones as well. Despite this seemingly rapid pace of progress, there is still no quantum computer currently available with any proven quantum advantage for a relevant task, such as being capable of breaking modern cryptographic schemes. This is mainly due to the fact that three key technical challenges still need to be overcome for the successful development of a universal quantum computer[21].

The first challenge relates to the scaling up of the required hardware. A quantum computer at scale would be able to control around 1 million qubits in a computation, which would allow for a sufficient number of error-corrected qubits to carry out quantum algorithms in a real-life application. The highest number of qubits to date has been achieved by IBM's Condor, which counted 1 121 qubits[22]. According to IBM's roadmap, upcoming iterations will reach over 1 000 qubits in 2023 and over 4 000 by 2025.

The second challenge is to increase the speed for carrying out effective quantum operations. The speed of quantum computers can be quantified as the number of operations that can be executed per second and is generally understood to improve the overall performance of a quantum computer. However, as the number of algorithms (or 'gates') depends on the number of qubits used in a circuit, an increase in this area may introduce more errors and, thus, decrease the overall speed of the quantum computer.

This leads to the third and arguably most critical of these challenges: quantum error correction. As quantum systems are exceedingly sensitive to disturbances, the manipulation of qubits by quantum computers is prone to errors. While classical computers are able to detect and correct errors as part of their data processing activities, quantum computers are susceptible to errors as a direct result of interactions between the qubits and the environment within the quantum system. This concept is also known as decoherence and requires quantum error correcting codes to be employed to actively detect and correct errors in order to improve the overall accuracy of quantum computing processes.

A number of quantum computational devices are available today. However, while it is possible to run some algorithms on them, such as approximate routines like the quantum approximate optimisation algorithm (QAOA),

they are still far removed from the final stage of the development process. Current iterations are severely limited in the number of qubits they can process and suffer from significant error-proneness and noise.

The maturity of a quantum computer can generally be measured by its development stage. Devoret and Schoelkopf identified seven such development stages, with each advancement requiring mastery (and continued perfection) of the preceding stages[23]. The final stage, a fault-tolerant quantum computer, requires completion of all previous stages and has to date not been achieved.

Recent progress in the research and development of quantum technologies coincides with significant public and private investments. In 2022, global investments reached more than EUR 32.6 billion, 85% of which came from the public sector[25]. Around EUR 6.6 billion of investment has been made in the European Union, with Germany, France, and the Netherlands putting the most resources into this field.

An important part of this progress has been contributed by major technology companies, chief among them IBM, Google, Microsoft, Intel, and Honeywell. IBM, in particular, has produced significant achievements in pushing the boundaries of technological capabilities and presented an ambitious roadmap towards the development of a universal quantum computer. Several of these companies are already offering Quantum-as-a-Service (QaaS) to allow individuals to experiment with qubits.

IMPLICATIONS OF QC FOR ENCRYPTION

Universal quantum computers are going to have a significant impact on cryptography. The speedup achieved by Shor's and Grover's algorithms will effectively mean that the way sensitive information is protected today is going to be vulnerable to this type of technology. As a result, quantum computers are a type of dual-use technology that is going to have a substantial impact on crime, as well as the work of law enforcement. This impact includes the breaking of cryptographic protocols, weakening of passwords, as well as new digital forensics techniques.

STORE NOW, DECRYPT LATER

The concept of 'store now, decrypt later' refers to the possibility of criminals, state actors, and other entities harvesting sensitive encrypted information today, with a view to decrypting it in the future once universal quantum computers become available. This information could include databases, protected files, or communications data, and can lead to a significant increase in crime in the future, including ransom demands, fraud, and advanced phishing attacks. At the same time, 'store now, decrypt later' may offer an opportunity for law enforcement in later gaining access to encrypted evidence that is obtained now. While quantum computers may not be immediately universally accessible even once the technology is mature enough for this type of decryption, criminals may abuse available applications such as Quantum-as-a-Service. This concept highlights the critical importance to initiate a timely transition of relevant systems to post-quantum cryptography.

PASSWORD GUESSING

Quantum computers have the potential to significantly improve password guessing. As quantum computers can process multiple possibilities at the same time, the action of retrieving a password from its stored secure form can be carried out much faster. Specific algorithms for matching an input to a particular function, such as Grover's algorithm, for instance, could mean a substantial improvement compared to currently available technology. Given the importance of accessing password-protected evidence in the context of criminal investigations, this means in practice that law enforcement may be able to use quantum computers to improve its ability to investigate high-profile criminal cases. Key applications include the fight against terrorism and against child sexual abuse and exploitation, both of which have important digital components that typically require highly efficient investigation measures.

Improved password guessing capabilities of law enforcement may prompt criminal actors to adjust their use of passwords or to choose new hash functions. As the currently held notion of what can be considered a strong password is going to be fundamentally challenged by the advent of quantum computing, more complex passwords and biometric authentication measures may become more widely used in the future.

Quantum password guessing is an active field of research and, as such, the actual application of this approach will still need to be proven and translated into practice. Law enforcement will need to closely follow the progress of research and actively participate to be able to make the most of quantum password guessing in the future.

NEW DIGITAL FORENSIC INVESTIGATION TECHNIQUES

New quantum side-channel attacks could help law enforcement investigate quantum computers. At the same time, quantum computers could increase the success ratio of existing forensic analysis techniques. This includes facilitating the analysis of data extracted from an attack. Grover's algorithm could be used in this case to identify relevant data extracted during a side-channel attack in order to deduct the cryptographic key.

New forensic approaches facilitated by quantum computing are critical in the context of criminal investigations, as law enforcement needs to be able access relevant electronic evidence. With an increasing amount of criminal investigations involving some form of encryption, digital forensics can provide the key in the fight against serious organised crime and terrorism.

QUANTUM COMMUNICATIONS

Quantum communications refers to an already relatively mature application of quantum technologies. Leveraging the same technology behind designing qubits, quantum communications can facilitate the design of quantum computing networks, as well as specific areas of secure communication. These new means of communication rely mainly on quantum key distribution that would facilitate the use of highly secure communication. While law enforcement may use this technology to share sensitive information in the context of criminal investigations, criminal actors themselves may take advantage of the enhanced security provided by quantum communications to evade law enforcement detection.

Cryptocurrencies

BASICS OF CRYPTOCURRENCY (PUBLIC-PRIVATE KEY CRYPTOGRAPHY AND MINING)

Cryptocurrencies are inherently reliant on cryptography. Public key cryptography is particularly important for the functioning of cryptocurrencies. Bitcoin, for example, uses Elliptic Curve Digital Signature Algorithm (ECDSA) and SHA256 to make sure funds are spent only by the rightful owners i.e. holders of the private key. The public key is also used to derive public addresses, using a combination of cryptographic hashing algorithms. The private key needs to be kept secret by the user, as it is used to access wallets and sign transactions. The sharing or theft of the private key can lead to loss of funds and/or impersonation.

Mining is also an important concept for cryptocurrency that is heavily reliant on cryptography. The main mining models are proof-of-work and proof-of-stake. These cryptocurrency consensus mechanisms are used for processing transactions and for the creation of new coins. Mining also prevents the double-spending of funds on a blockchain as the process verifies the validity of transactions (i.e. that the coins are not previously spent). It is the backbone of cryptocurrency and enables such systems to function without centralised entities.

Different forms of mining have attracted various types of criminal actors. For example, mining rigs or farms have been used to launder funds (buying crypto-mining equipment with criminal proceeds) or to pretend that funds are legally earned and hide the criminal origin. Even when such purchases were not profitable, criminals can still run such mining operations as it can be a cover for illicit earnings. Furthermore, in some cases it might bring criminals further profits, i.e. newly mined cryptocurrency. Such behaviour has also been observed in mining pools, specifically abused by ransomware actors[24].

Also, for over five years already, botnet mining or cryptojacking has been used by criminals to abuse victim's bandwidth and processing power to mine cryptocurrencies[25]. Finally, pool mining schemes have also been used by scammers to run their Ponzi schemes. For example, the BitClub Network promised earnings through pool mining, while these pools did not actually exist[26]; defrauded investors lost hundreds of millions of euros [27].

STORING FUNDS: CUSTODIAN, NON-CUSTODIAN AND OTHER CRYPTOCURRENCY WALLETS

Cryptocurrencies are stored in addresses, which are alphanumeric text sequences used to receive and/or send funds[de]. To keep the funds secured, addresses are generally stored in wallets, which require private keys for access. One wallet may store any number of addresses and types of cryptocurrencies. There are mainly two types of wallets: custodial and non-custodial (or self-custody). Custodial wallets refer to wallets where the user does not hold their own private key, but the service does so on behalf of the user. This is very

d Example for Bitcoin: bc1p000c9n4k7gvv76any96p4vgn2epaqcfcde5jn8a0np3wrr7f70fsa9feym
e Example for Ethereum: 0xAb5801a7D398351b8bE11C439e05C5B3259aeC9B

common, as for example funds stored at centralised cryptocurrency exchanges[f] are custodial. The phrase 'not your keys, not your crypto' refers to such storage. While easy to use, there can be risks using custodians. As the company holds the private keys, the user has no cryptographic control over these funds. For law enforcement agencies, this can be beneficial as they can request exchanges and custodian wallet providers to freeze or seize cryptocurrency assets, when they have legal grounds to do so and the exchange cooperates with the law enforcement request.

Since the entry into force of the 5th Anti Money Laundering Directive[28], exchanges and custodian wallet providers offering exchange of cryptocurrency to fiat are required to implement user identification measures (termed 'know your customer' or KYC measures). Exchanges and non-custodial wallet providers also have to register in the EU countries in which they operate.

Non-custodial wallets refer to hardware and software wallets where the user has responsibility for their own private keys storage. This comes with 'great responsibility' as a loss of the private key means the funds are not accessible anymore. Furthermore, (accidental) sharing or theft of the private key can lead to permanent loss of funds when obtained by a criminal.

As private keys are complicated non human-readable strings of alphanumerical text, mnemonic phrases were introduced in Bitcoin Improvement Protocol (BIP) 39[29]. A mnemonic phrase is a group of words, generally 12 or 24, which is used to access a wallet or several wallets. For example, if a user creates a wallet with a Trezor or a Ledger[g], a mnemonic phrase may be created. This phrase will work on any similar hardware device and give the user access to the funds from anywhere, even when the original hardware wallet is broken or lost. This also means that when law enforcement obtains the mnemonic phrase of a suspect in a house search for example, they can access and seize the funds. However, BIP38[30] allows for an extra password on top of the private key (mnemonic phrase). This may demand additional password guessing from law enforcement when trying to access a suspect's wallet, even when the mnemonic phrase is known.

Another development is SLIP39 or Shamir Backup[31], implemented for example by hardware wallet Trezor Model T, which allows for the creation of a user-set amount of recovery shares, instead of one single mnemonic phrase. Every recovery share is 20 words and a user-set number of them is needed to restore a wallet. This could for example mean that a user creates five shares, out of which three are needed to access a wallet. If all these shares are stored in different locations, law enforcements' task of recovering a (criminal) wallet can be complicated significantly.

Non-fungible tokens (NFTs) are digital goods that are unique, tradeable and (partly) stored and searchable through a blockchain. While pictures online can be easily copied, in the case of NFTs the cryptographic data on the blockchain determines ownership. NFTs are often stored in hardware or software wallets, similar to cryptocurrencies.

f For example: Binance, Coinbase, Kraken, Bitstamp

g Brands of hardware wallets

DATA OBFUSCATION OF CRYPTOCURRENCY TRANSACTIONS

While the majority of cryptocurrencies' transactions, addresses, blocks, timestamps and other data are publicly visible in blockchains, some cryptocurrencies obscure such visibility. These cryptocurrencies are generally referred to as privacy coins, of which Monero, Zcash and Grin are examples. Monero, introduced in 2014, is the most commonly used privacy coin. Despite its privacy features, Monero has not overtaken Bitcoin in popularity amongst criminals. This may be the case due to the higher liquidity of Bitcoin and other cryptocurrencies. Also, Monero has been delisted at many exchanges[32] because the origins of funds cannot be determined, which leads to a lack of compliance with anti-money laundering rules.

There are also cryptocurrencies where enhanced encryption is optional. One example is Dash, where it is possible to enable a 'PrivateSend' function, a method akin to mixing, complicating the tracing of the origins of funds[33]. Mimblewimble is another cryptographic blockchain protocol allowing for private transactions. It relies on elliptic-curve cryptography, which allows for the verification of transactions without revealing information. Litecoin implemented Mimblewimble as an optional feature, while other coins such as Grin and Beam use it for every transaction. Litecoin users can move their funds into 'extension blocks', which leads to concealment of addresses and amounts[34]. For Grin and Beam there are not even public blockchain explorers, as the Mimblewimble protocol uses a 'blinding factor' for its transactions. This encrypts the inputs and outputs of every transaction, along with both sender and receiver public and private keys. Mimblewimble uses a multi-signature model and puts several inputs and outputs in a block, which allows for the aggregation of all transacting parties. In this case, only the sum of transactions has to be verified, which makes it unnecessary to store individual addresses and amounts[35]. As law enforcement agencies usually trace cryptocurrency from address to address, this is a complicating factor. However, transactions using Mimblewimble are not frequently encountered.

Zero-knowledge proofs and layer 2 solutions also allow for transactions to take place without showing (some of the) transactional data publicly. Zero-knowledge cryptography allows for the verification of information without revealing any information publicly. With the privacy coin Zcash, this is already used to ensure a wallet's balance and transaction history is accurate without revealing the balance and transaction history on a public blockchain[36]. Mixer Tornado.cash[h] has also been using zero-knowledge proofs to enable users to withdraw funds from the mixer without revealing what their original deposit was[37]. This significantly complicates tracing the origins of (illicit) cryptocurrency for law enforcement.

Finally, there are many developments on so-called 'layer 2' that lead to advanced encryption of cryptocurrency transactions. Layer 2 solutions are systems or protocols built on top of blockchains. The lightning network is perhaps the most well-known example. The lightning network[i] is a layer 2

h Tornado.cash as a mixing service and two of its developers have been sanctioned by US OFAC, one of whom has been arrested in the United States. The Dutch FIOD has arrested another developer of Tornado.cash on the suspicion of involvement in concealing criminal financial flows and facilitating money laundering through the mixing of cryptocurrencies.

i Channels on the lightning network can be explored with public explorers, such as: https://mempool.space/lightning

solution for the Bitcoin blockchain that aims to lower transaction fees and increase speed by creating payment channels. The two-party multisignature payment channels will not broadcast all transactions to the blockchain, but only the opening and closing of the channel. Layer 2 solutions are also being developed on other blockchains and might cause additional problems for law enforcement investigations.

IMPLICATIONS FOR LAW ENFORCEMENT

In the majority of cases, LEAs investigate cryptocurrency addresses appearing on public blockchains. However, there are several trends aimed at obscuring the visibility of cryptocurrency transactions. Mixers and privacy coins have been complicating tracing for years, but Mimblewimble and zero-knowledge proofs are relatively new developments that can also obscure the visibility of cryptocurrency addresses, balances and transactions. Furthermore, layer 2 solutions such as the lightning network might also be abused by criminals. This can be used, for example, to make payments to each other without making times and amounts of these payments visible. Similarly, new wallet encryption schemes may also complicate lawful access by law enforcement.

Law enforcement authorities are advised to stay up to date on such developments to be prepared when they are encountered in investigations. All of these developments can still be investigated by law enforcement authorities, when access to the private keys of the suspect are gained. This will not change with new encryption schemes and investigative opportunities will keep arising.

Biometric data

In recent years, significant progress has been achieved in this field, especially within the protection approaches belonging to the category of “biometrics in the encrypted domain”. Among all biometric encryption methods reported in the literature, these aforementioned algorithms are the ones that have clearly shown a greater potential for their deployment in real-world scenarios so far. In particular, great advancement has been accomplished in the application of homomorphic encryption to biometrics, thanks to the increased investment in human and funding resources devoted by research and industry. This has resulted in a clear increase in the level of maturity of this technology, which is now close to being applicable for the protection of operational large-scale IT systems.

LEGAL FRAMEWORK FOR THE PROTECTION OF BIOMETRIC DATA

The deployment of biometric recognition[j] technology, both for public and private sector applications, has seen a significant increase over the last two decades. Currently, it is not an overstatement to say that identity management based on automatic biometric recognition is ubiquitous and an integral part of our daily lives in various contexts, such as National ID cards, passports, banking transactions, physical or device access and multiple recognition processes

j In order to avoid a too-lengthy section, we refer the readers that are not familiar with biometric technology to standard ISO/IEC 2382-37:2022, that establishes the harmonised biometric vocabulary and includes the definitions of all biometric-related terms used throughout the present text.

within the law enforcement context. Such a wide deployment of biometrics has raised privacy concerns regarding the storage and use of biometric data. As a result, biometric data is defined as sensitive personal data within the established legal framework defined by the European Union (EU) General Data Protection Regulation 2016/679[38] (GDPR), the EU Institutions Data Protection Regulation 2018/1725[39] and the Data Protection Law Enforcement Directive 2016/680[40]. This legal framework establishes that the use of this data is subject to the right of privacy preservation and requires that organisations and authorities create explicit guidelines to prevent any form of misuse or unauthorised access to biometric data.

POINTS OF VULNERABILITY OF BIOMETRIC SYSTEMS

Given the legal obligations regarding biometric data presented above, it is important to identify the main vulnerabilities of biometric systems that attackers may take advantage of. This will allow developers to devise the necessary protection methods that guarantee, to the greatest extent possible, that data processing complies with the legal requirements.

As presented in the ISO/IEC 30107-1:2016 standard[k], attacks on biometric systems can be performed in two domains:

1. in the physical domain, also referred to as "direct attacks" or, in the more extended and common terminology, "presentation attacks";
2. in the digital domain against some of the internal modules of the system, also referred to in the literature as "indirect attacks".

This categorisation, together with a diagram of a generic biometric system and its potential vulnerability points, is presented in Fig. 1 (adapted from ISO/IEC 30107).

It should be noted already at this stage that encryption in biometrics represents a protection method mainly against attacks in the digital domain (as represented in Fig. 1). Other countermeasures need to be specifically designed for attacks taking place in the physical domain, such as the widely studied Presentation Attack Detection (PAD) methods.

k ISO/IEC 30107-1:2016 Information Technology – Biometric presentation attack detection – Part 1: Framework

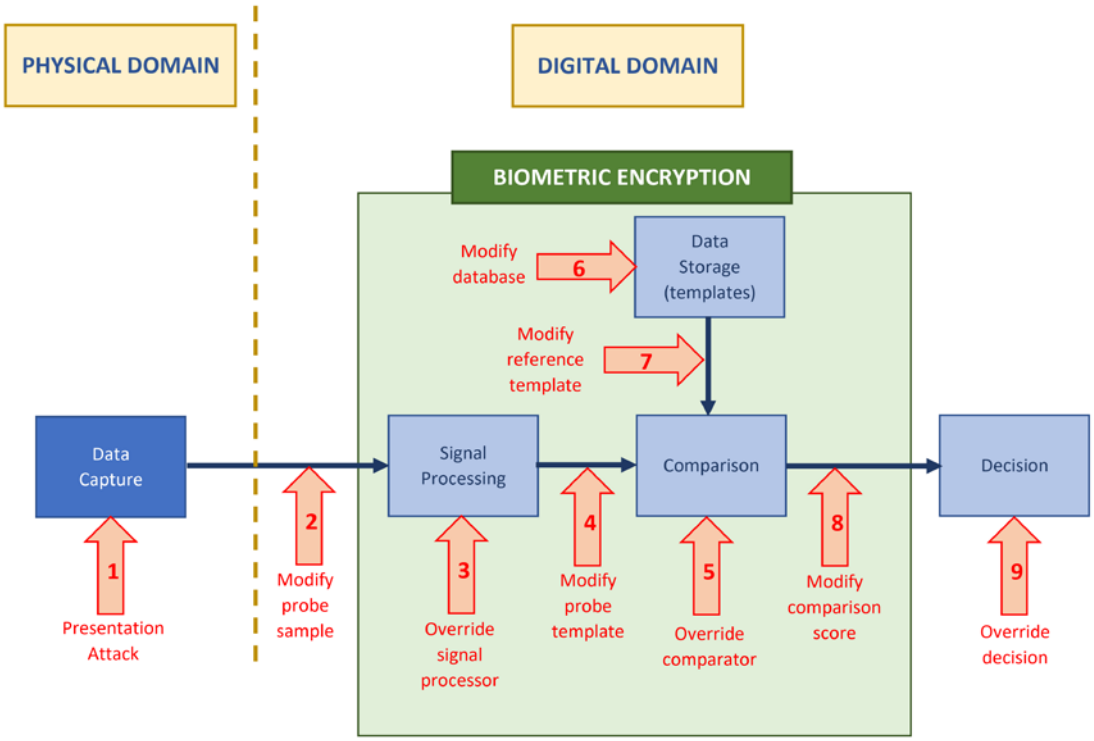

Figure 1. Diagram showing a generic biometric system and its main vulnerability points in the physical and digital domains. Encryption in biometrics represents a form of protection against attacks in the digital domain.

TECHNICAL REQUIREMENTS FOR THE PROTECTION OF BIOMETRIC DATA

The previous two subsections have outlined the legal provisions defined by the current data protection regulation and the potential vulnerabilities of biometric systems. Based on these premises, the ISO/IEC 24745 international standard on biometric information protection[l] has established two main technical requirements for protecting biometric templates: ***irreversibility*** and ***unlinkability***. This international standard states that, in order to protect the privacy of individuals, "knowledge of the transformed biometric reference cannot be used to determine any information about the generating biometric sample(s) or features", which makes clear reference to the necessity of storing irreversible biometric templates. Not only that, the ISO/IEC standard continues by stating *"[. . . and] the stored biometric references should not be linkable across applications or databases"*. That is, protected templates are not only required to be irreversible, but also unlinkable, in order to avoid the possibility of launching cross-matching attacks among different systems. Only by fulfilling both requirements (i.e. irreversibility and unlinkability), can we grant the privacy to which subjects are entitled.

Additionally, due to the fact that biometric characteristics cannot be replaced, renewability is also desired. Renewability is analogue to the unlinkability concept, but it is related to the time dimension — that is, to the ability to renew enrolled templates in one specific application at different points in time (i.e. if one template is lost or stolen, a new one, not matching the old template, should be issued). At the same time, other properties such as verification

l ISO/IEC 24745:2022 Information Security, cybersecurity and privacy protection – Biometric information protection

accuracy, speed and storage requirements should be maintained compared to the same system using unprotected data. It is important to note that all these requirements apply both to biometric samples as well as biometric templates.

WHY NOT USE TRADITIONAL ENCRYPTION APPROACHES?

The current report provides a comprehensive overview of traditional encryption methods. These approaches, designed to protect deterministic data (i.e. alphanumerical data), are unsuitable for protecting biometric data due to the intrinsic probabilistic nature of biometric samples stemming from the inherent intra-class variance of biometric characteristics. More precisely, biometric variance prevents the usage of symmetric cryptography and traditional hash functions with biometric input data since slight changes in the unprotected domain automatically leads to drastic changes in the protected domain. Consequently, the use of conventional cryptographic methods does not enable permanent protection since it would require the decryption of protected biometric data prior to the comparison. In summary, while classical encryption methods could be used to protect biometric data while stored, these data would have to be decrypted at some point in the system, prior to their comparison for recognition purposes.

WHAT IS BIOMETRIC TEMPLATE PROTECTION (BTP)?

As a result of traditional encryption/protection technology not being directly applicable to biometric-based systems, a new research/development area within biometrics referred to as: Biometric Template Protection (BTP) has appeared in the last two decades, receiving great attention from the scientific community and industry. This specific field encompasses a class of technologies which are designed to permanently protect biometric reference data, allowing recognition comparisons to take place in the encrypted domain, respecting the different technical requirements defined previously such as irreversibility, unlinkability and renewability. In contrast to conventional biometric recognition methods, BTP schemes generate protected reference templates (while unprotected biometric data is discarded). Protected templates prevent reconstruction attacks (i.e., irreversibility), but nevertheless make it possible to perform a biometric comparison in the protected domain. Moreover, template protection schemes typically enable the incorporation of random parameters in the generation process of protected templates. Through this, protected templates become variable and can be changed, which protects against crossmatching attacks (i.e., unlinkability).

WHAT CATEGORIES OF BTP TECHNIQUES EXIST?

As already mentioned, the main goal of biometric template protection is to secure the privacy and confidentiality of biometric template data while providing satisfactory recognition performance. To reach this objective, BTP schemes generate pseudonymous identifiers (PI) from unprotected biometric data. Biometric comparisons are then performed via the pseudonymous identifiers while unprotected biometric data is discarded.

Even though the abovementioned overall purpose and methodology are shared by all BTP algorithms, depending on the implementation, these protection schemes can be broadly divided into three categories, as shown in Figure 2:

cancellable biometrics, biometric cryptosystems and biometrics in the encrypted domain.

These categories differ in their protection techniques, such as non-invertible transformation used by cancellable biometrics, key binding/generation employed in biometric cryptosystems, and operations on ciphertext conducted by biometrics in the encrypted domain.

The selection of a given protection technique depends on each specific application and the desired balance between security, convenience, accuracy, processing/computational power and response time. Each of the three aforementioned categories presents its own unique properties, advantages and drawbacks.

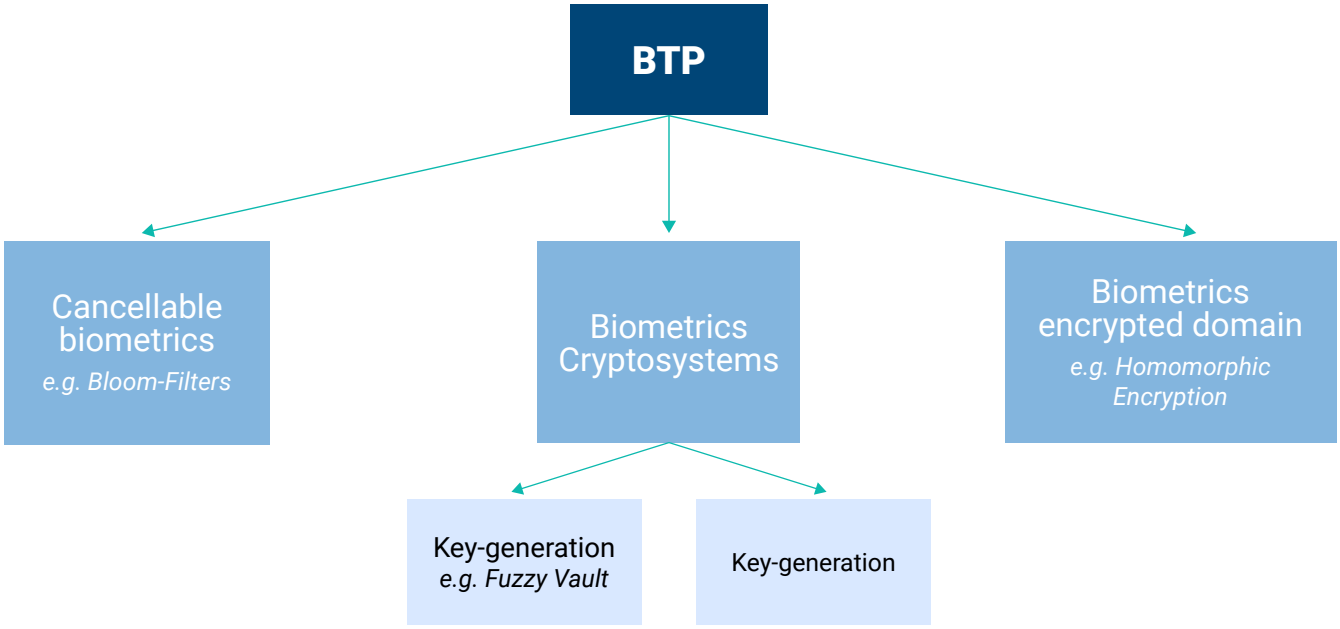

Figure 2. Summary of the three main categories of BTP methods proposed in the literature: cancellable biometrics, biometric cryptosystems and biometrics in the encrypted domain. The most successful and popular algorithms for each of the categories (mentioned in the text), are included as examples.

WHAT IS THE BTP CATEGORY: CANCELLABLE BIOMETRICS?

Cancellable biometrics, also referred to in the literature as feature transformation approaches, employ transformations in the feature or signal domains which enable a biometric comparison in the transformed (encrypted) domain[41]. Systems relying on cancellable biometrics do not store the original biometric data as templates. Instead, raw biometric data are transformed by a non-invertible transformation function in the enrolment phase, and the transformed data is stored in the database. Such a transformation is intentional and reproducible. An essential property of cancellable biometrics is irreversibility, meaning that it should be computationally unfeasible to retrieve the original biometric data from the transformed template. In the verification phase, the same transformation is applied to the query data. Matching is performed in the transformed domain so that no original biometric data is divulged. If the stored (transformed) template is compromised, a new version can be generated by altering the transformation parameters (meeting the renewability requirement).

Cancellable biometrics is considered relatively simple and easy to implement, yet to date these techniques have shown a significant degradation in accuracy performance compared to unprotected systems. Also, in many cases they require the use of auxiliary data during verification, which may be taken advantage of by a potential attacker.

The algorithms belonging to this category that have had the most success and have received the most attention by the biometric community are probably those based on bloom filters (BFs)[42]. As mentioned above, cancellable biometric systems suffer in general from a significant degradation in their recognition performance due to the use of non-invertible transformations (such as cryptographic hash functions) that hurt the biometric accuracy. Bloom filter-based BTP schemes partially overcome this drawback by taking advantage of the invariant property of BFs to conceal a distorted version of the raw biometric sample in a BF-based template and thus achieve diffusion of the statistical properties of biometric features while maintaining most of their distinctiveness.

WHAT IS THE BTP CATEGORY: BIOMETRIC CRYPTOSYSTEMS (BCSS)?

These methods, also referred to as helper data schemes, combine the benefits of biometrics and cryptography. In contrast to cancellable biometrics, in these approaches, secret keys are either technically tied to or directly produced from biometric data[43].

Due to the inherent biometric variance, it is not feasible to extract keys directly from biometric samples. As such, the majority of BCSs require the storage of biometric-dependent public information applied to retrieve or generate keys, which is usually known as helper data. Helper data (which must not reveal significant information about the original biometric templates) assists in reconstructing keys, and then comparisons are performed indirectly by verifying key validities, where the output of an authentication process is either a key or a failure message. Since the verification of keys represents a biometric comparison in the encrypted domain, BCSs are applied as a means of biometric template protection, in addition to providing biometric-dependent key-release. Based on how helper data is derived, BCSs are classified as either key-binding or key-generation systems.

- **Key-binding schemes:** Helper data is obtained by binding a chosen key to a biometric template. As a result of the binding process a fusion of the secret key and the biometric template is stored as helper data. Applying an appropriate key retrieval algorithm, keys are obtained from the helper data at authentication. Since cryptographic keys are independent of biometric features, these are revocable - while an update of the key usually requires re-enrolment in order to generate new helper data.
- **Key-generation schemes:** Helper data is derived only from the biometric template. Keys are directly generated from the helper data and a given biometric sample. While the storage of helper data is not obligatory, the majority of the proposed key-generation schemes do store helper data (if key-generation schemes extract keys without the use of any helper data, these are not updatable in case of compromise). Helper data-based key-generation schemes are also referred to as “fuzzy extractors” or “secure sketches”. A fuzzy extractor reliably extracts a uniformly random string from

a biometric input, while the stored helper data assists the reconstruction. In contrast, in a secure sketch, helper data is applied to recover the original biometric template.

The most popular and analysed BCS, which belongs to the key-binding category, is likely the fuzzy vault scheme, which was first introduced in 2002. Similar to the drawbacks presented by the algorithms belonging to the cancellable biometrics category, BCSs, as of today, present two main shortcomings:

1. performance degradation with respect to unprotected systems;
2. they require auxiliary data for verification purposes.

Attacks on this auxiliary data can potentially disclose sensitive information, which could compromise both the security of the system and the privacy of the subject.

WHAT IS THE BTP CATEGORY: BIOMETRICS IN THE ENCRYPTED DOMAIN?

As an alternative to the previous two categories, methods referred to as biometrics in the encrypted domain make it possible to compute operations directly in the encrypted domain. These are functionally equivalent to those in the plaintext domain, and thus enable the estimation of similarities between protected templates without having to decrypt them at any point and without the need of any auxiliary data. The result of the encrypted computations decrypted to plaintexts are equivalent to the results of the operations that would have been carried out on the original plaintext. Given that the result of the computations remains encrypted and can only be decrypted by the data owners, confidentiality is kept and any third party can operate over the ciphertext without accessing the original plaintext. Therefore, combining these encryption approaches with biometric verification systems would meet the BTP requirements of irreversibility, unlinkability and renewability, while preserving verification performance.

These techniques are relatively new and promising compared to cancellable biometrics and bio-cryptosystems. Even though some BTP schemes in this category have been developed relying on techniques such as garbled circuits, the vast majority of them are based on some version of homomorphic encryption.

Homomorphic encryption (HE) is, as of today, the most promising technique for the development of different BTP approaches as it allows the processing of encrypted templates without decryption[47, 44]. The use of a secure HE scheme guarantees unlinkability, irreversibility and renewability under the constraint of the complexity of the underlying mathematical problem. Unlike classical BTP schemes, HE-based BTPs provide template protection even for a remote biometric recognition since an encrypted template can be sent over an unprotected public channel, as only the party holding the private key is able to decrypt it. Therefore, as in classical cryptographic key-based systems, using a proper key management strategy is one of the most important factors in the design of HE-based BTPs. HE allows a distributed comparison between the client and the server where only the party with the disclosure right is entitled to learn the recognition outcome. Therefore, HE-based BTPs are commonly classified according to their key management approach: either a single-key

HE, where the template is encrypted with the public key of one of the parties and is decryptable with its private key, or threshold HE, where the template is encrypted using a joint public key between the client and the server and is decryptable using their both partial private keys.

The main shortcoming of HE for biometric template protection is that the practical implementations of fully homomorphic encryption (FHE) schemes still remain a big computational challenge. As a result, in practice, most BTP approaches relying on HE use non-fully homomorphic encryption algorithms. These algorithms only allow a limited subset of operations in the encrypted domain which, in general, does not allow for the most accurate comparison algorithms to be implemented in the encrypted domain. This in turn results in a certain degradation of accuracy. However, with the constant increase of computational power, and especially with the advent of quantum computing, it is expected that fully homomorphic encryption algorithms will be implementable in practice. Therefore, BTP methods based on these techniques are expected to be completely operable and probably a definite answer to biometric protection and privacy in the future.

IS BTP BEING APPLIED TO DEEP LEARNING?

Today, deep learning represents the most popular and successful form of machine learning. Deep learning has revolutionised the field of pattern recognition, including biometric recognition. Biometric systems utilising deep learning have been shown to achieve auspicious recognition accuracy, surpassing human performance. However, this huge breakthrough in terms of biometric accuracy has come with some caveats, as the use of deep learning has been reported to impact different aspects of biometrics such as algorithmic fairness, vulnerability to attacks, and template protection[45].

Very recently, the first attempts have been made to directly incorporate biometric template protection into deep learning-based systems[46]. The key idea behind these approaches is to embed some randomness into neural network-based feature extraction methods. That is, the neural network itself serves as a pseudonymous identifier encoder taking a biometric sample and a random key as input. This can be achieved by introducing a key-based random activation of neurons, i.e. a random subnetwork selection, or random permutation. Such a randomised network can be applied subsequently to an existing network trained for biometric recognition. Alternatively, networks can be trained from scratch or pre-trained models can be adapted to achieve template protection properties. Moreover, researchers have suggested special loss functions that may even incorporate a comparison of keys.

The aforementioned concepts have mostly been applied to facial data. However, similar schemes have already been proposed for other biometric characteristics as well as multibiometric systems. While the reported results of these recently proposed methods are promising, they are still at a very initial development research stage and further work needs to be performed before they can be considered fully functional.

WHAT IS THE DIFFERENCE BETWEEN BTP AND PRIVACY-ENHANCING BIOMETRICS?

A new trend within biometric technology has recently appeared in the literature, referred to as privacy-enhancing biometric techniques. These methods do not directly fall under the category of biometric template protection. In contrast to traditional template protection schemes, these methods attempt to only remove (or conceal) soft-biometric information, such as gender or age, from biometric data, while leaving other identity-related information unchanged. In other words, these approaches could be seen as attempting to fulfil the requirement of irreversibility for soft biometric attributes while unlinkability or renewability are not intended properties.

WHAT ARE THE CURRENT CHALLENGES WITH BTP AND ITS READINESS LEVEL?

With respect to their design goals, BTP algorithms generally offer significant advantages compared to unprotected systems in terms of enhanced privacy and security, providing biometric recognition capabilities at a higher security level. However, two main challenges remain before reaching a readiness level that would enable BTP technology and the deployment of these techniques in fully operational large-scale scenarios:

- **Degradation of recognition accuracy.** On the one hand, BTP techniques which provide provable enhanced security/privacy still present a significant degradation in recognition accuracy with respect to the best unprotected systems.
- **Increase in the computational complexity and time**. On the other hand, the increased security also comes, in the vast majority of cases, at the expense of an exponential increase in the execution time and the computational power required to run such protected systems.

While BTP techniques have proven to have a great potential in the future, especially those based on homomorphic encryption, further research is still needed with regard to these two major shortcomings.

Another challenge that contributes to BTP algorithms reaching their full maturity and needs to be addressed is the development of clear standards and protocols for their proper, objective and fair evaluation. The proposal and generalised adoption of such evaluation standards will provide the basis to improve the two main current drawbacks described before.

Currently, the robustness of biometric template protection methods is commonly evaluated in terms of its ability to satisfy three criteria: recognition accuracy, irreversibility, and renewability/unlinkability.

In most cases, the metrics and plots used to evaluate the recognition accuracy of protected biometric recognition systems are the same as those used to evaluate standard (unprotected) systems. This is to be expected, since the incorporation of a BTP algorithm into a biometric recognition system does not change the system's aim, which is to provide automated identity recognition capabilities. These metrics and plots are clearly defined by the ISO/IEC

19795 standard[m] and provide a solid ground for the comparison of systems recognition capabilities, both protected and unprotected.

However, for the irreversibility and unlinkability criteria, there is still no common approach in most scientific literature for their evaluation. Regarding irreversibility, most evaluations of BTP techniques are largely based on theoretical assumptions and estimations, which may result in inadequate or misleading representations of the irreversibility in practice (especially in the worst-case scenario of a fully-informed attacker, which is the most difficult threat model outlined in the ISO/IEC 30136 standard[n]). Similarly, with regard to the renewability/unlinkability evaluation techniques among BTP methods, there is an overwhelming tendency to present theoretical statements implying the fulfilment of this criterion, as opposed to providing in-depth data-based and experimental-based analysis that back up the simple verbal claims. Although there exists an unlinkability evaluation framework[47], which is being considered by ISO for its formal standardisation in ISO/IEC 30136, thus far, it has only been used by a handful of researchers in their proposals for and assessments of BTP approaches.

Therefore, further efforts should be invested towards developing and adopting empirical and experiment-based evaluation protocols, both for the assessment of irreversibility and unlinkability. This would help the BTP community establish a more concrete (and unified) definition of what it means to satisfy the irreversibility and the renewability/unlinkability criteria in practice, while also helping to establish a clear comparison among the capabilities of BTP techniques.

Once an independent and fair evaluation framework has been established that would allow for the fair and objective comparison of BTP approaches, it will be up to the practitioners and system designers to select the most appropriate protection method for their particular business cases. This decision should be based on, mainly: level of protection provided (i.e., level of irreversibility/unlinkability), recognition accuracy, and processing time.

However, a trade-off between these different factors needs to be met. For large-scale applications, response time and computational power may be the key parameter to be considered, at the cost of allowing somewhat lower protection. For high-security applications, with small-to-medium datasets (e.g. access control for critical infrastructure), the protection level and accuracy may be favoured with respect to response time or computational capacity.

Domain Name System (DNS)

This chapter presents a brief introduction on the DNS protocol, and it describes all existing proposals (standard and experimental) for DNS encryption. Following the DNS introduction, we discuss the implications of DNS encryption from the law enforcement perspective.

m ISO/IEC 19795:2007 Information Technology – Biometric performance testing and reporting

n ISO/IEC 30136:2018 Information Technology – Performance testing of biometric template protection techniques

DNS PROTOCOL

The Domain Name System (DNS) is one of the backbones of the Internet (RFC1034 and RFC1035). In a nutshell, DNS provides the means to translate "human readable" addresses, like https://europol.europa.eu, to "computer readable" addresses, like "127.0.0.1" (IPv4) or "::1" (IPv6), allowing us to navigate through the Internet and local networks.

The Internet Assigned Numbers Authority (IANA) maintains a list of "well-known" ports, which are ports assigned to a specific protocol (e.g. port 53 is assigned to DNS; port 80 is assigned to HTTP, etc.). In practice, this means that DNS traffic is easily recognisable (e.g. all UDP messages to port 53 are DNS requests). Moreover, the messages are in plaintext and therefore their contents can be read.

DNS traffic is generated every time a user accesses a network resource, and in an automated manner by applications running in the background. The contents of DNS requests and their responses provide information regarding which services an individual is using and when these services were accessed. This data can be used, among other things, to identify users of illegal forums and services, such as command and control (C2) servers of criminal infrastructures.

The traffic patterns of DNS can provide insights into the habits of a suspect. For instance, continuous 24/7 traffic with repetitive patterns is an indication of activity generated by a computer, whereas clear patterns of 8-12 hours of random-like activity, followed by 12-16 hours of inactivity, indicate human actions. Moreover, the pattern along with the time zone might also provide clues of the location of the suspects.

In recent years, the Internet Engineering Task Force (IETF) has proposed different privacy preserving standards related to DNS, summarised in Table 1, which could affect how DNS data can support criminal investigations.

DNS OVER TLS AND DNS OVER HTTPS

The first proposal to protect the privacy of users is DNS over TLS (DoT), standardised by the IETF as RFC7858. This standard uses the well-known port number 853 and TLS to encrypt the content of the DNS messages. Shortly after DoT appeared, DNS over HTTP/S (DoH) was proposed, standardised by the IETF as RFC8484. DoH uses the standard HTTPS port 443 to send requests encrypted with TLS over HTTP, which make these requests almost indistinguishable from regular web HTTPS traffic.

Year	Reference	Name	Transport Protocol	Port	Encryption
2016	RFC7858	DNS over TLS	TCP	853 (DNS only)	TLS 1.2, 1.3
2017	RFC8094	DNS over DTLS experimental	UDP	853 (DNS only)	TLS 1.2
2018	RFC8484	DNS over HTTPS	TCP	443 (HTTPS shared)	TLS 1.2, 1.3
2022	RFC9250	DNS over QUIC	UDP	853 (DNS only)	TLS 1.3
	RFC9230	Oblivious DNS over HTTPS experimental	TCP	443 (HTTPS shared)	HPKE (RFC9180) + TLS 1.2, 1.3
	RFC9114 [HTTP/3]	DNS over HTTP/3	UDP	443 (HTTPS shared)	TLS 1.3
2023	draft-ietf-ohai-ohttp-09	Oblivious HTTP	TCP	443 (HTTPS shared)	HPKE RFC9180

Table 1. Summary of DNS encryption standards

OBLIVIOUS DNS OVER HTTPS

To further enhance the privacy of DoH, decoupling users from requests, the IETF proposed oblivious DNS over HTTP/S (ODoH) which is defined in the ***experimental*** RFC9230. In ODoH, messages are end-to-end encrypted between client and DNS server, but the messages are sent through a proxy service, typically provided by a third party provider (different from the DNS one). In this way, the proxy service is not aware of the contents of the message request and the DNS provider does not know the source IP address, since all requests come from the same IP address (i.e. that of the proxy service).

DNS OVER QUIC AND DNS OVER HTTP/3

QUIC is a protocol developed by Google to improve the performance of web communications, later standardised by the IETF as RFC9000. It uses TLS 1.3 to encrypt the communications.

In a similar way that DoT was created, the IETF also standardised DNS over QUIC (DoQ) as RFC9250 to send TLS 1.3 encrypted DNS messages over QUIC. DoQ reuses the well-known port 853 defined by the DoT standard.

HTTP version 3 (HTTP/3) is standardised under RFC9114. It uses QUIC as underlying protocol to send and receive DNS messages over HTTP using TLS 1.3. The latest privacy enhancing proposal for DNS is using DNS over HTTP/3[48], the equivalent to DoH for HTTP v3 (instead of v2), using QUIC and TLS 1.3. As in the case of DoH, DoH/3 messages cannot be easily distinguished from HTTP/3 messages.

IMPLICATIONS FOR LAW ENFORCEMENT

As of today, the level of adoption of DNS encryption protocols remains low[49], but with a continuous and steady growth[50, 51].

DoT/DoQ and DoH/DoHTTP/3 propose two approaches to solving DNS encryption, each with its own respective implications for law enforcement. On one hand, DoT/DoQ uses a dedicated port number, 853, and on the other hand, we have DoH/DoHTTP/3, which reuses the well-known port 443, typically used for encrypted web traffic (HTTPS). DoT/DoQ traffic is easily identifiable through filtering by port 853, whereas the DoH/DoHTTP/3 approach makes DNS traffic almost indistinguishable from regular web browsing traffic. To distinguish between DNS requests and web browsing, we have to further analyse the traffic; for instance, we can use the destination IP address to identify the messages sent to IPs corresponding to DNS providers. Another option is to analyse the TLS handshake to obtain the Server Name Indication (SNI) and then compare it with a list of known DNS providers.

For LE purposes, DoT and DoQ still allow LEAs to obtain information from traffic patterns, since DNS traffic can be easily identified (filtering by port 853). However, this hinders its ability to lawfully access the DNS messages, since the contents are encrypted with TLS. To obtain insights on the contents of DNS messages, LEAs require the collaboration of the DNS providers.

In the case of DoH and DoH/3, LEAs cannot easily obtain information from traffic patterns since it is more difficult to distinguish regular web traffic (HTTP/2 or HTTP/3) from DNS traffic. Moreover, since the messages are encrypted, the contents are also not available for analysis. The only solution for LEAs to use DNS traffic is for the DNS providers to collaborate. One possible path to address the collaboration between LEAs and DNS providers would be to allow LEAs to send lawful requests to DNS providers in order to obtain the DNS traffic data.

The biggest challenge for LEAs in using DNS information in criminal investigations comes from the experimental ODoH. In this case, LEAs could leverage the traffic pattern information with the collaboration of the provider of the proxy service, but they will need the collaboration of both providers (DNS service and proxy service) to be able to obtain information regarding the contents of a suspect's DNS requests.

Even though in some cases (DoT and DoQ) LEAs can still identify DNS requests and obtain some information from them, they cannot access its contents because they are encrypted. The introduction of DNS encryption requires enhancing the existing collaboration between DNS providers and LEAs to leverage DNS data in criminal investigations. The extension of collaboration between DNS providers and LEAs should include the means for LEAs to request the contents of DNS messages and DNS activity.

CRIMINAL ABUSE OF DNS ENCRYPTION

Criminals are already abusing DNS encryption to support their activities. In particular, there are reports[52] of criminal abuse on the following domains:

- **Command and control communications.** This is also a typical use case for plaintext DNS, where fake DNS request/response messages are used by malware to communicate and receive commands from C2 servers. Encrypted DNS increases the advantages of using this channel, since the contents cannot be analysed. Moreover, in the case of DoH, these communications cannot be easily distinguished from regular web traffic.

- **Covert channel/data exfiltration**. Since the contents of DNS encrypted messages are not available for inspection, malware can use them to send data outside the infected machine to a remote host without being detected.
- **Unintentional usage**. Researchers[53] have also reported the unintentional abuse of DNS encryption by malware applications when DNS encryption is enabled at OS level (DoT/DoQ) or at web browser level (DoH, DoH/3). In this case, the malware will use DNS encryption even without being aware of it.

Telecommunication technologies

LAWFUL INTERCEPTION IN 5G NETWORKS

A home routing or a roaming scenario is a situation where a mobile phone user travels to a country different from the country where the user has a mobile subscription. In this case, the mobile phone user can only connect to mobile networks of the visiting country which have a roaming agreement with the user's mobile network operator (MNO).

In 5G standalone (5G SA) communications, the IP Multimedia Subsystem (IMS) allows the transmission of voice calls (among other services) as data. The encryption of IMS voice calls is negotiated during the call setup through the signalling channel and if agreed, the IMS voice call is transmitted through the data channel, encrypted from the caller user equipment (UE) to the recipient UE. This process is under the control of the MNO of the public land mobile network (PLMN) to which the UE is connected, therefore the MNO is able to comply with lawful requests to access data if needed.

In the case of roaming where the UE connects to a Visitor PLMN (VPLMN), the negotiation is under the control of the MNO of the Home PLMN (HPLMN), which can be a problem in case of a request to access data if the HPLMN operates in a foreign country. This effectively means that individuals within national borders can no longer be intercepted when using a foreign SIM card, unless the foreign service provider (which issued the SIM card) cooperates with the domestic service provider and prosecuting authorities. This scenario is even more problematic where the service provider operates in a country outside the EU or does not want to comply with the request. This situation is not new to 5G, it is also present with VoLTE roaming in 4G networks.

Ensuring EU LEAs' capability of lawfully requesting data from MNOs would necessitate a requirement to disable IMS encryption and other privacy-enhancing technologies in roaming scenarios. This would need to be a mandatory part of roaming agreements between MNOs. In this situation, in the case of a lawful request to access data where the HPLMN does not want to or cannot comply, the VPLMN would still be able to carry out the request. This solution does not affect the integrity of the IMS voice calls, nor the network level encryption that protects the data channel between the VPLMN and the HPLMN.

SUBSCRIBER IDENTITY IN 5G NETWORKS

In 4G networks and earlier, law enforcement agencies were able to obtain the subscriber identity information, the international mobile subscriber identity (IMSI), directly from the PLMN since the IMSI was transmitted in clear text. In 5G, the subscriber identifier is called the subscription permanent identifier

(SUPI) and it is always sent encrypted[o]. The encrypted version of the SUPI is called the subscription concealed identifier (SUCI).

The encryption of the SUPI is a challenge for LEAs. In order to request lawful access to data, the LEA must provide the MNO with the suspect's permanent identifier, either the IMSI in 4G or the SUPI in 5G.

This challenge is partly addressed from 3GPP Release 16, which introduced the LHQ_I interface which allows LEAs to send a request with a temporary identifier, obtaining the permanent identifier as a response. What the standard does not define is how the LEAs can obtain the temporary identifier.

To address this problem, LEAs require a legal framework allowing them to connect to a protected interface in the MNOs network. From there they can obtain the temporary identifiers, and later use them in a LHQ_I request to obtain the permanent identifier (SUPI) of suspects.

Moving forward, it is crucial that law enforcement agencies are involved in creation of international standards for new technologies. This would help ensure that the architectures are designed in a way that maintains capabilities to carry out investigative activities.

o There is an exception, for user equipment using legacy SIM cards without storage support for home network public keys

Machine learning (ML) and artificial intelligence (AI)

USAGE OF ML AND AI IN CRYPTOGRAPHY

The use of machine learning (ML) on cryptography is in itself not a new concept, with one of the first mentioned examples dating all the way back to 1991[54]. Since then, the number of scientific publications and applications of ML algorithms in cryptography has been constantly growing. Following a significant increase of data availability and computational power, ML (and as a consequence also AI-based systems) are now becoming increasingly more accurate; consequentially they are becoming increasingly relevant to and present in all aspects of our lives. As a result, ML and AI also have a substantial impact on cryptography.

STRENGTHENING ENCRYPTION

In symmetric cryptography, AI is used to design S-boxes from vectorial Boolean functions and to study their cryptographic properties in order to select the most efficient and the most secure schemes[55, 56]. In asymmetric cryptography based on RSA, AI can be used to generate safe primes for the RSA modulus and to generate safe public and private keys by running the known attacks such as factorisation, small private key attacks, partial key exposure attacks, and side-channel attacks. RSA is vulnerable to side-channel attacks and artificial neural networks can be used to test the RSA cryptosystem and its implementations against side-channel attacks before deployment[57].

WEAKENING ENCRYPTION

In addition to strengthening existing cryptographic applications, ML and AI can also be used for the purposes of cryptanalysis, which is the study of cryptographic schemes for vulnerabilities. Specifically, there are mainly two methods of deploying cryptanalysis: mathematical and side-channel. Mathematical cryptanalysis, or algebraic cryptanalysis, consists of breaking cryptographic schemes by scrutinising their mathematical properties, often through cryptographic algorithm identification. On the other hand, side-channel cryptanalysis consists of studying and manipulating the implementations in order to collect information on the keys or on the plaintext itself[62].

CRYPTOGRAPHIC ALGORITHM IDENTIFICATION

Identifying cryptographic algorithms is one of the essential steps for key recovery and it is useful in the application of cryptanalysis. If the algorithm is identified, it can help to develop techniques to break the encryption and recover the plain text.

ML techniques can be used to identify the cryptographic algorithm based on the features of the ciphertext. Additionally, the ciphertext can be analysed to look for patterns that are characteristic of certain cryptographic algorithms. The ciphertext can also be compared with known ciphertexts that have been encrypted using different algorithms. For all these identification techniques, ML can be used following the block diagram shown in Figure 3[58].

Furthermore, there is a challenge that comes with the increasing complexity of network data and the increasing number of various cryptosystems and cryptographic algorithms in each category. Specifically, designing an identification scheme for a specific cryptographic algorithm in a multi-cryptosystem scenario has become an urgent problem to be solved, and continues to grow as a research hotspot[59]. Most of the known approaches rely on classical ML-based approaches. To name just a few:

- random forest and logistic regression for AES,
- DES,
- Blowfish,
- CAST and RC2 algorithms[60],
- XGB-LGBM ensemble learning methods that can identify 10 common block cipher algorithms with the overall accuracy of almost 90%[61],
- dynamic identification schemes that can adapt to various cryptosystem identification scenarios based on heterogeneous ensemble learning[62].

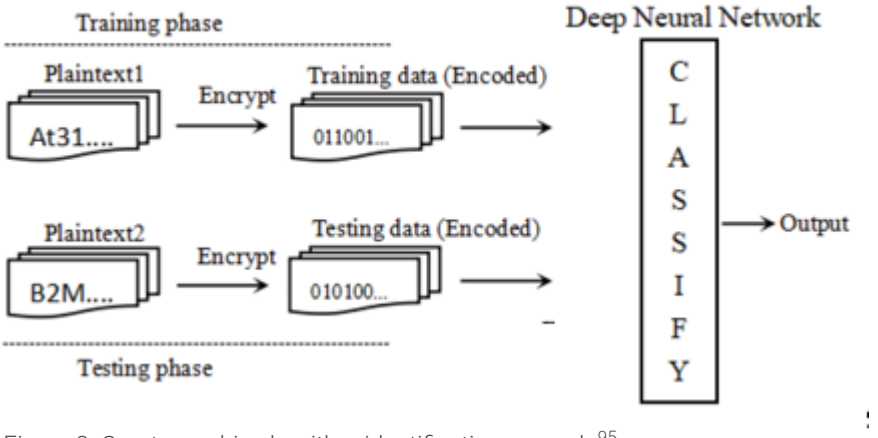

Figure 3. Cryptographic algorithm identification example[95].

In recent years, deep learning algorithms have been increasingly implemented in cryptanalyses[66, 63, 64].

SIDE-CHANNEL APPROACH

Common attacks on both symmetric and asymmetric cryptography are side-channel attacks (SCA), introduced by Kocher in 1996[65]. Various physical leakages such as timing delay[74], power consumption[66], and electromagnetic emanation (EM)[67] become available during the device's computation with the (secret) data. By combining the physical observation of a specific internal state within computation and a hypothesis on the data being manipulated, it is possible to recover the intermediate state processed by the device. Thus, it is possible to "break" the device.

Therefore side-channel analysis (SCA) differs from traditional mathematical cryptanalysis, which considers cipher algorithms as a black box where an analyst only knows plaintexts and ciphertexts. In SCA, the adversary can obtain not only the input and output of cipher algorithm but also some additional (physical) information, so SCA is considered as a *grey box model.*

There are various types of possible side-channel attacks depending on the cryptosystem and the device. Due to the characteristics of easy acquisition and processing, power and electromagnetism become the most commonly used kinds of information. Accordingly, many power-based (electromagnetism-based) SCA methods have been proposed, such as differential power analysis (DPA)[76] and correlation power analysis (CPA)[68], among others. Conventional side-channel attacks such as DPA and CPA are based on theories of cryptographic algorithms and signal processing and are an application of statistical analysis. Hence, the attacker would require prior knowledge in these scientific disciplines.

In recent years, there has been an increase in publications and datasets covering deep learning side-channel analysis (DL-SCA), both on software implementation targets[69, 70] and hardware implementation targets [71, 72] (see Figure 4).

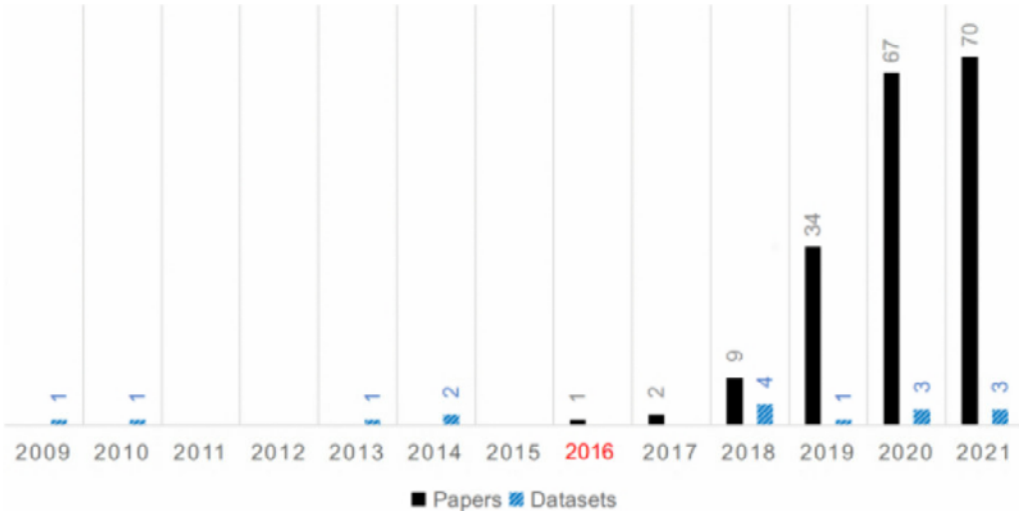

Figure 4. The distribution of papers in English and datasets per year that are used by deep learning-based side-channel analysis.[97]

An important reason why deep learning can be introduced into SCA is that the 'profiling' and 'attack' phases in profiled SCA can be theoretically transformed to the training and testing phases of deep learning. Namely, in scenario of profiled SCA, the attacker has access to a clone device which can be profiled for any chosen or known key. Afterwards, he is able to use the obtained knowledge to extract the secret key from a different device.

Profiled attacks are conducted in two distinctive phases; the first is known as the profiling (or sometimes learning/training) phase, while the second phase is called the attack (test) phase[73]. The profiling phase is particularly important as it establishes a probability function between the power consumption and corresponding intermediate values - that is, a power trace can be divided into different categories according to the intermediate value[74]. In the DL-SCA scenario, an attacker trains a neural network to identify a side-channel leak stemming from the cryptographic module and tries to unveil the secret key with the trained network.

As stated in the work of Picek et al.[75], the main disadvantage of using DL-SCA (and an inspiration for many research works) is the need to conduct hyperparameter tuning, which is considered an important and challenging task. Furthermore, it is not easy to choose which ML model to use, and a systematic

comparison on feature engineering techniques and model evaluation is still missing. Furthermore, there is a gap between academia and industry that uses more realistic targets and overfitting is one of the dominant problems. Nevertheless, DL-SCA is very powerful and can break targets protected with countermeasures, and requires less (or no) effort to pre-process the side-channel measurements and prepare the measurements for the attack.

EU AI ACT

On the 9th of December 2023, Parliament and Council negotiators reached a provisional agreement on the Artificial Intelligence Act, the so-called AI Act. It is the world's first comprehensive AI law. It follows a risk-based approach, establishing obligations for AI based on its potential risks and level of impact. The AI Act classifies AI systems into four categories: minimal risk, limited risk, high risk and prohibited applications.

The applications of AI to encryption identified in this report (such as strengthening encryption, weakening encryption, cryptographic algorithm identification and side-channel attacks) are likely to fall in the first category, minimal risk AI systems, since they do not require any personal data and do not automate tasks with significant impact to end users.

Only the basic transparency requirements apply for minimal risk AI systems under the EU AI Act, which means they have to provide information on the data used for training and the logic behind the AI system.

Research and funding

RESEARCH AREAS CURRENTLY IN FOCUS

Three major areas where understanding future trends and technologies is important for policymakers in the Justice and Home Affairs (JHA) domain are the future of "user-controlled" encryption and its relation to digital forensics and decryption capabilities, the development of quantum computing, and the utilisation of encrypted data for the development of ML algorithms.

Encryption, privacy and digital forensics

In order to protect privacy, encryption technology is increasingly used in all areas of public and private life. Mobile phones are often a key factor in criminal cases (for example intrusions, personal data and intellectual property theft etc.). The data stored in these devices usually contains critical evidence associated with the above-mentioned types of crimes. However, encryption often renders access to, and the analysis of, criminal evidence extremely challenging or impossible in practice. Currently-used digital forensic tools have several limitations. For example, they operate as a black box, they do not always work on contemporary devices given the increasing number of data encryption mechanisms, and they are often not affordable.

Ongoing or just-finished EU projects in this area relevant for law enforcement agencies are EXFILES[p]- Extract Forensic Information for LEAs from Encrypted Smartphones, CERBERUS[q], and its follow-up project OVERCLOCK. The EXFILES project aims to provide LEAs with new tools to extract data and associated evidence from these devices in strict legal contexts. The CERBERUS project develops finely-tuned algorithms that utilise high-performance computers to crack passwords for devices seized during law enforcement investigations. In its follow-up project, OVERCLOCK[r], a set of guidelines on the appropriate handling of encrypted devices retrieved during the course of an investigation will be outlined, and a forensic tool to support the lawful access to data on sized devices will be developed. This tool will be made available on a dedicated secure platform restricted to EU law enforcement.

Not only are electronic devices and applications encrypting stored user data by default, but a growing number of communication channels and data storage services are also secured by end-to-end encryption[76]. An ongoing project that started in 2022, POLIIICE[s], will demonstrate an array of innovative LI measures at cloud, network and edge device level to overcome these challenges.

Quantum computing

The advent of a cryptographically significant quantum computer is only a matter of time, and it is already changing the threat landscape with adversaries downloading encrypted information to be decrypted once the technology is available ('store now, decrypt later'). This threat, as well as investigative

p Extract Forensic Information for LEAs from Encrypted Smartphones (https://exfiles.eu/)

q Child Exploitation Response by beating Encryption and Research to Unprotect Systems (https://www.forensicinstitute.nl/research-and-innovation/international-projects/cerberus)

r Operational Vanguard: using Encryption Research for Criminal LOCKdown (https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-details/31077817/101038710/ISFP)

s Powerful Lawful Interception, Investigation, and Intelligence (https://poliiice-project.eu/)

opportunities for law enforcement resulting from quantum computing, has been explored in Europol's recent report on quantum technologies[24] Among others, the report's recommendations highlight the need to foster research and development projects in this field. One of the research objectives of the POLIIICE project is the usage of quantum computing for decryption of LI, while quantum-resistant algorithms based on hardness of lattice problems are developed in the PROMETHEUS project[t]. Meanwhile, The National Institute of Standards and Technology (NIST) in the US has announced that four quantum-resistant algorithms are approved[77], three of them supported by European research organisations[78]. As there is a need to advance swiftly in the transition to quantum-resistant cryptography, EU funding schemes targeting this problem are available and new solutions are expected in the near future.

Furthermore, the other technology that can ensure quantum-resistant environments in the long term is quantum key distribution (QKD) that enables two parties to establish a security communication link using principles of quantum physics[79]. The European Commission has established EuroQCI[u] that will safeguard sensitive data and critical infrastructures by integrating quantum-based systems into existing communication infrastructures, providing an additional security layer with QKD. This initiative will make use of quantum communication technologies developed in the Quantum Technologies Flagship[v] and OPENQKD[w] project. Project PETRUS[x] will act as a link between all projects, industrial and national, within EuroQCI. These first projects under the Commission's Digital Europe Programme[y] will together make it possible to take the first steps towards services offering operational quantum key distribution (QKD), a highly secure way of delivering encryption key material.

The European Union is also supporting wider quantum research and expertise. The Quantum Technologies Flagship[80] is an EU-funded research and innovation initiative aimed at putting Europe at the forefront of quantum technologies. Launched in 2018 with an overall budget of EUR 1 billion, the initiative seeks to fund projects over a time span of 10 years in the areas of quantum computing, quantum simulation, quantum communication, and quantum metrology and sensing. The two most prominent projects developed during the first phase of the initiative are OpenSuperQ and AQTION.

- OpenSuperQ is a project of ten international partners from academia and industry that aims to design, build, and operate a quantum information processing system of up to 100 qubits[81]. One of the goals of the project is to then make it available centrally for external users.
- AQTION is a research project focused on developing and exploiting a robust, compact ion-trap quantum computer that is based on scalable hardware and widespread industry standards[82].

t Prometheus Project (https://www.h2020prometheus.eu/)
u The European Quantum Communication Infrastructure (EuroQCI) Initiative (https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci)
v Quantum Flagship (https://qt.eu/)
w Open Quantum Key Distribution (https://openqkd.eu/)
x Petrus Project (https://petrus-euroqci.eu/)
y The Digital Europe Programme (https://digital-strategy.ec.europa.eu/en/activities/digital-programme)

Encryption and ML/AI

The third area that is in focus of research due to increased usage of AI based systems and need for privacy preserving requirements is homomorphic encryption algorithms. Perhaps the most relevant ongoing project in this field is HARPOCRATES[z], which aims to design several practical cryptographic schemes (functional encryption and hybrid homomorphic encryption) for analysing data in a privacy-preserving way. Their focus of application is the medical field, but the results are transferable to LE applications. Additionally, the SENTINEL[aa] project aims to integrate tried-and-tested modular cybersecurity technologies with novel ideas, including an end-to-end digital privacy and personal data protection compliance framework for SMEs. Recent projects relevant to this topic, although also not specifically targeting LE applications but where results are transferable, are SDN-microSENSE[ab] privacy protection framework and the CyberKit4SME[ac], which provides a set of cyber security tools and methods to protect data being stored, processed or exchanged.

6G

Finally, it is important to invest in research and innovation development for 6G in relation to lawful access. The discussions on the global standards for 6G have been ongoing since early 2021. In June 2023, 6G took an important first step as the International Telecommunication Union — Radiocommunication Sector (ITU-R) put forward a Framework Recommendation for 6G (known as Draft IMT 2030[83]). On that basis, standards development organisations — including the 3rd Generation Partnership Project (3GPP) — will in mid-2025 start designing technologies that satisfy the vision suggested by the 6G Framework. These will be submitted roughly 3 years later to ITU-R as candidate technologies. 6G networks could launch in 2030 or so (or possibly a little earlier in Asia and other regions that were the first to introduce 5G), at a time where 5G standalone will be on its way to be fully deployed. In any case, most telecom firms will be conducting trials at that period, and phone manufacturers will likely start teasing 6G-capable phones at that point.

The European Smart Networks and Services Joint Undertaking (SNS JU[84]) - a public-private partnership supported by the European Commission to facilitate and develop industrial leadership in Europe in 5G and 6G networks and services – is shaping a solid research and innovation roadmap and deployment agenda by for 6G. In that context NetWorld Europe put forward a strategic vision of 6G[85] as well as detailed technological orientations and priorities[86].

Amongst priorities is trustworthy 6G. Trustworthiness considerations rely to a large extent on encryption measures and cover all aspects of cybersecurity, including resilience against attacks, enhanced privacy, as well as end-to-end security by design that shall impact lawful access activities. Such research and innovation activities are supported by the SNS JU through open calls of interest for security practitioners[87].

z Harpocrates project (https://harpocrates-project.eu/)
aa Sentinel project (https://sentinel-project.eu/)
ab SDN-microSENSE project (https://www.sdnmicrosense.eu/)
ac CyberKit4SME ToolKit (https://cyberkit4sme.eu/cyberkit4sme_tools/)

GAPS AND RECOMMENDATIONS

Regarding quantum-safe technologies, a transition plan to protect sensitive data from quantum computing attacks needs to be coordinated, with the most sensitive data having to be prioritised for migration. Post-quantum cryptography should be a key objective for stakeholders in the JHA domain, as well as wider society, in order to mitigate the aforementioned 'store now, decrypt later' threat.

Additionally, quantum networks use trusted nodes that receive information in quantum states, store them in classical states, and transmit them in quantum states again. This adds a new layer of vulnerability as attackers could read and steal information once put back in zeroes and ones[92]. Hence, there is a need to develop quantum nodes to ensure long-range connections for QKD. OPENQKD offers a funding and collaboration network between European academia, industry and start-ups in field of QKD, while the EUROQCI project aims to become a backbone of secure communications in the future and will incorporate a space segment as part of the IRIS[2 88].

Gaining access to data at rest, either stored on devices or on communication providers' systems, remains a major challenge in law enforcement investigations. LEAs would benefit from tools that will assist password guessing to quickly decrypt data at rest. The European Commission will significantly increase Europol's decryption platform capacity in 2024. Furthermore, the European Commission proposes to foster the development of complementary solutions through targeted funding and building on the projects listed above.

Standardisation of new technologies is necessary to align the digital ecosystem. In order to achieve that, more contributions from experts are necessary, since law enforcement needs are not always taken into consideration when new standards are created. For example, end-to-end encryption poses problems to telecommunication operators when it comes to implementing lawful access obligations. The main challenge is to design solutions that would allow at the same time a lawful and targeted access to communications and that guarantees that a high level of cybersecurity, data protection and privacy.

FUNDING SCHEMES

The Digital Europe Programme (DIGITAL) is the central programme for digital in the Multiannual Financial Framework 2021-2027. It aims to stimulate the economy and drive the digital transformation of Europe. With its budget of EUR 7.5 billion, DIGITAL will provide strategic funding to support projects in, among other topics, cybersecurity, supercomputing, and AI. The funding will be available for entities from the EU Member States as well as other countries associated to the Programme.

However, for certain actions under the Digital Europe Programme referring to Cybersecurity, High-Performance Computing and AI, Data & Cloud, the participation of legal entities controlled from non-EU countries can be restricted, according to art. 12(5) and 12(6) of the Digital Europe Regulation[89]. This is also the case for legal entities established in the territory of an eligible country but controlled by a third country or by a third country legal entity. EEA EFTA countries are fully associated to the Digital Europe Programme and benefit from

a status equivalent to that of the Member States. The specific requirements for the individual call topics can be found in the respective call documents[ad].

DIGITAL will fund supercomputing in various domains, including:

- security applications with EUR 2.2 billion,
- cybersecurity coordination, tools and data infrastructures with EUR 1.6 billion,
- AI (including safe access and storage in trustworthy cloud infrastructure) with EUR 2.1 billion,
- design and delivery of specialised programmes and traineeships for future experts in key capacity areas, including cybersecurity and quantum.

The second relevant EU programme for cryptography and JHA is Horizon Europe[ae], which is the EU's key funding programme for research and innovation with a budget of EUR 95.5 billion. Legal entities from the EU and associated countries can participate in its funding schemes. Particularly interesting for the topic of this report is Pillar II, Cluster 3 "Civil Security for Society"[90], with Work Programmes 2021-2022[af], 2023-2024[ag] and 2025-2027. Within Work Programme 2023-2024[91], several calls for proposals that are relevant for the topic of this report are listed: Fighting Crime and Terrorism, Border Management, and Increased Cybersecurity. More specifically, the Commission allocated around EUR 11 million for research on PQC[92] via the Increased Cybersecurity topic.

DIGITAL and HORIZON EUROPE are jointly funding the EUR 1 billion Quantum Technologies Flagship initiative, which aims to fund over 5 000 of Europe's leading quantum technology researchers in the 2018-2028 period. Its long term vision is to develop a so-called quantum web in Europe, where quantum computers, simulators and sensors are interconnected via quantum communication networks. Quantum technologies are and will be supported by the proposed Horizon Europe programme for research and space applications, as well as the proposed DIGITAL programme. DIGITAL will develop and reinforce Europe's strategic digital capacities, supporting the development of Europe's first quantum computers and their integration with classical supercomputers, as well as a pan-European quantum communication infrastructure (see Figure 6). Alongside this, the Connecting Europe Facility[ah] (CEF) will provide funding for projects developing cross-border links between national networks, and interconnections with the EuroQCI's space component.

ad Funding & tender opportunities (https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/how-to-participate/reference-documents)

ae Horizon Europe (https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en)

af Horizon Europe 2021-2022 Work Programme 6 (https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/wp-call/2021-2022/wp-6-civil-security-for-society_horizon-2021-2022_en.pdf)

ag Horizon Europe 2023-2024 Work Programme 6 (https://research-and-innovation.ec.europa.eu/document/download/ed4ea470-af89-49d7-85c1-f9bb3039ccbd_en)

ah Connecting Europe Facility (https://cinea.ec.europa.eu/programmes/connecting-europe-facility_en)

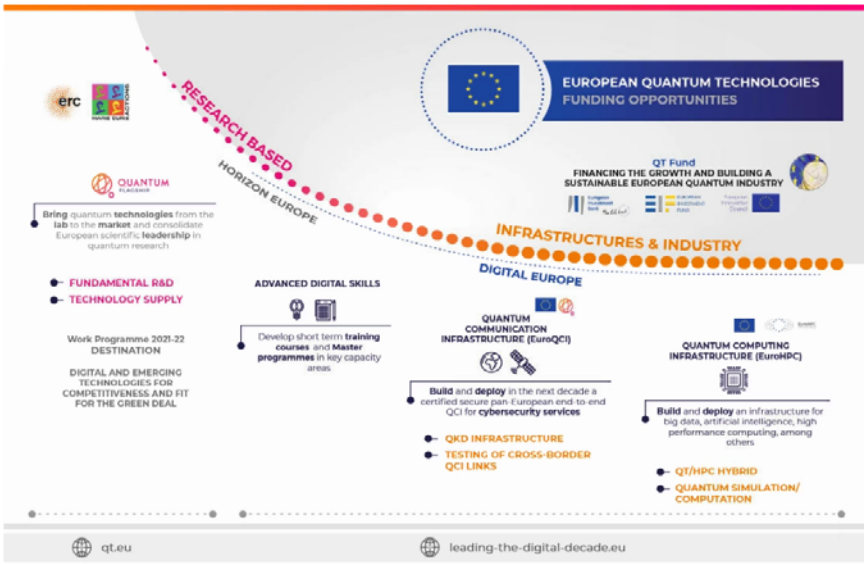

Figure 5: European Quantum Technologies – funding opportunities.[96]

The Internal Security Fund (ISF) is set up for period 2021-2027[93], with a total budget of EUR 1.93 billion. It aims to prevent and combat terrorism, radicalisation, serious and organised crime and cybercrime. In the Work Programme 2023-2025[94], and within calls for proposals for Digital Investigations, projects enhancing the capacity of law enforcement and/or judicial authorities to address the use of encryption by criminals and its impact on criminal investigations will be funded. Applicants can be from Member States participating in the ISF (all EU Member States excluding Denmark). Also eligible to apply are:

- public bodies or, by the competent authority's mandate, a public or non-public implementing agency or body of a Member State participating in the ISF,
- non-profit private entities,
- profit-making private entities (including non-public implementing agencies, industrial or service/consultant companies),
- international organisations.

Under the Work Programme's thematic facility component ***Actions implemented under shared management***, EUR 16.5 million will be allocated for the period 2023-2025. Among the topics targeted with these actions is cybercrime, with a focus on issues such as encryption and lawful interception, and non-cash-payment facilities (NCPFs). All Member States participating in the ISF are eligible to apply.

Conclusions

The presence of encrypted data in criminal investigations is steadily increasing and is expected to grow even more in the coming years. Many member states **have reacted to this trend with new or updated general legal provisions to help LEAs bypass encryption used by criminals to hide their activities.**

In recent years, the debate between the privacy of individuals and collective security and integrity of a person has matured to a more constructive discussion, although it remains an ongoing challenge. The key to success is to foster dialogue, cooperation and innovation to ensure that both individual rights and the need for lawful interception are respected.

The majority of EU Member States have general legal provisions in place concerning accessing encrypted information. Some EU Member States have recently **introduced amendments to existing national legislation in areas relevant for bypassing encryption,** as these newly-adopted pieces of legislation might offer additional opportunities to capture and use (encrypted) data. **Extended search capabilities and means for targeted lawful access could be beneficial in capturing encrypted data.**

Regarding European and international legislation concerning encryption, it appears the **recently adopted EU electronic evidence package** is a step in the right direction for access to digital information in cross-border criminal investigations and prosecutions. **Although the related regulation does not provide an obligation for service providers to decrypt data,** the anticipated faster transmission of requested data might prove beneficial considering the **differences in data retention periods in Member States, which in some cases are problematically short.**

Up to now, the majority of court rulings related to the use of evidence gathered from encrypted communication channels in courts appears favourable for prosecuting authorities. It is recommended to continue monitoring developments in this area,
as jurisprudence in this area might have a considerable impact.
The wider debate on the use or introduction of alternative means of bypassing encryption (e.g. client-side scanning) is another area that deserves continued scrutiny.

Technologies utilising cryptography continue to present challenges for law enforcement agencies. **Home routing in 4G and 5G networks creates problems** because individuals within national borders that use a foreign SIM-card can no longer be intercepted, unless the foreign service provider cooperates with the domestic one. **From a technical perspective, further research is required to reach a solution where both individual privacy and LI are respected. In the meantime, this problem can be solved by requiring that privacy-enhancing technologies are disabled in home routing.** LEAs also require a legal framework for using interception technologies for user identification (i.e. SUPI-catchers) in the next generation mobile networks (5&6G).

Cryptocurrencies continue to be popular with criminals for hiding their transactions and laundering criminal proceeds. There are currently various difficulties in finding the real identities of criminals, due to mixing services and non-compliant exchanges. Moreover, criminal adoption of **zero-knowledge**

proofs and layer 2 applications will further complicate law enforcement efforts to trace criminal funds. **Collaboration with academia and private industry is needed, so these trends can be monitored and novel tools can be created.**

Similarly, DNS encryption is an area of concern for the investigative powers as new approaches may create increased dependency on services providers' cooperation. This cooperation cannot always be guaranteed. **It is crucial that DNS encryption, if implemented, would allow law enforcement to access and process suspects' DNS traffic.**

The use of artificial intelligence and large language models is already standard practice in information technology and data science. These tools can help or hinder law enforcement efforts to fight serious organised crime. To continue to effectively carry out their duties, **LEAs need to have a legal framework, underpinned by robust and adequate data protection safeguards, in which they can leverage the same modern technologies as other stakeholders in the private sector and academia.**

Continued research on and development of biometric systems and quantum computing is equally as important, as the advancements made in these fields create many opportunities for enhanced security for citizens. As with any technology, there will be those who seek to bypass the security of systems or even weaponise them for criminal purposes. **Quantum computing can significantly improve investigative capabilities of law enforcement** when encountering encryption in the future. At the same time, it is critical that the transition to post-quantum cryptography is addressed with priority in order to protect European citizens from this pressing threat.

As technology progresses, new opportunities and challenges in the area of encryption will continue to arise. As such, it is vital **that relevant stakeholders in the JHA domain are aware of these developments and are provided with the means to stay on top of these technological advancements.**

List of acronyms

5G SA	5G Standalone
AI	Artificial Intelligence
BCS	Biometric Cryptosystems
BF	Bloom Filters
BIP	Bitcoin Improvement Protocol
BTP	Biometric Template Protection
C2	Command and Control
CEF	Connecting Europe Facility
CJEU	Court of Justice of the European Union
CJM	Cybercrime Judicial Monitor
CPA	Correlated Power Analysis
CSAM	Child Sexual Abuse Material
CSP	Communication Service Provider
DL-SCA	Deep-Learning Side-Channel Analysis
DMA	Digital Markets Act
DNS	Domain Name System
DOH	DNS over HTTPS
DOHTTPS3	DNS over HTTPS 3.0
DOQ	DNS over QUIC
DOT	DNS over TLS
DPA	Differential Power Analysis
DSA	Digital Sevices Act
E2EE	End-to-End Encryption
ECDSA	Elliptic Curve Digital Signature Algorithm
EECC	European Electronic Communications Code
EIO	European Investigation Order
EU	European Union
GDPR	General Data Protection Regulation
HE	Homomorphic Encryption
HLG	High Level Group
HPLMN	Home PLMN
IANA	Internet Assigned Numbers Authority
IETF	Internet Engineering Task Force
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
ISF	Internal Security Fund

JHA	Justice and Home Affairs
KYC	Know Your Customer
LEA	Law Enforcement Agency
LEON	Law Enforcement Operational Needs
LI	Lawful Interception
LLM	Large Language Model
ML	Machine Learning
MNO	Mobile Network Operator
NCMEC	National Center for Missing & Exploited Children
NCPF	Non-Cash Payment Facilities
NFT	Non-Fungible Tokens
NGO	Non-Governmental Organisation
ODOH	Oblivion DNS over HTTP/S
OS	Operative System
OTT	Over-The-Top
PAD	Presentation Attack Detection
PLMN	Public Land Mobile Network
QAAS	Quantum-as-a-Service
QAOA	Quantum Approximate Optimisation Algorithm
QC	Quantum Computing
QKD	Quantum Key Distribution
RCS	Rich Communication Services
SCA	Side-Channel Attacks
SMS	Short Message System
SNI	Server Name Indication
SNS JU	Smart Networks and Services Joint Undertaking
SUCI	Subscription Concealed Identifier
SUPI	Subscription Permanent Identifier
UE	User Equipment
VOLTE	Voice over LTE
VPLMN	Visitor PLMN

Endnotes

1 Eurojust (2023), Cybercrime Judicial Monitor – Issue 8, Eurojust, The Hague, ISBN: 978-92-9490-914-5, ISSN: 2600-0113, DOI: 10.2812/063826.

2 Loredana Crisan, Launching Default End-to-End Encryption on Messegner, Meta, 2023, https://about.fb.com/news/2023/12/default-end-to-end-encryption-on-messenger/

3 Council of the European Union, Council Resolution on Encryption - Security through encryption and security despite encryption, rev1, Council of the European Union, Brussels, 2020, https://data.consilium.europa.eu/doc/document/ST-13084-2020-REV-1/en/pdf

4 UK Home Office, G7 London interior commitments (accessible version), UK Home Office, September 2021 (updated December 2021), https://www.gov.uk/government/publications/g7-interior-and-security-ministers-meeting-september-2021/g7-london-interior-commitments-accessible-version

5 European Commission, High-Level Group (HLG) on access to data for effective law enforcement, Migration and Home Affairs, 2024, https://home-affairs.ec.europa.eu/networks/high-level-group-hlg-access-data-effective-law-enforcement_en

6 Directive (EU) 2018/1972 of the European Parliament and of the Council of 17 December 2018 establishing the European Electronic Communications Code, Official Journal of the European Union, 2018, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018L1972

7 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, Official Journal of the European Communities, 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32002L0058

8 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, Official Journal of the European Union, 2016, https://eur-lex.europa.eu/eli/reg/2016/679/oj

9 Council of the European Union (2023), Law Enforcement Operational Needs for Lawful Access to Communications (LEON) - Presentation by the Swedish Police and the Swedish Security Service, Council of the European Union. https://data.consilium.europa.eu/doc/document/ST-6050-2023-INIT/en/pdf

10 Europol and Eurojust (2021), Third report of the observatory function on encryption, European Union, Publications Office of the European Union, Luxembourg.Publications Office of the European Union, Luxembourg.

11 Eurojust (2023), Cybercrime Judicial Monitor – Issue 8, Eurojust, The Hague, ISBN: 978-92-9490-914-5, ISSN: 2600-0113, DOI: 10.2812/063826.

12 Police Hacking regulation abroad: A comparative law study into legal regulations and safeguards regarding the quality of data. WODC, 2023. https://repository.wodc.nl/handle/20.500.12832/3303

13 European Council of the European Union, Access to e-evidence: Council authorises member states to ratify international agreement, 2023, https://www.consilium.europa.eu/en/press/press-releases/2023/02/14/access-to-e-evidence-council-authorises-member-states-to-ratify-international-agreement/

14 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), Official Journal of the European Union, 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32022R2065

15 Regulation (EU) 2021/1232 of the European Parliament and of the Council of 14 July 2021 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse, Official Journal of the European Union, 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32021R1232

16 Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down rules to prevent and combat child sexual abuse, European Commission, Brussels, 2022, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2022:209:FIN

17 European Commission, E-evidence – cross-border access to electronic evidence, 2023, https://commission.europa.eu/law/cross-border-cases/judicial-cooperation/types-judicial-cooperation/e-evidence-cross-border-access-electronic-evidence_en

18 European Court of Justice, Case number C-670/22, InfoCrucia, 2024, https://curia.europa.eu/juris/documents.jsf?num=C-670/22

19 Eurojust, New strike against encrypted criminal communications with dismantling of Exclu tool, 2023, https://www.eurojust.europa.eu/news/new-strike-against-encrypted-criminal-communications-dismantling-exclu-tool

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

21 World Economic Forum, State of Quantum Computing: Building a Quantum Economy, 2022, https://www.weforum.org/publications/state-of-quantum-computing-building-a-quantum-economy/

22 Jay Gambetta, The hardware and software for the era of quantum utility is here, IBM, 2023, https://research.ibm.com/blog/quantum-roadmap-2033

23 Devoret, Michel H. and Robert J. Schoelkopf, Superconducting Circuits for Quantum Information: An Outlook, Science 339, 2013, p. 1169 - 1174.

24 Chainalysis, Cryptocurrency Mining Pools and Money Laundering: Two Real World Examples, 2023 [accessed 20.09.2023], https://blog.chainalysis.com/reports/cryptocurrency-mining-pools-money-laundering/

25 Europol (2018), Internet Organised Crime Threat Assessment (IOCTA) 2018, [accessed 20.09.2023], https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2018.

26 United States Attorney's Office District of New Jersey, Bitclub, [accessed 20.09.2023], https://www.justice.gov/usao-nj/bitclub

27 United States Attorney's Office District of New Jersey, Nevada Man Admits Money Laundering and Tax Offenses Related to BitClub Network Fraud Scheme, 2022 [accessed 20.09.2023], https://www.justice.gov/usao-nj/pr/nevada-man-admits-money-laundering-and-tax-offenses-related-bitclub-network-fraud-scheme

28 Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU (Text with EEA relevance), European Union, 2018, [accessed 20.09.2023], https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32018L0843

29 Github, bips/bip-0039.mediawiki, [accessed 20.09.2023], https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki

30 Github, bitcoinjs/bip38, [accessed 20.09.2023], https://github.

com/bitcoinjs/bip38

31 Trezor, Shamir Backup — A Better Way to Secure Your Keys, 2019, [accessed 20.09.2023], https://blog.trezor.io/shamir-backup-the-revolution-of-private-keys-backup-is-here-858687ed7fe7

32 Europol (2022), Cryptocurrencies: tracing the evolution of criminal finances, [accessed 20 September 2023], https://www.europol.europa.eu/publications-events/publications/cryptocurrencies-tracing-evolution-of-criminal-finances

33 DASH, The Impact of Bitcoin on Dash, 14 March 2023, accessed 20 September 2023, https://www.dash.org/blog/the-impact-of-bitcoin-on-dash/

34 Elliptic, Explaining MimbleWimble: The Privacy Upgrade to Litecoin, 2022, [accessed 20.09.2023], https://www.elliptic.co/blog/explaining-mimblewimble-the-privacy-upgrade-to-litecoin

35 Coinbureau, What is Mimblewimble, What Does it Do, and Why You should Care, 2023, [accessed 20.09.2023], https://www.coinbureau.com/education/what-is-mimblewimble/#defining-mimblewimble

36 Z.cash, WHAT ARE ZERO-KNOWLEDGE PROOFS?, [accessed 20.09.2023], https://z.cash/learn/what-are-zero-knowledge-proofs/#:~:text=In%20Zcash%2C%20zero%2Dknowlege%20proofs,actual%20balance%20and%20transaction%20history.

37 Chainalysis, Understanding Tornado Cash, Its Sanctions Implications, and Key Compliance Questions, 2022, [accessed 20.09.2023], https://www.chainalysis.com/blog/tornado-cash-sanctions-challenges/

38 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal of the European Union, 2016, https://eur-lex.europa.eu/eli/reg/2016/679/oj

39 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC , Official Journal of the European Union, 2023, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32018R1725

40 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, Official Journal of the European Union, 2016.

41 Christian Rathgeb and Andreas Uhl, A survey on biometric cryptosystems and cancellable biometrics, EURASIP Journal on Information Security, 2011.

42 A. Bassit, F. Hahn, R. Veldhuis and A. Peter, Hybrid biometric template protection: Resolving the agony of choice between bloom filters and homomorphic encryption, IET Biometrics, Vol. 11, pp. 430-444, 2022.

43 Christian Rathgeb and Andreas Uhl, A survey on biometric cryptosystems and cancellable biometrics, EURASIP Journal on Information Security, 2011.

44 C. Aguilar-Melchor, S. Fau, C. Fontaine, G. Gogniat and R. Sirdey, Recent advances in homomorphic encryption: a possible future for signal processing in the encrypted domain, IEEE Signal Processing Magazine, Vol. 30 (2), pp. 108–117, 2013.

45 S. Minaee, A. Abdolrashidi, H. Su, M. Bennamoun and D. Zhang, Biometrics recognition using deep learning: a survey, Artificial Intelligence Review, Vol. 56, pp. 8647–8695, 2023.

46 C. Rathgeb, J. Kolberg, A. Uhl and C. Bush, Deep learning in the field of Biometric Template Protection: An overview, arXiv:2023.02715v1 cs.CV, 2023.

47 M. Gomez-Barrero, J. Galbally, C. Rathgeb and C. Busch, General framework to evaluate unlinkability in Biometric Template Protection systems, IEEE Trans. on Information Forensics and Security, Vol. 13, pp. 1406-1420, 2018.

48 M.Maurer & M. Yu, DNS-over-HTTP/3 in Android, Google Security Blog, 2022, [accessed at 02.03.2024], https://security.googleblog.com/2022/07/dns-over-http3-in-android.html

49 Kampourakis, G. and Karopoulos, G., Domain Name System Security Extensions (DNSSEC) standards: an analysis of uptake in the EU, 2022, EUR 31273 EN, Publications Office of the European Union, Luxembourg, 2022, ISBN 978-92-76-58633-3, doi:10.2760/975868, JRC128815.

50 Kosek, M., Doan, T. V., Granderath, M., & Bajpai, V., One to rule them all? a first look at DNS over QUIC. In International Conference on Passive and Active Network Measurement, 2022, pp. 537-551,. Cham: Springer International Publishing.

51 Lyu, M., Gharakheili, H. H., & Sivaraman, V., A survey on DNS encryption: Current development, malware misuse, and inference techniques. ACM Computing Surveys, 2022 55(8), 1-28.

52 Hynek, K., Vekshin, D., Luxemburk, J., Cejka, T., & Wasicek, A., Summary of DNS over https abuse. IEEE Access, 2022, 10, 54668-54680.

53 Lyu, M., Gharakheili, H. H., & Sivaraman, V., A survey on DNS encryption: Current development, malware misuse, and inference techniques. ACM Computing Surveys, 2022, 55(8), 1-28.

54 Rivest, R.L, Cryptography and machine learning. In Advances in Cryptology—ASIACRYPT'91, Proceedings of the ASIACRYPT 1991, Fujiyoshida, Japan, 11–14 November 1991; Lecture Notes in Computer Science; Imai, H., Rivest, R.L., Matsumoto, T., Eds.; Springer: Berlin/Heidelberg, Germany, 1991; Volume 739.

55 Nitaj et al., Applications of Neural Network-Based AI in Cryptography, Cryptography, 2023.

56 Kim et al., Generating Cryptographic S-Boxes Using the Reinforcement Learning, 2021, IEEE Access PP(99):1-1.

57 Carbone, M.; Conin, V.; Cornélie, M.-A.; Dassance, F.; Dufresne, G.; Dumas, C.; Prouff, E.; Venelli, A. Deep Learning to Evaluate Secure RSA Implementations. IACR Trans. Cryptogr. Hardw. Embed. Syst. 2019, 132–161. [CrossRef]

58 Xia et al., Cryptographic algorithms identification based on deep learning, Computer Science & Information Technology (CS & IT), 2022.

59 Yuan, K., Huang, Y., Du, Z. et al., A multi-layer composite identification scheme of cryptographic algorithm based on hybrid random forest and logistic regression model. Complex Intell. Syst., 2023, https://doi.org/10.1007/s40747-023-01212-2

60 Ke Yuan, Yabing Huang, Jiabao Li, Chunfu Jia, and Daoming Yu. 2022. A Block Cipher Algorithm Identification Scheme Based on Hybrid Random Forest and Logistic Regression Model. Neural Process., 2023, Lett. 55 3, 3185–3203. https://doi.org/10.1007/s11063-022-11005-2

61 Zhao L, Chi Y, Xu Z, Yue Z (2023), Block cipher identification scheme based on hamming weight distribution. IEEE Access 11:21364–21373. https://doi.org/10.1109/ACCESS.2023. 3249753

62 Wang X, Chen Y, Wang Q, Chen J (2021), Cryptosystem identification scheme combining feature selection and ensemble learning. Comput Eng 47(1):139–145. https://doi.org/10.19678/j.issn.1000-3428.0056918

63 Grari H, Zine-Dine K, Azouaoui A, Lamzabi S (2022), Deep learning-based cryptanalysis of a simplified aes cipher. Int J Inf Secur Priv (IJISP) 16(1):1–16. https://doi.org/10.4018/IJISP.300325

64 Kim, Hyunji, Sejin Lim, Yeajun Kang, Wonwoong Kim, Dukyoung

Kim, Seyoung Yoon, and Hwajeong Seo. 2023. Deep-Learning-Based Cryptanalysis of Lightweight Block Ciphers Revisited. Entropy 25, no. 7: 986. https://doi.org/10.3390/e25070986

65 Kocher, P. Timing attacks on implementations of Diffie-Hellmann, RSA, DSS, and other systems. In Proceedings of the CRYPTO'96, Santa Barbara, CA, USA, 18–22 August 1996; Volume 1109, pp. 104–113.

66 Kocher Paul C., Jaffe Joshua, and Jun Benjamin, Differential power analysis. In Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology (CRYPTO'99), 1999, Springer-Verlag, London, UK, 388–397. http://dl.acm.org/citation.cfm?id=646764.703989

67 Quisquater Jean-Jacques and Samyde David, ElectroMagnetic analysis (EMA): Measures and counter-measures for smart cards. In Smart Card Programming and Security, 2001, Attali Isabelle and Jensen Thomas (Eds.). Springer Berlin, Berlin, 200–210.

68 BrierEric et al. Correlation power analysis with a leakage model.

69 Lang Li, Yu Ou, A deep learning-based side channel attack model for different block ciphers, Journal of Computational Science, Volume 72, 2023.

70 Cagli E. et al., Convolutional neural networks with data augmentation against jitter-based countermeasures, 2017, Paris.

71 Stjepan Picek, Guilherme Perin, Luca Mariot, Lichao Wu, and Lejla Batina, SoK: Deep Learning-based Physical Side-channel Analysis. ACM Comput. Surv., 2023, 55, 11, Article 227, https://doi.org/10.1145/3569577

72 Takaya Kubota, Kota Yoshida, Mitsuru Shiozaki, Takeshi Fujino, Deep learning side-channel attack against hardware implementations of AES, Microprocessors and Microsystems, 2021, Volume 87, 103383, ISSN 0141-9331, https://doi.org/10.1016/j.micpro.2020.103383

73 Picek Stjepan et al. On the performance of convolutional neural networks for side-channel analysis, Lecture Notes in Computer Science - SPACE 2018: International Conference on Security, Privacy, and Applied Cryptography Engineering, 2018, Springer, Cham.

74 Lang Li, Yu Ou, A deep learning-based side channel attack model for different block ciphers, Journal of Computational Science, 2023, Volume 72, 102078, ISSN 1877-7503.

75 Stjepan Picek, Guilherme Perin, Luca Mariot, Lichao Wu, and Lejla Batina. 2023. SoK: Deep Learning-based Physical Side-channel Analysis. ACM Comput. Surv. 55, 2023, 11, Article 227 https://doi.org/10.1145/3569577

76 Council of the European Union, Security through encryption and security despite encryption, Council resolution on encryption, 2020, Brussels.

77 NIST, NIST Announces First Four Quantum-Resistant Cryptographic Algorithms, 2022, [accessed on 02/03/2024], https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms

78 N.Roos, Dutch and Belgian involvement in new post-quantum cryptography standard, Bits&Chips, 2022, [accessed on 02/03/2024], https://bits-chips.nl/artikel/dutch-and-belgian-involvement-in-new-post-quantum-cryptography-standard/

79 A. G. Rodriguez, A quantum cybersecurity agenda for Europe: Governing the transition to post-quantum cryptography. European Policy Center, Brussels, 2023.

80 European Commission, Quantum Technologies Flagship, 2023, [accessed 22/06/2023], https://digital-strategy.ec.europa.eu/en/policies/quantum-technologies-flagship

81 OpenSuperQ, About OpenSuperQ, 2023, [accessed 22/06/2023], https://opensuperq.eu/project

82 Aqtion, About, 2023, [accessed 22/06/2023], https://www.aqtion.eu/about/

83 International Telecommunication Union, Radiocommunication Sector (2023), Recommendation ITU-R M.2160-0: Framework and overall objectives of the future development of IMT for 2030 and beyond, M Series: Mobile, radiodetermination, amateur and related satellite services, Electronic publication, Geneva.

84 6GSNS, Mission and Objectives, 2023 [accessed 02/03/2023], https://smart-networks.europa.eu/missions-and-objectives/

85 Networld Europe (2023), White Paper #1: Technologies & Standards to Enable Vertical Ecosystem Transformation in 6G, White Paper Series.

86 Networld Europe (2022), Strategic Research and Innovation Agenda 2022 : Technical Annex, 10.5281/zenodo.7455433.

87 6GSNS, Project Portfolio, 2023 [accessed 02/03/2023], https://smart-networks.europa.eu/project-portfolio/

88 European Commission (2022), Regulation of the European Parliament and of the Council establishing the Union Secure Connectivity Programme for the period 2023-2027., Strasbourg: France.

89 REGULATION (EU) 2021/694 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 29 April 2021: establishing the Digital Europe Programme and repealing Decision (EU) 2015/2240. Official Jouranl of European Union, 2021.

90 European Commission (2023), Horizon Europe, Cluster 3: Civil security for society, [accessed 02/03/2023], https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe/cluster-3-civil-security-society_en

91 European Commission (2023). Horizon Europe: Work Programme 2023-2024: 6. Civil Security for Society., European Commission Decision C(2023) 2178 of 31 March 2023.

92 European Commission (2022), Transition towards Quantum-Resistant Cryptography, Funding and Tender Opportunities Portal, [accessed 02/03/2023] https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/horizon-cl3-2022-cs-01-03

93 European Commission Migration and Home Affairs, Internal Security Fund (2021-2027), [accessed 02/03/2023] https://home-affairs.ec.europa.eu/funding/internal-security-funds/internal-security-fund-2021-2027_en

94 European Commission (2022), COMMISSION IMPLEMENTING DECISION on the financing of the components of the Thematic Facility under the Internal Security Fund and the adoption of the work programme for 2023, 2024 and 2025.Brussels, 2022.

95 Xia, Ruisi, Manman Li, and Shaozhen Chen. "Cryptographic Algorithms Identification based on Deep Learning." In CS & IT Conference Proceedings, vol. 12, no. 12. CS & IT Conference Proceedings, 2022

96 Quantum Flagship, accessed via https://qt.eu/funding-opportunities/

97 Stjepan Picek, Guilherme Perin, Luca Mariot, Lichao Wu, and Lejla Batina. ''SoK: Deep Learning-based Physical Sid e-channel Analysis.'' ACM Computing Surveys, vol. 55, issue 11, Article 227. ACM Computing Surveys, 2023

www.europol.europa.eu