https://utilitasmathematicapublishing.com
Vol: 1, ISSUE: 1, 2025
Journal of Quantum Algorithms and Cryptography (JQAC)
Pg No: 43-58

Intelligent systems and quantum encryption

[1] **A. Sudhakar Reddy,** Research Scholar, Department of Mathematics School of Engineering, Presidency University, Bangalore, Karnataka, India.

[2] **Dr. V. Ramalatha,** Associate professor, Department of Mathematics School of Engineering, Presidency University, Bangalore, Karnataka, India.

Abstract

Recent innovations in technology, especially in the fields of artificial intelligence (AI) and quantum computing, have caused a sea shift in the way technology is used. Quantum cryptography has been greatly affected by these developments, and artificial intelligence approaches show great promise for improving the security and efficiency of cryptographic systems in this area. While current security algorithms have their work cut out for them, a new danger known as the "quantum threat" has emerged with the advent of quantum computers. Notwithstanding these obstacles, there are encouraging ways to incorporate AI based on neural networks into cryptography, which will greatly affect the paradigms of digital security in the future. The possible advantages of AI-driven cryptography, the obstacles that must be overcome, and the future of this multidisciplinary field of study are all outlined in this overview of the major subjects at the confluence of AI and quantum cryptography.

Keywords: neural networks, quantum algorithms, AI-quantum integration, quantum dangers, AI-enhanced security, and quantum data processing.

Introduction

An sophisticated branch of cryptography, quantum cryptography uses concepts from quantum physics to encrypt data. In contrast to conventional cryptography, which relies on intricate mathematical procedures to encrypt data, quantum cryptography builds an intrinsically secure communication system using the physical features of quantum particles, including photons.
Quantum key distribution (QKD) is the backbone of quantum cryptography; it's a mechanism for two people to create a shared random secret key, which is necessary for secure message encryption and decryption that may be detected by an eavesdropper. The Heisenberg uncertainty principle and quantum entanglement are cornerstones of quantum mechanics that provide the foundation for QKD's security. According to the Heisenberg uncertainty principle, taking a measurement of a quantum system will always cause it to change its state. So, if someone tries to listen in on the quantum keys and measure them, they will cause noticeable changes, which will let the individuals involved in the conversation know that someone is trying to eavesdrop on them.
Another key idea in quantum physics is quantum entanglement, which connects two quantum particles so that their states are instantly affected by each other, distance being no longer an issue... It is possible to create a secure key between two people using this attribute. Providing communication channels that are immune to eavesdropping is the main advantage of quantum cryptography. It gets beyond a lot of the problems with traditional advancements in traditional cryptography capability, like quantum computers. Because of this, it is an important field of research for the future of quantum computing when it comes to protecting sensitive information.

Experts in the fields of science and technology have recently taken a keen interest in the potential for artificial intelligence and quantum cryptography to combine. Thanks to its superior data processing, pattern recognition, and decision-making capabilities, artificial intelligence (AI) has revolutionized the healthcare and financial sectors, respectively. Concurrently, quantum cryptography offers unrivaled physical-law based security, mainly via quantum key distribution (QKD) and associated protocols. It is not a coincidence that AI and quantum cryptography are aligning. It seems to reason that in this digital era of massive data flows and increasing cybersecurity risks, the computing capacity of AI and the unbreakable security mechanisms of quantum cryptography should be combined. Algorithms developed by artificial intelligence have the ability to improve quantum cryptography techniques by analyzing massive volumes of data. At the same time, quantum cryptography may provide a safe foundation for AI systems, making sure that the algorithms and data they handle are never compromised. The impending release of quantum computers has elevated the significance of quantum cryptography. The rapidity with which these computers can decipher traditional cryptographic systems is a major concern for contemporary cybersecurity. So, to solve this critical problem, we need to combine AI with quantum cryptography, and it's not simply a theoretical exercise. This review delves deep into the ways in which quantum cryptography and artificial intelligence interact. Highlighting notable experiments and applications, we go deeply into the historical evolution of both fields and how they interact with each other, highlighting both the obstacles and possibilities that come with them simultaneously. Our goal is to ensure that readers fully understand the present state of research and to highlight the tremendous future potential of this combination.

Rationale
Two revolutionary domains are coming together at the intersection of AI and quantum cryptography. Artificial intelligence has revolutionized data processing and analysis, while quantum cryptography provides unparalleled protection for data transmission. There is an exciting new frontier at the junction of these two fields, which are both dynamic and ever-changing. Discussed in this article are the possible benefits, drawbacks, and interactions between artificial intelligence and quantum cryptography.

Aims of the research
With this research, we want to fill in certain gaps in our understanding of AI and quantum cryptography's past and present.

study and practical situation where they meet. We will also discuss the opportunities and problems that may arise from combining AI with quantum cryptography, as well as the potential benefits of this multidisciplinary area of study.

Research questions

1. How flave tfle fields of artificial intelligence and quantum cryptograpfly evolved flistorically?
2. How can AI improve Quantum Cryptograpflic protocols and vice versa?
3. Wflat are tfle main cflallenges in combining AI and quantum cryptograpfly?
4. Wflat opportunities emerge from tfle interaction of AI and quantum cryptograpfly, and flow migflt tfley influence future researcfl and applications?

The following sections will explore the exciting and interdisciplinary intersection, guiding researchers and enthusiasts.

A brief history of both AI and quantum cryptography

Introduction to cryptography

The Greek terms kryptós (meaning hidden or secret) and graphein (meaning to write) and logia (meaning to study) are the origins of the English words cryptography and cryptology, respectively. "Secret writing" is the Greek definition of cryptography. (According to Liddell, 1894). The "computa-tional hardness assumption" is the cornerstone of contemporary cryptography, which is based on cryptographic algorithms (Braverman et al. 2015). It has real-world uses in several fields, including digital money, computer passwords, chip-based payment cards, and military communications (Paar and Pelzl 2009). When it comes to cybersecurity and encryption (e.g., HTTPS, PGP), it is essential.
Cryptographic hash functions, cryptographic keys, and Zero Knowledge Proofs (ZKP) are widely used cryptographic approaches in the crypto-economics and cryptocurrency communities.
Among the many encryption algorithms available is the advanced encryption standard's triple data encryption algorithm (3DEA). Using the 3DES cipher, which stands for "Triple DES," it encrypts data three times. Data Encryption Algorithm—DEA, or the Lucifer symmetric-key algorithm, is the foundation of DES (Feistel 1971). Ronald Rivest, Adi Shamir, and Leonard Adleman's asymmetric RSA public-key encryption technique is another well-known encryption method (Rivest et al. 1978).

In addition, IPAA Regulatory Compliance, GDPR (GDPR 2023; ICO 2023), and PCI-DSS also play significant roles in ensuring the safety and security of sensitive information.

Cryptography vs cybersecurity

In recent years, most of the cryptographic development has been for cybersecurity. In this short section, we wanted to emphasise the specific strengths and vulnerabilities in recent cryptography applications in cybersecurity.

First and foremost, good cryptography depends on the difficulty of the mathematical problem. In other words, the encryption is only as strong as the mathematical problem the cryptographic algorithm solves.

The second factor is implementation quality because correct implementation is critical to the algorithm's security.

The third requirement is critical secrecy because secret keys must be stored somewhere, usually by a centralised trusted authority.

Suppose you are a hacker attempting to hack a cryptosystem. In that case, you will begin by attempting to solve the math problem, looking for vulnerabilities in the implementation, or attempting to obtain access to the secret keys.

Quantum cryptography vs low memory cryptography

The National Institute of Standards and Technology (NIST) has announced Ascon as the algorithm that will serve as the official standard for lightweight cryptography of low-memory internet-of-things devices.[1] Since the NIST competition was announced in 2018, selecting the best, most secure, and most efficient algorithm has been ongoing, and the standard may not be ready until late 2023. However, it is essential to note that other institutes, such as ISO and ENISA, have yet to select the most appropriate algorithms. Other standard-setting organisations from around the world will likely leverage NIST's efforts. The other option is to go through this process themselves, leaving their IoT infrastructure vulnerable to cyber threats.

According to NIST, the most peculiar aspect of the selection process was the effectiveness of these new algorithms 'most of the finalists exhibited performance advantages over NIST standards on various target platforms without introducing security concerns'.[2] This statement is especially concerning given that NIST is one of the most frequently updated and globally recognised as one of the most advanced cybersecurity frameworks. Assume that other standard-setting organisations have not even begun identifying a lightweight cryptographic standard and that numerous available algorithms exist. Consequently, this reaffirms that cybersecurity and cryptography are strongly linked to the global standardisation of security frameworks and regulations.

For the NIST lightweight cryptography standard, 57 solutions were initially submitted in response to the call for submissions3. Data transmission to and from the "innumerable" small IoT devices must be protected using lightweight cryptography, which calls for a new class of cryptographic algorithms. Inadequate electrical power powers the vast majority of Internet of Things (IoT) micromachines, sensors, actuators, and other low-memory devices used for network guidance and communication. These gadgets are similar to keyless access fobs and RFID tags used in warehouses and supply chains in that they include little circuitry. These Internet of Things technologies are tiny, inexpensive, and have a much less constrained chip than even the most basic mobile phone. This is their main benefit. The computing power and electrical resources needed by existing encryption methods are more than what is available on IoT devices. Therefore, the main drawback of any Internet of Things gadget is also its main advantage.

In contrast to lightweight encryption, such as Ascon, which targets devices with little memory, such as Internet of Things (IoT) devices, quantum cryptography offers a novel method. It provides potentially unbreakable security by following the principles of quantum physics and primarily focusing on quantum key distribution (QKD). Ascon is the primary focus of NIST's efforts to secure data stored on low-powered Internet of Things (IoT) devices. Quantum cryptography, on the other hand, seeks to use the unique properties of quantum bits (qubits) for secure communication, independent of the computational capability of the device. Current scalability and compatibility issues with traditional communication systems are major hurdles for quantum cryptography. In contrast, lightweight cryptography must provide security even when computing resources are few. Internet of Things devices have trouble using standard encryption methods because of their limited processing power. These devices may have much more formidable challenges in the event that direct quantum cryptography techniques are put into action.

[1] flttps://www.nist.gov/news-events/news/2023/02/nist-selects-ligfltweigflt-cryptograpfly-algoritflms-protect-small-devices.

[2] flttps://csrc.nist.gov/News/2023/ligfltweigflt-cryptograpfly-nist-selects-ascon.

[3] flttps://www.nist.gov/news-events/news/2018/04/nist-issues-first-call-ligfltweigflt-cryptograpfly-protect-small-electronics.

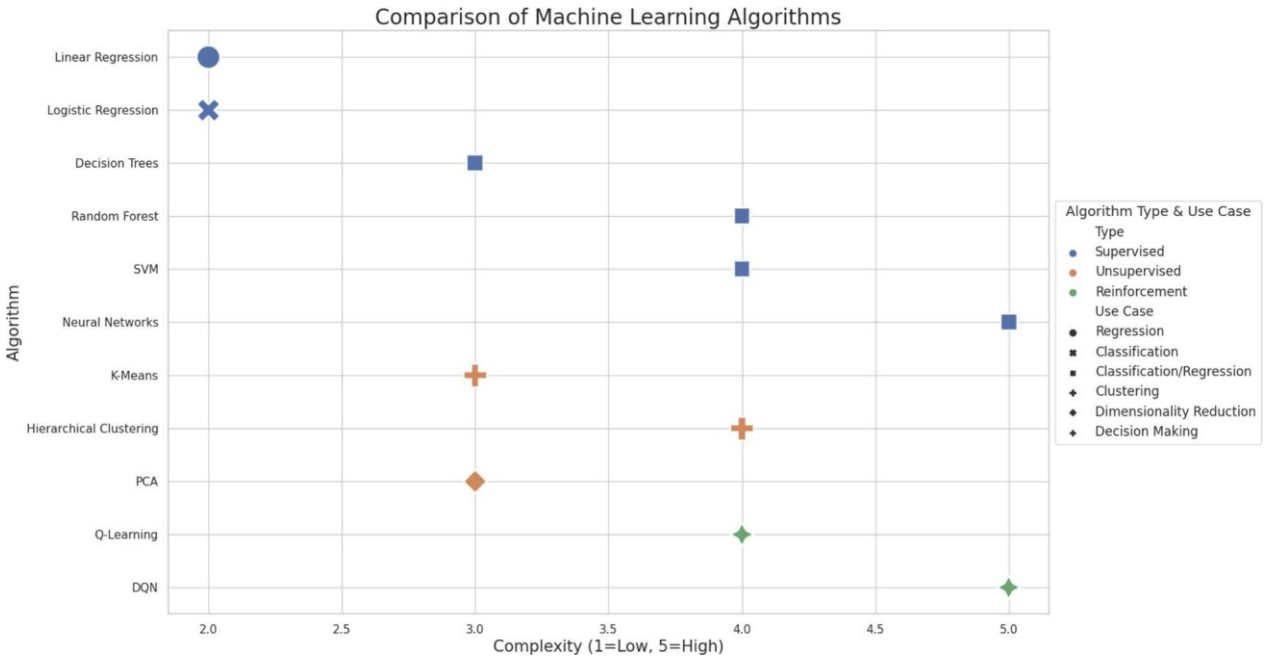

Fig. 1 Navigating through popular and traditional ML algorithms

The convergence of classical and quantum domains has paved the way for developing hybrid cryptographic techniques that can provide enhanced security measures, even on low-power devices. Such solutions are designed to combine the strengths of both classical and quantum systems, ensuring the utmost protection of sensitive data and information. By leveraging the unique properties of quantum mechanics, hybrid cryptographic algorithms can overcome the limitations of classical cryptography and offer advanced levels of security that are essential in today's digital age.

Review of advancements in artificial intelligence

Although the concept of machines and statues that mimic human thought and behaviour can be found in ancient myths and legends, the scientific field of AI emerged in the mid-twentieth century. In 1950, British mathematician Alan Turing established the Turing Test as a benchmark for a machine's ability to exhibit intelligent actions identical to a human.

Over the years, AI research has experienced peaks and troughs, commonly called "AI winters" and "AI springs." In the 1960s, there was a lot of optimism and funding for AI, as early problem-solving algorithms and knowledge representation showed potential. However, there were soon computational limitations and difficulties in emulating human intelligence. The 1980s witnessed a revival with the development of expert systems, which mimicked human decision-making skills. Nevertheless, by the end of the decade, the shortcomings of these systems became more apparent. In Fig. 1, we can visually compare the complexity of different algorithms.

Some of the more complex algorithms seen in Fig. 1 did not exist in the 1980s. The twenty-first century has brought remarkable progress in computational power and data accessibility. With the help of machine learning and intense learning, machines can now handle extensive datasets and efficiently perform tasks such as speech and image recognition. As a result, AI has become a crucial component of modern technological advancement.

Review of advancements in quantum cryptography

In the early 20th century, the groundwork for quantum cryptography was laid. The paradoxical features of quantum systems, such entanglement and superposition, presented both problems and possibilities for information processing in the field of quantum mechanics. The field of quantum information theory made great strides forward in the '70s and '80s. Building on prior work in quantum mechanics and information theory, the BB84 protocol, developed by Charles Bennett and Gilles Brassard in 1984, established the notion of quantum key distribution (QKD). This protocol made use of the rules of quantum physics to enable two parties to generate a shared, secret random key, which was physically secure. Both theoretical and practical components saw substantial progress in the subsequent years.

to quantum cryptography. Quantum cryptography algorithms have broadened their use to include quantum digital signatures and secure direct communication in addition to critical distribution. Commercial quantum secure communication networks are now within reach, thanks to the protocols' implementation and testing in real-world circumstances made possible by advancements in photonics and quantum technology. Despite coming from separate scientific traditions, AI and quantum cryptography have eventually come together thanks to shared ground-breaking discoveries, ever-improving technology, and an insatiable need for knowledge. Potentially revolutionizing information security and AI, this combination brings both opportunities and difficulties.

Review of integration in AI with quantum cryptography

Massive developments in artificial intelligence and quantum computing have altered several fields, cryptography included. Harnessing AI's processing power to improve the efficiency, security, and resilience of quantum cryptographic systems is one of the main goals of integrating AI with quantum cryptography. AI approaches may greatly aid in the optimization of quantum cryptography protocols and the resolution of their complicated problems due to their data-processing, pattern-recognition, and scenario-adaptive capabilities.

Simultaneously, quantum cryptography offers a novel approach to AI system security, thanks to its underlying security rooted in quantum physics. Nowadays, with all the data being shared online and the number of cyberattacks on the increase, this integration couldn't be more pertinent and appropriate. In this context, AI plays a vital role. Quantum cryptography may greatly benefit from the analysis and interpretation of big datasets made possible by artificial intelligence algorithms.

A new and serious danger to cryptographic systems, known as the "quantum threat," has emerged with the advent of quantum computers. Because quantum computers may be able to crack many of the present encryption techniques, this danger threatens conventional cryptographic approaches. The integration of AI and quantum cryptography is therefore an essential step forward in our strategy for protecting sensitive data online, and not just a theoretical exercise. In order to guarantee a safe computing future, AI-driven methodologies in quantum cryptography seek to foresee, lessen, and fiercely resist the quantum danger.

The relationship between artificial intelligence and quantum cryptography is thoroughly examined in this study, which examines their

evolution over time, difficulties brought about by the introduction of quantum computing, and the revolutionary possibilities of combining the two. Its goal is to help readers grasp the present situation as well as the promising future of safe computing that this interdisciplinary union promises.

Review of the quantum threat

The 'quantum danger' is the idea that powerful quantum computers might compromise current encryption techniques. The computational complexity of certain mathematical problems determines the cryptographic techniques used, such as Elliptic Curve Cryptography (ECC) and RSA. For instance, ECC is based on the difficulty of solving the discrete logarithm problem involving elliptic curves, while RSA is based on the difficulty of factoring big prime numbers. These issues, which conventional computers are finding challenging, may be amenable to efficient solution by quantum computers using methods like Shor's algorithm.

Unlike conventional computers, quantum computers use quan-tum physics concepts like entanglement and superposition to process data in a unique way. They are able to execute targeted computations at a far higher rate than conventional computers because of this capabilities. As shown by Shor's algorithm, quantum computers might factor huge numbers exponentially quicker than the most popular conventional techniques. Consequently, once sufficiently powerful quantum computers are built, encryption schemes that rely on the complexity of these challenges for security would become susceptible.

In the not-too-distant future, the quantum menace will become more than a theoretical worry. New cryptographic methods, also called "post-quantum" or "quantum-resistant," are therefore required in light of the arrival of quantum computing to provide security against quantum assaults. With these devices, we want to implement cryptographic techniques and algorithms that quantum computers will have a hard time cracking.

Against this danger, a strategic answer is to combine AI with quantum cryptography. When it comes to creating, testing, and perfecting algorithms that are resistant to quantum computing, AI's superior pattern recognition and prediction powers may be invaluable. To further fortify cryptographic systems against the ever-changing quantum computing landscape, AI can aid in their real-time assessment and adaption. To guarantee data security and privacy in the next quantum computing age, research into the convergence of AI and quantum cryptography is crucial.

Research methodology

The complex interplay between artificial intelligence and quantum cryptography is explored in depth in this study by means of a qualitative methodology grounded on an interpretative paradigm. Cybersecurity is a dynamic field, constantly changing as new standardized tools and ontologies are developed to improve data sharing and automate risk assessment. The "Reference Ontology for Cybersecurity Operational Information" is one such tool suggested by Takahashi and Kadobayashi (2015). This application is designed to help with cybersecurity operations by providing a defined framework for information and making it easier to communicate. This method encourages cooperation and the sharing of information across businesses by providing a reference ontology for operational cybersecurity data. Cybersecurity information is structured using the ontology, which is in line with industry standards. By reviewing industry specification coverage, the authors showed how the ontology may be useful, and they collaborated with cybersecurity organizations to build it. In addition to outlining a prototype cybersecurity knowledge base that allows for information interchange, they created an extensible information structure that matches industry standards. The essay delves into the possible uses of the knowledge base and ontology in cybersecurity operations. Improving the sharing of cybersecurity-related data is the goal of the suggested ontology.
In order to provide a universal standard for the exchange of cybersecurity information, the CYBEX framework (Rutkowski et al., 2010) is a big deal. The goal of CYBEX, an effort of the International Telecommunication Union (ITU-T), is to standardize and guarantee the integrity of communication between cyber security agencies. By using CYBEX, the fragmentation of cybersecurity information availability will be reduced, enabling a more consistent defense posture on a global scale. This article provides an overview of the framework, including its specifications, potential uses, and current status. Data Description, Data Discovery, Data Query, Data Assurance, and Data Transport are the five distinct functional blocks that make up CYBEX. When put together, these building pieces improve cyber-security operations' automation and efficiency, which might lead to a decrease in operational expenses and human error. Despite their useful insights and contributions to the larger aims of vulnerability management and security information sharing, these studies are not the primary emphasis of this study. Therefore, although our study does not go into these areas specifically, we do recognize their importance within the larger framework of cybersecurity. This study seeks to further our understanding of how these two technical developments have affected cybersecurity. Consistent with previous worldwide initiatives to create, improve, and implement various cryptographic methods that are resistant to quantum computing (Kumar Sep. 2022).

Data collection

We employed two primary methodologies to gather data. Firstly, we gathered primary data from industry standards and guidelines (Nist et al. 2016; NIST 2023a, b, 2011; Tabassi 2023; https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework). Then, we conducted a case study with the authors and the organisations behind these standards. These interactions were systematically recorded, transcribed, and coded for further analysis. The process is recorded and can be visualised in Fig. 2.

Secondly, we reviewed a comprehensive literature by examining reputable scholarly journals and books. Our focus was on papers that critically evaluated the role of encryption in the context of AI and quantum mechanics (Kop 2023), particularly from the literature on quantum technology applications (Broadbent et al. 2015) and their societal impact, which were integrated during the analysis (Elaziz and Raheman 2022).

Data analysis

Thematic analysis (Yin 2009a) was the primary method to analyse the interactions between national and international standards. To begin with, preliminary codes were generated based on thoroughly scrutinising the interactions (Eisenhardt 1989). These codes were then sorted and organised into more comprehensive themes. It was a detailed and iterative analysis process, requiring ongoing data review to ensure an accurate representation (Yin 2009b). Moreover, valuable insights from academic literature were incorporated into the analysis (Eisenhardt 1989), explicitly focusing on quantum technology applications' societal impact (Alyami et al. 2021).

Validation procedures

To uphold the validity of our research, we employed the triangulation technique for evaluating software security through quantum computing techniques, such as the durability perspective (Alyami et al. 2021), the Hybrid Fuzzy ANP-TOPSIS Approach (Agrawal et al. 2020), and the integrated hesitant fuzzy-based decision-making framework for evaluating sustainable and renewable energy (Sahu et al. 2023). This involved verifying the insights we derived from case study interactions with the conclusions drawn from scholarly literature. Furthermore, we engaged peer-reviewed papers and assessed specific data portions and corresponding analyses. Their contributions were pivotal in anchoring the research's findings and aligning with the broader academic dialogue.

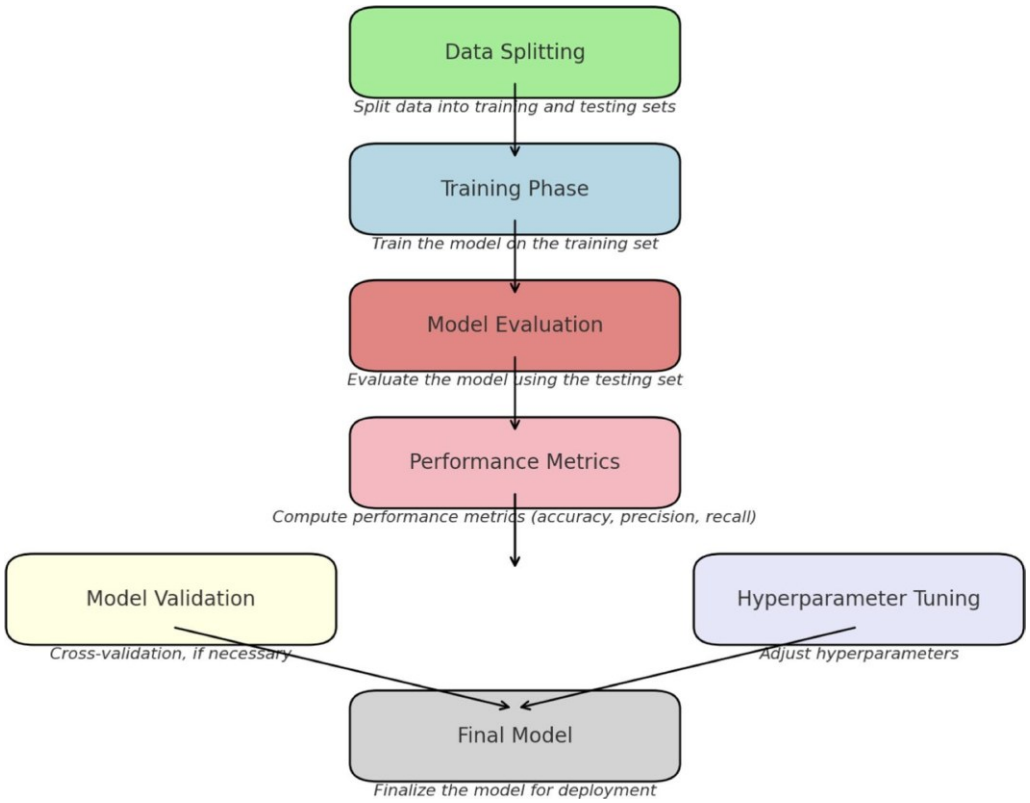

Fig. 2 AI model evaluation and validation

Review of the interplay between AI and quantum cryptography

The convergence of AI (Ying 2010) and quantum cryptography (Shapna Akter 2023) is a fascinating development that offers exciting computational and information security possibilities. This intersection represents a novel approach to secure communication and intelligent data processing that has the potential to revolutionise the way we perceive and utilise technological advancements. In this article, we will delve deeper into this fusion, closely examining its technical details, recent progress, and challenges to regulatory standards. This comprehensive analysis aims to provide a more nuanced understanding of this cutting-edge field and its potential implications for the future of technology and security.

AI in quantum cryptography

In modern cryptography (Paar and Pelzl 2009), one can find S-boxes, complex mathematical structures that are essential components within many symmetric key algorithms. These S-boxes have been created using vectorial Boolean functions in conjunction with AI, specifically by utilising neural network-based techniques (Nitaj and Rachidi 2023). This AI-driven approach allows for a more streamlined design process. It supports the analysis of cryptographic properties, ultimately developing more optimised and secure cryptographic protocols (Sevilla and Moreno, 2019). Through this method, the speed and efficiency of the design process are enhanced (Ying 2010; Diffie and Hellman 1976) while also ensuring that the result is a robust and reliable cryptographic protocol (Ayoade et al. 2022).

Optimising quantum key distribution (QKD)

Quantum cryptography is a highly secure communication method based on the principles of quantum mechanics. It relies on the QKD (quantum key distribution) method, which allows two parties to exchange a secret, shared random key for encrypting and decrypting their messages. The BB84 protocol is a well-known example of the QKD methods (Shamshad et al. 2022).

QKD is a highly secure method but is not immune to errors and security breaches. Hence, AI has the potential to enhance QKD in several ways.

Firstly, AI can help with error correction, an inevitable occurrence in any real-world QKD system. By predicting and correcting errors, AI can ensure the quantum key's integrity, which is essential for maintaining the security of the communication channel.

Secondly, AI-powered techniques can continuously monitor QKD systems to detect potential security breaches or eavesdropping attempts. This enhances security analysis and keeps the system safe from unauthorised access or tampering.

Finally, AI algorithms can optimise the rate of quantum key generation (Ying 2010) by considering environmental factors and hardware performance. This helps generate a quicker and more efficient key rate, crucial for high-speed communication channels. By leveraging AI-powered techniques, QKD can become even more secure and reliable, paving the way for the future of secure communication.

Quantum cryptography in AI: securing AI systems

In today's technologically advanced world, industries that rely on AI must prioritise the security of their algorithms and the data they handle. Data breaches can have severe consequences, including reputational damage and financial loss. One way to add an extra layer of security to AI systems is by using quantum cryptographic techniques. These techniques use the principles of quantum mechanics to protect data from potential attackers, making it computationally impossible for anyone to breach the system. By implementing these advanced security measures, industries can ensure the safety and integrity of their AI systems and the sensitive data they process.

Quantum principles in AI algorithms

The principles that govern the world of quantum physics vastly differ from those of classical physics. These principles can be a source of inspiration and innovation to design advanced AI algorithms. One such technique in quantum computing is quantum entanglement, which can optimise AI algorithms, particularly in training neural networks (Ying 2010). This results in the creation of more efficient and faster AI models. Furthermore, scientists have discovered that quantum entanglement, where particles become intertwined, can be leveraged to develop AI models that can process information in previously impossible ways. This breakthrough can revolutionise the field of AI and pave the way for even more advanced applications.

Regulatory landscape and standards

Integrating AI technology with quantum cryptography has presented novel challenges (Kop 2023) in regulatory and standards compliance (Ying 2010). To address this, various international organisations have come together to establish comprehensive guidelines and protocols for ensuring the reliability and security of quantum cryptographic systems. These efforts aim to establish a dependable and trustworthy framework to support the continued development and deployment of advanced quantum cryptographic solutions.

Notable advancements in data privacy and security have been made with the help of prominent organisations such as ISO/IEC (ISO 2022, 2017, 2023; NIST 2023a, b, c, d, e, 2001, f, g, 2022a, b, 2018, 2014, 2011; Tabassi 2023; SWID 2023; Petrov 2021; Udroiu et al. 2022; Catril Opazo 2021; NIST 2020; NIST 800-53 2020; NIST Advanced Manufacturing Office 2013; Johnson et al. 2016; https://advisera.com/27001academy/what-is-iso-27001/; https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework; https://csrc.nist.gov/Projects/block-cipher-techniques; https://csrc.nist.gov/Projects/post-quantum-cryptography; https://csrc.nist.gov/Projects/lightweight-cryptography; https://csrc.nist.gov/Projects/pec; https://www.nist.gov/cyberframework/getting-started), and EU/UK GDPR (GDPR 2023; ICO 2023). These entities have provided valuable insights and guidelines for protecting sensitive information, thus promoting user trust and confidence. With their contributions, the industry is better equipped to address emerging threats and challenges, paving the way for a more secure digital landscape.

The prestigious International Electrotechnical Commission (IEC) and the prestigious International Organization for Standardization (ISO) have begun initiatives to standardize protocols for quantum cryptography. The safe transfer of sensitive and secret information is an integral part of this, as are the essential processes for its creation. Projects like this make sure that many sectors, including healthcare, government, and finance, recognize quantum cryptography as a safe and dependable way to communicate securely. It is crucial for organizations to have better confidence in the security of their communication systems in today's more linked world. The standardization of these protocols will help with that.

A government institution under the United States Department of Commerce, the National Institute of Standards and Technology (NIST) (NIST 2023a, b) has meticulously produced standards and benchmarks for quantum cryptography systems. Because of this, you can be certain that these systems are secure enough to handle sensitive data in the age of quantum computing. Because of their potential importance in future cybersecurity, NIST is working to provide a solid foundation for quantum communication and cryptography. Problems specific to AI regulation exist. Artificial intelligence (AI) encounters regulatory roadblocks at the same time as quantum standardization concerns emerge. Data privacy, ethical concerns, and other related issues being open and honest while making decisions. Discussing the most effective ways to control AI is an international need for resolving these issues. As an

example, the EU's General Data Protection Regulation (GDPR) lays forth specific requirements for how AI should make decisions. This guarantees that AI will be used responsibly by establishing openness and accountability. Safe and ethical development and deployment of AI requires tackling the complicated and numerous difficulties of regulation. Although there is great potential in the future of AI and quantum cryptography working together, there are now roadblocks to implementation, improvement, and compliance with regulations. To make the most of this convergence, it is crucial to embrace a collaborative approach that includes academics, politicians, and business professionals. As we go forward, we need to be aware of the obstacles and collaborate to overcome them.

Challenges and opportunities: integrating AI and quantum cryptography

Great things could happen when artificial intelligence and quantum cryptography meet. But it's not easy for these two innovative domains to intersect. In this chapter, we will explore the major obstacles and possibilities that have arisen as a consequence of their combination. For instance, there are a number of real-world examples that illustrate how neural network-based AI might improve cryptographic systems. As an example, cryptographic algorithms themselves have been developed with the help of neural networks. An excellent illustration of this is the optimization of S-boxes (substitution boxes) in symmetric key cryptography by the use of machine learning methods. Many cryptographic methods rely on these S-boxes, which add nonlinearity and complication to the encryption process; one such algorithm is AES (the advanced encryption standard). To create safer and more efficient cryptographic algorithms, AI-driven approaches may study S-box features such differential uniformity and nonlinearity.
The area of cryptanalysis is another potential use. An automated cryptanalysis of several cryptographic methods has been carried out using AI algorithms and sophisticated learning models. Finding security flaws in cryptographic methods may be achieved by training neural networks with instances of both plaintext and ciphertext. These models can then learn to decode communications without the key or to anticipate the key.
When it comes to solving problems caused by quantum computers, AI based on neural networks is just as important as it is for improving conventional cryptography systems. Quantum computers take advantage of certain security holes in a broad Used algorithms for cryptography. For example, the RSA encryption depends on the difficulty of factoring the product of two big prime numbers; Shor's algorithm exploits quantum computers' capacity to efficiently factor huge numbers, thereby destroying the encryption. The security of ECC and Diffie-Hellman key exchange may be compromised because quantum computers are able to effectively solve the discrete logarithm problem. These flaws originate from two aspects of quantum computing: the superposition principle and quantum entanglement, which let the computers to concurrently consider several options and correlate the attributes of physically isolated particles. Current cryptography approaches are rendered susceptible by these properties, which allow quantum computers to execute particular computations significantly quicker than conventional computers.
The development of novel algorithms that can resist quantum computers' capabilities requires integrating AI with quantum-resistant cryptography research. One way AI is helping researchers discover and address flaws is by simulating quantum assaults on cryptographic systems. In addition, optimization approaches powered by AI may help develop post-quantum cryptography algorithms that are both more efficient and safe, guaranteeing that digital information will be adequately protected even in the quantum age.

Challenges: technological limitations

While quantum systems have the potential to provide unparalleled computational power, numerous technological limitations make their practical implementation difficult (Gill et al. 2022). One of the primary challenges in this field is the design of distributed quantum systems, which requires significant advancements in quantum hardware and error correction techniques (Awan et al. 2022). Despite these challenges, researchers remain dedicated to exploring the potential of quantum computing and developing new strategies to overcome the obstacles that stand in the way of progress.

Data challenges in AI and the transition to post-quantum cryptography

Integrating AI systems with quantum cryptographic systems is a complex process dependent on data quality, volume, privacy, security, and potential biases.

Real-time applications face several challenges in implementing AI-driven quantum cryptography. The scalability and performance of these technologies remain challenging, especially for large-scale data encryption and internet communication. Quantum cryptographic systems require significant infrastructure and can be resource-intensive, making large-scale deployments challenging. Integrating advanced quantum cryptographic

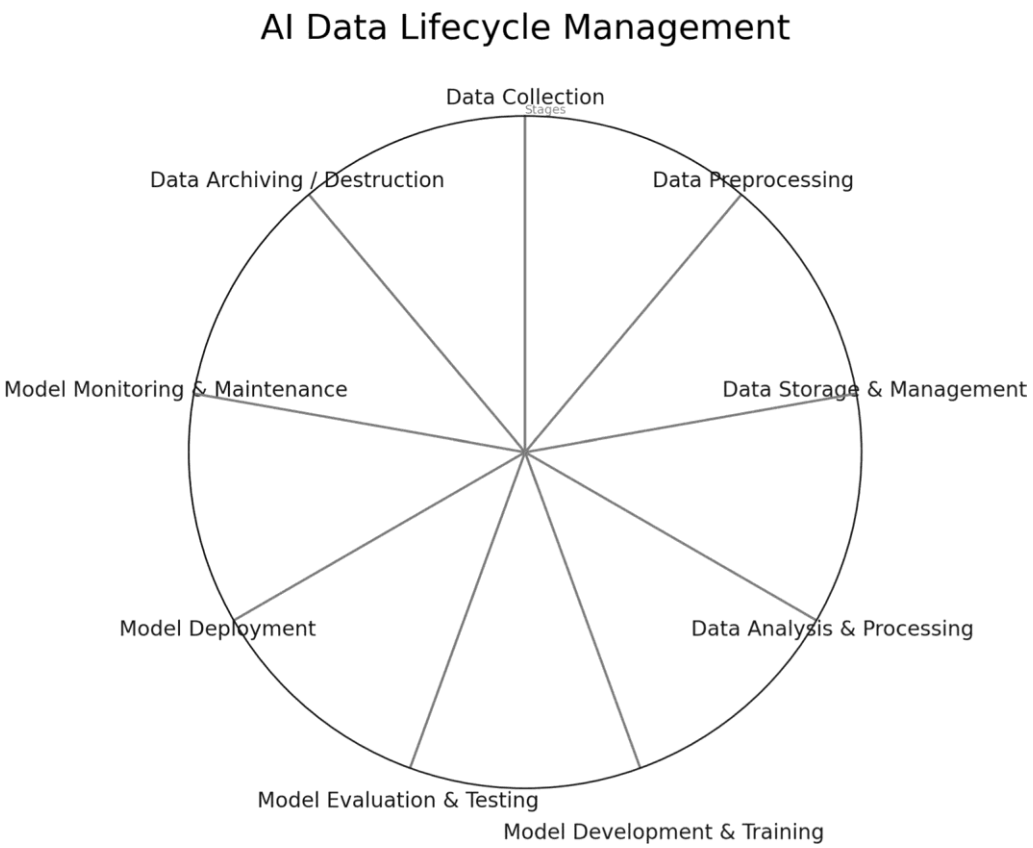

Fig. 3 Data challenges in the AI data lifecycle management caused by quantum cryptography

methods into existing communication systems without disrupting service is complex, and ensuring seamless operation during the transition to quantum-secure systems is crucial. Real-time applications demand minimal latency, and AI algorithms combined with quantum cryptographic processes can introduce latency that affects the efficiency and usability of real-time systems. Quantum cryptographic systems are sensitive to environmental factors, leading to higher error rates and making it challenging to ensure reliability and accuracy in diverse environments.

There is a real possibility that quantum cryptography and AI can work together, which would greatly improve cryptographic security. Artificial intelligence algorithms improve the flexibility and efficiency of quantum cryptography systems. Through the use of AI, the quantum danger has been successfully reduced, opening the road to the creation and improvement of cryptographic algorithms that are resistant to quantum computing. In spite of obstacles, the future seems bright for artificial intelligence (AI) thanks to its successful implementations and its uses in improving quantum cryptography systems. Secure communication routes, improved data privacy, and strong security solutions for different businesses are all part of this. In order to solve the problems with real-time applications, make them more scalable, lower their latency, and make sure they work with current systems, more R&D is required. In order to ease the shift to cryptographic systems that are resistant to quantum attacks, the findings highlight the need of policymaking and business involvement. This necessitates the investment in infrastructure, the standardization of procedures, and the promotion of cooperation among policy-makers, academics, and businesses. In Fig. 3, we can see this procedure shown. Figure 3 shows that post-quantum cryptographic approaches are necessary for the effective use of AI in this setting, which is especially important in light of the imminent advent of quantum computers (Aldoseri et al., 2023). Standardization and broad adoption may provide considerable obstacles, therefore the shift to these systems needs much planning and thought. Therefore, it is of the utmost importance to focus on developing dependable solutions that can effectively handle these concerns and safeguard critical information.

Opportunities for enhanced security mechanisms and AI-driven quantum systems

The combination of AI's remarkable data processing skills with quantum cryptography's unbreakable security might lead to the development of communication channels that are very safe and resistant to both classical and quantum attacks. The exponential growth of quantum computing has led many to predict that, in terms of processing power, quantum computers would soon surpass conventional ones (Ayoade et al. 2022). With the use of AI, quantum systems might be much improved, which could have far-reaching consequences for the development of quicker algorithms and more efficient cryptographic protocols. Secure communication and data transmission might be revolutionized by such breakthroughs. More substantial financing in quantum cryptography and exciting new frontiers in both domains might result from the intersection of AI with quantum notions, opening up new avenues of study.

The integration of artificial intelligence with quantum encryption presents formidable obstacles, but the payoffs might be enormous. New developments in computing and security may be built upon the multitude of possibilities that researchers can access. How we approach these professions may be revolutionized by these breakthroughs, and society can be substantially impacted as a result. An essential part of this endeavor is public key (PK) cryptography. With public key (PK) cryptography, also known as asymmetric cryptography, two mathematically connected keys—public and private—are used. When it comes to encryption and decryption, PK cryptography is head and shoulders above symmetric cryptography. This makes things more secure and makes sure that private information stays private, even if someone gets their hands on the public key. Cryptographic capabilities including digital signatures, encrypted data, and secure communication are made possible via PK cryptography. It provides improved security, scalability, and flexibility across a wide range of applications, making it an essential part of current cryptographic systems.

Creating digital signatures is an important part of cryptography. A digital signature can only be generated if the signatory has generated a set of keys, including a public key and a private key. In contrast to the publicly accessible public key, the private key is always kept secret. A hash function is used to create a one-of-a-kind hash of the text or document that has to be signed. The content of the document is uniquely represented by this hash value. To do hash signing, the signer must encrypt the hash value they create with their private key. They might associate a certain document with their signature in this way. A cryptographic digital signature, distinct from the document and the signer, is produced when the hash value is encrypted. Exciting prospects arise when AI and quantum cryptography are combined. Regardless of the substantial problems that need fixing, opportunities for gain that might be enormous, and consequences that could have far-reaching effects. By bringing these two areas together, promising new avenues for research and development in computing and security may be unlocked. As a result, this has the potential to spur new lines of inquiry and expand the frontiers of both secure communication and data transport.

Quantum cryptography

Quantum cryptography is a revolutionary technique that has the potential to provide unparalleled security measures based on the principles of quantum mechanics. In contrast to traditional cryptography, which relies on complex mathematical problems, quantum cryptography utilises the unique characteristics of quantum particles to establish an unbreakable encryption method. One of the critical components of this approach is quantum key distribution (QKD), which allows two parties to generate a secret and shared random key that can be used for secure communication. Furthermore, any attempt to eavesdrop on the quantum communication would be detected, as it would disrupt the quantum states being transmitted, revealing the presence of an intruder. This feature provides an added layer of safety and protection to the communication between the two parties.

Role of artificial intelligence in security

The role of AI in cybersecurity has become increasingly significant in recent times due to its ability to leverage machine learning and advanced algorithms to rapidly identify patterns, anomalies, and potential threats within vast data sets. This capability is especially critical in a world where cyber threats constantly evolve and become more sophisticated. AI not only helps to identify cyber threats in real-time, but it also provides predictive analysis to anticipate potential vulnerabilities, enabling proactive security measures. Furthermore, AI-driven systems can enhance authentication processes, simplify security operations, and facilitate faster responses to identified threats. AI is revolutionising cybersecurity by providing a powerful tool to combat cyber threats and protect sensitive data.

Previous studies on AI and quantum cryptography

There is ongoing research into the relationship between artificial intelligence and quantum cryptography, a growing study area. A study conducted by Ayoade (2022) demonstrated the impressive capabilities of quantum computing compared to traditional systems, suggesting the potential for AI at the quantum level. Gupta's research (Gupta et al. 2023) explores how AI and machine learning can aid quantum computing in the healthcare industry. In 2019, a discussion delved into how quantum

cryptography could protect communication between trusted parties from unauthorised listeners, indicating potential intersections with AI-driven security measures. These studies highlight the importance of continued exploration in this interdisciplinary field, as AI and quantum cryptography can shape the future of cybersecurity.

Artificial intelligence in cryptography

Overview of AI techniques in cryptography

AI has transformed many fields, including cryptography. Using machine learning techniques, AI offers new ways to tackle old and new cryptographic problems. Neural network-based AI is particularly useful for improving cryptographic methods and cryptanalysis (Nitaj and Rachidi 2023). AI's ability to quickly analyse vast amounts of data makes it an essential tool for identifying patterns and predicting potential cryptographic threats, which helps enhance security measures.

AI in classical cryptography

In traditional cryptography, AI is mainly used for cryptanalysis. By training machine learning algorithms to recognise patterns and deviations in encrypted data, they can anticipate potential encryption keys and decode encrypted texts without the key. Furthermore, these AI methods strengthen classical encryption techniques, making them more resilient against brute-force attacks and other standard decryption methods. The combination of AI and classical cryptography has progressed considerably, with cryptography contributing to advancing AI techniques and vice versa.

AI in quantum cryptography

Integrating quantum cryptography and AI presents challenges and opportunities (Kop 2023). As quantum computing technology advances, there could be vulnerabilities in cryptographic algorithms. Still, AI's predictive abilities can help identify these weaknesses and assist in creating algorithms that are resistant to quantum computing (Zolfaghari et al.). Additionally, AI techniques can enhance quantum essential distribution procedures, ensuring secure communication in quantum networks. While this field is still in its early stages, it has the potential to bring about transformative advancements in secure communication shortly.

Quantum cryptography

Principles of quantum cryptography

The security of quantum cryptography is based on the principles of quantum mechanics, a field of physics that examines the behaviour of subatomic particles. It functions because data preserved in quantum states cannot be replicated or accessed without altering the original state. This fundamental concept, the "no-cloning theorem," is essential in safeguarding quantum cryptographic networks (Shapna Akter, 2023).

Quantum key distribution

An encrypted approach that uses principles of quantum physics to generate and distribute cryptographic keys between two entities is known as quantum key distribution (QKD) (Gyongy-osi and Imre 2020; Tsai et al. 2021). When it comes to QKD protocols, the BB84 protocol is among the most used ones. One important thing about QKD is that it can identify any kind of eavesdropping effort. Intercepting the exchanged quantum keys would impair the conveyed quantum states. According to Diamanti et al. (2016), this would promptly notify the parties involved in the communication of any potential security violation.

Protocols for quantum cryptography

Quantum cryptography techniques have several uses beyond QKD. For example, quantum secure direct communication, quantum coin tosses, and quantum digital signatures. These protocols guarantee stronger security protections by using quantum physics to accomplish tasks that conventional encryption cannot (Broadbent et al. 2015).

Problems and their resolutions

Although quantum cryptography raises exciting new possibilities for safe communication, it is not without its share of obstacles. Challenges including noise, quantum channel loss, and technical limitations make real-world implementation of QKD networks challenging (Lovic 2020). Nevertheless, scientists are making great strides to find solutions to these problems. To close the gap between classical and quantum encryption, post-quantum cryptography (PQC) provides algorithms that are resistant to quantum attacks (Tsai et al. 2021). Fusion of artificial intelligence and quantum cryptography

Collaborative methods

New possibilities for safe computing and enhanced cryptographic protocols have never existed before thanks to the coming together of artificial intelligence and quantum cryptography. Complex AI models highlight the critical need for quantum-secure algorithms. With the use of quantum computing, AI algorithms can now handle massive datasets in polynomial time, greatly improving the efficiency and effectiveness of AI operations.

AI for enhanced quantum cryptographic protocols

Quantum cryptographic protocols such as BB84 can be optimised using AI's machine learning capabilities (Shor

1994). By analysing quantum states and predicting the likelihood of eavesdropping, artificial intelligence can dynamically adjust quantum key distribution parameters to improve security. In addition, AI can aid in developing post-quantum cryptographic algorithms, ensuring resistance to quantum computer attacks.

Quantum computing for AI model security

Novel encryption techniques can be introduced when combining quantum computing with AI, making AI models more secure (Bennett and Brassard 2020). Quantum bits (qubits) can simultaneously represent multiple states, providing a higher-dimensional computation space for artificial intelligence that can be utilised to develop ever-evolving encryption systems. This type of dynamic encryption can present difficulties for potential attackers (Mallow et al. 2022).

Potential risks and mitigations

Integrating artificial intelligence and quantum cryptography holds promise but is not without risk. A constantly evolving encryption system may introduce new vulnerabilities or be challenging to administer. It is essential to balance innovation and risk management, ensuring that ethical and security considerations remain at the forefront of development as quantum technologies advance.

Applications and implications

The convergence of quantum computing and AI has made significant strides in several scientific domains, including the field of cryptography. The power of quantum computation has improved the encryption methodologies of AI algorithms, making them more impregnable. Moreover, cryptography is evolving with the emergence of quantum key distribution (QKD), which exploits the singular traits of quantum mechanics.

In addition to cryptography, quantum computing is revolutionising biochemical research by providing cutting-edge computational potential. Quantum computers could simulate intricate biochemical interactions and lead to significant medical advancements.

The consolidation of quantum computing and AI holds tremendous potential to revolutionise various industries. However, the ongoing development of these technologies also brings ethical dilemmas to the forefront. Quantum capabilities could decrypt sensitive data, posing privacy risks, and the vast potential of quantum-AI convergence may produce dependencies that can be exploited maliciously.

To harness the full potential of quantum and AI integration while mitigating associated risks, policymakers must proactively understand the complexities of these technologies. Regulatory bodies must ensure data privacy and security while safeguarding individual rights and societal welfare. The difficulty lies in balancing the potential benefits and risks of these technologies.

The combination of quantum computing and AI has tremendous potential in various scientific domains and industries. However, it is essential to consider these technologies' ethical considerations and regulatory implications to harness their potential fully. Policymakers and regulatory bodies must ensure data privacy and security while safeguarding individual rights and societal welfare.

Case studies: the intersection of AI and quantum cryptography

Implementation of AI in quantum cryptographic systems

The convergence of AI and quantum mechanics has paved the way for innovative encryption methods that efficiently tackle the ever-changing and increasingly complex security risks (Awan et al. 2022). By combining the power of quantum computing with AI algorithms, these techniques can effectively safeguard sensitive data and prevent unauthorised access, ensuring the highest level of protection for critical information (Taylor 2020).

Real-world applications and results

When it comes to the safety of customer information and financial transactions, quantum AI has been a game-changer. Improved security measures that can adapt to new threats have resulted from changes in encryption methods brought about by AI methodologies. Identifying sophisticated and insider threats is challenging with traditional security measures due to their limitations. Cybersecurity methods rooted on artificial intelligence are essential in light of the fact that cybercriminals have started automating assaults via the use of AI, data poisoning, and model theft.

A few examples of such techniques include the CS-FSM approach and the K-nearest neighbour (KNN) algorithm. The CS-FSM approach guarantees the security of financial information by encrypting and decrypting data using the enhanced encryption standard (EES) algorithm. By leveraging training data to make predictions, the KNN algorithm is able to identify and prevent malware infections. Improved cybersecurity system performance is achieved by the use of these technologies, which in turn improve data privacy, scalability, risk reduction, data protection, and attack prevention.

More safe and efficient transactions have been made possible by the use of quantum artificial intelligence in the retail sector. Retailers can protect their customers' data and guarantee smooth transactions by harnessing the potential of quantum AI. Customers' sensitive information can be reliably protected by this system.

Major improvements to cryptography systems may result from combining artificial intelligence with quantum mechanics. Although the transition to quantum cryptography has

even if it has many advantages, there are certain obstacles to implementation that may be solved with good preparation and execution. Particularly in industries like retail, where consumer data and transaction security have been considerably enhanced, the advantages of integrating quantum AI into cryptography are apparent.

Discussion

Data protection and transaction security in several sectors stand to be radically transformed by integrating AI and quantum physics into cryptography systems. Important for protecting sensitive information, this convergence makes systems stronger and more secure, able to endure ever-changing cyber assaults. It paves the way for new forms of cryptography and algorithms that are resistant to quantum computing.
In order to move this area forward, researchers need to keep coming up with new ideas and investigating the ethical implications and long-term viability of these technologies. By establishing regulations that encourage best practices, policymakers may encourage R&D while also protecting the privacy and security of individuals' personal information. Experts in the field should put money into R&D, keep up with technological developments, and teach their employees to use these new tools. Policies and standards influencing the rollout of these technologies are areas in which they should actively engage.
In an age when quantum computing is poised to make a big splash, the prospect of establishing a secure computational environment is tantalizing, and the advantages of combining AI with quantum cryptography are enormous. The banking, e-commerce, healthcare, telecom, and national security sectors might all benefit greatly from an uptick in customer confidence if data security were to improve across the board.
The topic that is developing at the crossroads of artificial intelligence and quantum cryptography has the potential to improve digital security on a global scale and ensure the continued viability of cryptographic systems in the future. We can fully use these technologies and elevate data security to new heights by international cooperation in creating global standards and procedures.

The future of AI-powered quantum cryptography

We need to get more into the many industries that are using quantum cryptography driven by AI. Researchers may learn more about the practical difficulties and opportunities in each sector if they do this. As a result, quantum cryptography driven by artificial intelligence (AI) may find more efficient and productive uses. Given the rapid advancements in technology, it is crucial to carefully examine the ethical implications, especially those related to data privacy and the risk of misuse. It is imperative that we address these concerns head-on and put safeguards in place to prevent any unintended harm that may result from using new technologies. Therefore, it is essential to think carefully about how to address new discoveries and their consequences, as well as the possible effects on people and society as a whole.
Given the rapid progress in AI and quantum physics, it is crucial to carefully examine the robustness and adaptability of these processes. By doing this thorough analysis, we can guarantee their durability and flexibility to accommodate future changes.
Working together with experts in artificial intelligence and quantum physics has the potential to extend research capacities. They may advance scientific research more comprehensively by pooling their knowledge. Quantum cryptography and artificial intelligence have great promise. In the future, with hard work and study, this technology may be completely uncovered.

Conclusion

We have shown how artificial intelligence (AI) and quantum cryptography (QC) are interdependent, and how integrating these two fields may strengthen security and improve cryptographic systems. The integration of AI with quantum cryptography has brought about significant progress in industries like e-commerce and banking. This has allowed for the creation of strong security procedures and has strengthened the confidence of customers in these areas.
Research on AI-driven quantum cryptography is continuing at a breakneck pace, and significant advances are anticipated in the near future. Emerging areas of research and development in the field of cryptography include safe multi-party computing (MPC), automated cryptographic protocol design, post-quantum cryptography, hybrid systems, and quantum machine learning for cryptanalysis.
Combining quantum-resistant algorithms with more conventional cryptographic techniques is an area of intense investigation. The development and optimization of these hybrid systems for optimal efficiency and security may greatly benefit from AI-powered analysis and optimization. To better protect users from both conventional and quantum encryption attacks, these hybrid systems combine the best features of the two.

In the automated design of cryptographic protocols, AI, specifically machine learning and neural networks,

is a promising research direction. AI algorithms can analyse vast amounts of data to identify patterns and potential vulnerabilities in cryptographic protocols, leading to more robust and secure system design. This approach could lead to the discovery of novel cryptographic methods inherently resistant to quantum attacks.

Improving the performance and reliability of QKD systems with the application of AI is now a topic of ongoing research. Optimizing the QKD process, reducing mistakes, and enhancing key generation rates may be achieved with the use of AI algorithms. One example is adaptive QKD, which makes use of AI to dynamically alter the QKD system's settings in reaction to shifting environmental circumstances and any security risks.

Post-quantum cryptography methods are anticipated to be developed at a faster pace by AI. Artificial intelligence (AI) may steer the development of new quantum-resistant cryptographic systems by mimicking quantum assaults, which can reveal possible flaws in existing algorithms. A new generation of cryptographic algorithms that can protect data from both conventional and quantum computing threats may be born out of this. Cryptoanalysis may benefit from the new discipline of quantum machine learning, which integrates quantum computers with ML methods. Cryptanalysis might become more efficient and speedier with the use of quantum-enhanced machine learning. The results of this study may provide light on how secure cryptography methods are in the face of sophisticated quantum computing attacks.

Improved and more efficient secure multi-party computing (MPC) is anticipated as a result of developments in artificial intelligence and quantum cryptography. By helping to optimize the algorithms and protocols utilized by MPC, AI can guarantee that several parties may securely collaborate on computations without disclosing any specific data inputs.

Nevertheless, it is crucial to think about the moral consequences and make sure that developments in AI-driven quantum cryptography are in line with privacy concerns and worldwide data protection norms as these fields grow. Implications for ethical application and worldwide regulation are among the problems and opportunities presented by the potential of AI-driven quantum cryptography, which holds the promise of improved efficiency and security. Businesses relying on encrypted data transfers should invest in AI-quantum science research and development so we can learn more about AI-driven quantum cryptography. This has the potential to enhance data security by creating cryptographic systems that are more robust and adaptive. Also, companies should make educating their personnel to use these new technology a top priority.

Finally, there is great promise in the emerging area of artificial intelligence (AI) combined with quantum cryptography for the improvement of data security and privacy. The field is poised for a revolution thanks to ongoing research and advancements in areas such as secure multi-party computation, post-quantum cryptography, automated cryptographic protocol design, quantum key distribution enhancements, and hybrid cryptographic systems. Nevertheless, it is of utmost importance to think about the moral consequences and make sure that developments in quantum cryptography driven by AI are in line with international privacy regulations and data protection norms.

References

Advisera, "What is the meaning of ISO 27001?". https://advisera.com/27001academy/what-is-iso-27001/

Agrawal A, et al. Software security estimation using the hybrid fuzzy ANP-TOPSIS approach: design tactics perspective. Symmetry. 2020;12(4):598. https://doi.org/10.3390/SYM12040598.

Aldoseri A, Al-Khalifa KN, Hamouda AM. Re-thinking data strategy and integration for artificial intelligence: concepts, opportunities, and challenges. Appl Sci. 2023;13(12):7082. https://doi.org/10.3390/APP13127082.

Alyami H, et al. The evaluation of software security through quantum computing techniques: a durability perspective. Appl Sci. 2021;11(24):11784. https://doi.org/10.3390/APP112411784.

Awan U, Hannola L, Tandon A, Goyal RK, Dhir A. Quantum computing challenges in the software industry. A fuzzy AHP-based approach. Inf Softw Technol. 2022;147:106896. https://doi.org/10.1016/J.INFSOF.2022.106896.

Ayoade O, Rivas P, Orduz J. Artificial intelligence computing at the quantum level. Data. 2022;7(3):28. https://doi.org/10.3390/DATA7030028.

Bennett CH, Brassard G. Quantum cryptography: public key distribution and coin tossing. Theor Comput Sci. 2020;560(P1):7–11. https://doi.org/10.1016/j.tcs.2014.05.025.

Braverman M, Ko YK, Weinstein O. Approximating the best Nash equilibrium in no (1ogn)-time breaks the exponential time hypothesis. Proc West Mark Ed Assoc Conf. 2015;2015-Janua(January):970–82. https://doi.org/10.1137/1.9781611973730.66.

Broadbent A, Schaffner C, Broadbent Abroadbe BA, Uottawaca B, Schaffner C. Quantum cryptography beyond quantum key distribution. Des Codes Cryptogr. 2015;78(1):351–82. https://doi.org/10.1007/S10623-015-0157-4.

Catril Opazo JE, NIST cybersecurity framework in South America: Argentina, Brazil, Chile, Colombia, and Uruguay (2021)

Diamanti E, Lo HK, Qi B, Yuan Z. Practical challenges in quantum key distribution. Npj Quantum Inf. 2016;2(1):1–12. https://doi.org/10.1038/npjqi.2016.25.

Diffie W, Hellman ME. New directions in cryptography. IEEE Trans Inf Theory. 1976;22(6):644–54. https://doi.org/10.1109/TIT.1976.1055638.

Eisenhardt KM. Building theories from case study research. Acad Manag Rev. 1989;14(4):532. https://doi.org/10.2307/258557.

Elaziz A, Raheman F. The future of cybersecurity in the age of quantum computers. Fut Internet. 2022;14(11):335. https://doi.org/10.3390/FI14110335.

Feistel H, Block cipher cryptographic system (1971)

GDPR, What is GDPR, the EU's new data protection law?—GDPR.eu. Accessed 07 Jul 2023. https://gdpr.eu/what-is-gdpr/

Gill SS, et al. AI for next generation computing: Emerging trends and future directions. Internet of Things. 2022;19:100514. https://doi.org/10.1016/J.IOT.2022.100514.

Gupta S, Modgil S, Bhatt PC, Chiappetta Jabbour CJ, Kamble S. Quantum computing led innovation for achieving a more sustainable Covid-19 healthcare industry. Technovation. 2023;120:102544. https://doi.org/10.1016/J.TECHNOVATION.2022.102544.

Gyongyosi L, Imre S. Secret key rate adaption for multicarrier continuous-variable quantum key distribution. SN Comput Sci. 2020;1(1):1–17. https://doi.org/10.1007/s42979-019-0027-7.

ICO, Information Commissioner's Office (ICO): The UK GDPR, UK GDPR guidance and resources. Accessed 08 July 2023. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/lawful-basis-for-processing/consent/

ISO, "ISO/IEC 27035–1:2016—Information technology—Security techniques—Information security incident management—Part 1: Principles of incident management." Accessed 25 July 2023. https://www.iso.org/standard/

60803.html
ISO, "ISO - International Organization for Standardization." Accessed 26 Dec 2017. https://www.iso.org/home.html
ISO, "ISO/IEC 27001 and related standards Information security management 2022
ISO, "ISO/IEC DIS 42001 - Information technology—Artificial intelligence—Management system." Accessed 06 April 2023. https://www.iso.org/standard/81230.html
Johnson C, Badger L, Waltermire D, Snyder J, Skorupka C. Guide to cyber threat information sharing. NIST Spec Publ. 2016. https://doi.org/10.6028/NIST.SP.800-150.
Kop M. Quantum-ELSPI: a novel field of research. Digit Soc. 2023;2(2):1–17. https://doi.org/10.1007/S44206-023-00050-6.
Kumar M. Post-quantum cryptography Algorithm's standardization and performance analysis. Array. 2022;15:100242. https://doi.org/10.1016/J.ARRAY.2022.100242.
Liddell HG. A greek-english lexicon. Cape Palmas: Harper; 1894.
Lovic V, Quantum key distribution: advantages, challenges and policy 2020. https://doi.org/10.17863/CAM.58622
Mallow GM, Hornung A, Barajas JN, Rudisill SS, An HS, Samartzis D. Quantum computing: the future of big data and artificial intelligence in spine. Spine Surg Relat Res. 2022;6(2):93. https://doi.org/10.22603/SSRR.2021-0251.
NIST, "Advanced Encryption Standard (AES), 2001. Accessed 19 March 2023. https://web.archive.org/web/20170312045558/http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf
NIST, "Framework for Improving Critical Infrastructure Cybersecurity," 2014. Accessed 24 Dec 2017. https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf
NIST, "Cybersecurity Framework Version 1.1," 2018
NIST, "Product Integration using NVD CVSS Calculators," 2022. https://nvd.nist. gov/Vulnerability-Metrics/Calculator-Product-Integration
NIST, "Key Management - Symmetric Block Ciphers, Pair-Wise Key Establishment Schemes," 2022, [Online]. https://csrc.nist.gov/projects/key-manag ement/key-establishment
NIST, "Artificial intelligence | NIST." Accessed 06 April 2023. https://www.nist.gov/artificial-intelligence
NIST, "AI Risk Management Framework | NIST," National Institute of Standards and Technology. Accessed 18 April 2023. Available: https://www.nist.gov/ itl/ai-risk-management-framework
NIST, "Software Security in Supply Chains: Software Bill of Materials (SBOM) | NIST," National Institute of Standards and Technology. Accessed 18 April 2023. https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/software-security-supply-chains-software-1
NIST, "Post-Quantum Cryptography | CSRC | Competition for Post-Quantum Cryptography Standardisation," 2023. Accessed 06 Sept 2023. https://csrc. nist.gov/projects/post-quantum-cryptography
NIST, "SP 800-61 Rev. 2, Computer Security Incident Handling Guide | CSRC." Accessed 25 July 2023. https://csrc.nist.gov/pubs/sp/800/61/r2/final
NIST, "Post-Quantum Cryptography | CSRC | Selected Algorithms: Public-key Encryption and Key-establishment Algorithms," 2023. Accessed 06 Sept 2023. https://csrc.nist.gov/Projects/post-quantum-cryptography/selec ted-algorithms-2022
NIST, "NVD—CVSS v3 Calculator," CVSS Version 3.1. Accessed 03 Jan 2023. https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator
NIST 800-53, "Security and Privacy Controls for Information Systems and Organizations 2020
NIST Advanced Manufacturing Office, "Advanced Manufacturing Partnership," 2013. Accessed 04 May 2020. https://www.nist.gov/amo/programs
NIST C, *Cybersecurity Framework | NIST*. 2016. https://www.nist.gov/cyberframework
NIST, "Block Cipher Techniques." https://csrc.nist.gov/Projects/block-cipher-techniques
NIST, "Post-Quantum Cryptography PQC." https://csrc.nist.gov/Projects/post-quantum-cryptography
NIST, "Privacy-Enhancing Cryptography PEC." https://csrc.nist.gov/Projects/pec
NIST, "Lightweight Cryptography." https://csrc.nist.gov/Projects/lightweight-cryptography
NIST, "Cybersecurity Framework." https://www.nist.gov/cyberframework/getti ng-started
NIST, "Hash Functions," 2020. https://csrc.nist.gov/Projects/Hash-Functions
NIST, "NIST Special Publication 800–128," 2011. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-128.pdf
NIST, "NIST Version 1.1," National Institute of Standards and Technology, U.S. Department of Commerce. https://www.nist.gov/news-events/news/ 2018/04/nist-releases-version-11-its-popular-cybersecurity-framework
Nitaj A, Rachidi T. Applications of neural network-based AI in cryptography. Cryptography. 2023;7(3):39. https://doi.org/10.3390/CRYPTOGRAPHY7030039.
Paar C, Pelzl J. Understanding cryptography: a textbook for students and practitioners. Berlin: Springer; 2009.
Petrov M, Adapted SANS cybersecurity policies for NIST cybersecurity framework
Rivest RL, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Commun ACM. 1978;21(2):120–6.
Rutkowski A, et al. CYBEX. ACM SIGCOMM Comput Commun Rev. 2010;40(5):59–64. https://doi.org/10.1145/1880153.1880163.
Sahu K, Srivastava RK, Kumar S, Saxena M, Gupta BK, Verma RP. Integrated hesitant fuzzy-based decision-making framework for evaluating sustainable and renewable energy. Int J Data Sci Anal. 2023;16(3):371–90. https://doi.org/10.1007/S41060-023-00426-4.
Sevilla J, Moreno P, Implications of quantum computing for artificial intelligence alignment research 2019
Shamshad S, Riaz F, Riaz R, Rizvi SS, Abdulla S. An enhanced architecture to resolve public-key cryptographic issues in the internet of things (IoT), employing quantum computing supremacy. Sensors (basel). 2022;22(21):271–6. https://doi.org/10.3390/S22218151.
Shapna Akter M Quantum cryptography for enhanced network security: a comprehensive survey of research. Developments, and Future Directions 2023
Shor PW, Algorithms for quantum computation: discrete logarithms and factoring. In: Proceedings—annual IEEE symposium on foundations of computer science, FOCS, 1994. Pp. 124–134. https://doi.org/10.1109/SFCS.1994.365700
SWID, "Software Identification (SWID) Tagging | CSRC | NIST," National Institute of Standards and Technology. Accessed 19 April 2023. [Online]. https://csrc.nist.gov/projects/Software-Identification-SWID
Tabassi E, AI risk management framework | NIST. (2023) https://doi.org/10.6028/NIST.AI.100-1
Takahashi T, Kadobayashi Y. Reference ontology for cybersecurity operational information. Comput J. 2015;58(10):2297–312. https://doi.org/10.1093/COMJNL/BXU101.
Taylor RD. Quantum artificial intelligence: a 'precautionary' U.S. approach? Telecomm Policy. 2020;44(6):101909. https://doi.org/10.1016/J.TELPOL.2020.101909.
Tsai CW, Yang CW, Lin J, Chang YC, Chang RS. Quantum key distribution networks: challenges and future research issues in security. Appl Sci. 2021;11(9):3767. https://doi.org/10.3390/APP11093767.
Udroiu A-M, Dumitrache M, Sandu I, Improving the cybersecurity of medical systems by applying the NIST framework. In 2022 14th international conference on electronics, computers and artificial intelligence (ECAI). IEEE, 2022, pp 1–7
Yin KR, Case study research: design and methods (2009) Accessed 25 April 2023. https://books.google.com/books?hl=en&lr=&id=FzawIAdilHkC&oi=fnd&pg=PR1&dq=Yin,+R.+K.+(2009).+Case+study+research:+Design+and+methods+(Vol.+5).+sage.&ots=l_5Q4fkSYt&sig=flCdRmFfBrFKJIHQRApE252vNhQ#v=onepage&q&f=false
Yin RK. Case study research: design and methods, vol. 5. Newcastle upon Tyne: Sage; 2009b.
Ying M. Quantum computation, quantum theory and AI. Artif Intell. 2010;174(2):162–76. https://doi.org/10.1016/J.ARTINT.2009.11.009.
Ying M. Quantum computation, quantum theory and AI ☆. Artif Intell. 2010;174:162–76. https://doi.org/10.1016/j.artint.2009.11.009.
Zolfaghari B, Rabieinejad E, Yazdinejad A, Parizi RM, Dehghantanha A, Crypto makes AI evolve