Radanliev
Journal of Analytical Science and Technology (2024) 15:4
https://doi.org/10.1186/s40543-024-00416-6

Journal of Analytical Science and Technology

REVIEW

Open Access

Artificial intelligence and quantum cryptography

Petar Radanliev[1,2*]

Abstract

The technological advancements made in recent times, particularly in artificial intelligence (AI) and quantum computing, have brought about significant changes in technology. These advancements have profoundly impacted quantum cryptography, a field where AI methodologies hold tremendous potential to enhance the efficiency and robustness of cryptographic systems. However, the emergence of quantum computers has created a new challenge for existing security algorithms, commonly called the 'quantum threat'. Despite these challenges, there are promising avenues for integrating neural network-based AI in cryptography, which has significant implications for future digital security paradigms. This summary highlights the key themes in the intersection of AI and quantum cryptography, including the potential benefits of AI-driven cryptography, the challenges that need to be addressed, and the prospects of this interdisciplinary research area.

Keywords Artificial intelligence, Quantum algorithms, Neural networks, Quantum-AI integration, Quantum threats, AI-enhanced security, Quantum information processing

Introduction

Quantum cryptography is an advanced subfield of cryptography that employs the principles of quantum mechanics to ensure secure communication. Unlike classical cryptography, which typically utilises complex mathematical algorithms to encode data, quantum cryptography uses the physical properties of quantum particles, such as photons, to create an inherently secure communication system.

The cornerstone of quantum cryptography is quantum key distribution (QKD), a method that enables two parties to generate a shared random secret key, which is essential for encrypting and decrypting messages in such a way that any eavesdropper's presence can be detected. The security of QKD is rooted in fundamental quantum mechanical principles, such as the Heisenberg uncertainty principle and quantum entanglement.

The Heisenberg uncertainty principle states that measuring a quantum system inevitably alters its state. Thus, any eavesdropper attempts to intercept and measure the quantum keys will introduce detectable anomalies, alerting the communicating parties to the presence of an intrusion.

Quantum entanglement is another fundamental concept in quantum mechanics that links two quantum particles so that the state of one instantaneously affects the state of the other, regardless of the distance separating them. This property can be used to establish a secure key between two parties.

The primary benefit of quantum cryptography is its potential to provide communication channels impervious to eavesdropping. It overcomes many limitations of traditional cryptographic methods, particularly in advancing computational power, such as quantum computers. This makes it a crucial study area for ensuring the security of sensitive data in the quantum computing era.

*Correspondence:
Petar Radanliev
radanliev@yahoo.com
[1] Department of Computer Sciences, University of Oxford, Oxford, UK
[2] School of Management, University of Bath, Bath, UK

The convergence of AI and quantum cryptography has been a recent topic of great interest among scientific and technological experts. Both fields have changed their respective industries: AI has made remarkable strides in healthcare and finance by leveraging its exceptional ability to process data, recognise patterns, and make informed decisions. In parallel, quantum cryptography provides unparalleled security based on physical laws, primarily through quantum key distribution (QKD) and related protocols.

The alignment of AI and quantum cryptography is no accident. In our present digital age, marked by significant data transfers and escalating cybersecurity threats, it's logical to integrate AI's computational power with quantum cryptography's unbreakable security measures. By examining extensive amounts of data, AI algorithms have the potential to elevate quantum cryptographic procedures, making them more robust and efficient. Meanwhile, quantum cryptography can provide a secure framework for AI systems, ensuring that the data and algorithms they manage remain impervious to breaches.

Quantum cryptography has become increasingly important due to the imminent arrival of quantum computers. These computers can crack classical cryptographic codes in a short amount of time, which poses a significant threat to modern cybersecurity. Therefore, combining AI and quantum cryptography is not just an academic exercise but a necessary measure to address this pressing issue.

This review thoroughly explores the intersection of AI and quantum cryptography. We take a deep dive into the historical development of both areas, how they interact with each other, and the challenges and opportunities they bring at the same time, and we also spotlight significant experiments and applications in the field. We aim to give readers a complete comprehension of the current research environment and to stress the immense potential of this combination for the future.

Rationale

The convergence of AI and quantum cryptography represents a ground-breaking union of two transformative fields. AI has transformed how we process and analyse data, while quantum cryptography offers unparalleled security in information transmission. As these two domains continue to evolve, their intersection provides a captivating area for exploration. This paper explores the interplay, potential advancements, and challenges of AI and quantum cryptography.

Objectives of the study

This study aims to explore the historical background of AI and quantum cryptography and examine the current research and application scenario at their intersection. We will also analyse the challenges of integrating AI with quantum cryptography and highlight possible opportunities and prospects in this interdisciplinary field.

Research questions

1. How have the fields of artificial intelligence and quantum cryptography evolved historically?
2. How can AI improve Quantum Cryptographic protocols and vice versa?
3. What are the main challenges in combining AI and quantum cryptography?
4. What opportunities emerge from the interaction of AI and quantum cryptography, and how might they influence future research 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 study of cryptography, also known as cryptology, originates from the Greek words kryptós and graphein, meaning hidden or secret and to write, respectively, and logia, meaning to study. In Greek, cryptography is defined as "secret writing." (Liddell 1894).

The basis of modern cryptography is cryptographic algorithms designed around the concept of 'computational hardness assumption' (Braverman et al. 2015). It finds practical applications in various sectors, such as chip-based payment cards, digital currencies, computer passwords, and military communications (Paar and Pelzl 2009). It plays a crucial role in cybersecurity and securing communications with encryption (e.g. HTTPS, PGP).

In the realm of cryptocurrencies and crypto-economics, Zero Knowledge Proofs (ZKP), cryptographic keys, and cryptographic hash functions are commonly used cryptographic techniques.

Algorithms for encryption include the triple data encryption algorithm (3DEA) of the advanced encryption standard (AES). It encrypts data three times with the data encryption standard (DES) cypher, 3DES (Triple DES). DES is based on the Lucifer (cypher) symmetric-key algorithm (known as Data Encryption Algorithm—DEA) (Feistel 1971).

Another popular encryption method is the asymmetric RSA public-key encryption algorithm developed by Ron Rivest, Adi Shamir, and Leonard Adleman (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.

The original request for submissions[3] for the NIST lightweight cryptography standard resulted in 57 solutions submitted for review by NIST. Lightweight cryptography ensures that data is securely transmitted from and to the "innumerable" tiny IoT devices, necessitating a new category of cryptographic algorithms. Most IoT micromachines, sensors, actuators, and other low-memory devices used for network guidance and communication operate on deficient electrical power. These devices have minimal circuitry, like the electronics in keyless entry fobs and Radio-Frequency Identification (RFID) tags used in supply chains and warehouses. Comparatively, even the most basic mobile phone would have a significantly less limited chip, and the primary advantage of these Internet of Things technologies is their low cost and small size. Existing cryptographic algorithms require more computational power and electronic resources than IoT devices have. Consequently, the primary weakness of all IoT devices is tied to their primary strength.

Quantum cryptography presents a unique approach compared to lightweight cryptography like Ascon, which caters to low-memory devices like IoT devices. It follows the principles of quantum mechanics and primarily focuses on quantum key distribution (QKD), offering security that is theoretically impossible to break.

NIST is concentrating on Ascon to protect data on small IoT devices with limited computing abilities. On the other hand, quantum cryptography aims to utilise the distinctive characteristics of quantum bits (qubits) for secure communication, regardless of the device's computational power. One of the main obstacles of quantum cryptography is its current scalability and compatibility with conventional communication systems. Lightweight cryptography, on the other hand, must maintain security despite limited computational resources. Due to their computational limitations, IoT devices face challenges in employing conventional cryptographic algorithms. If direct quantum cryptography methods were to be implemented, these devices could face even more significant difficulties.

[1] https://www.nist.gov/news-events/news/2023/02/nist-selects-lightweight-cryptography-algorithms-protect-small-devices.

[2] https://csrc.nist.gov/News/2023/lightweight-cryptography-nist-selects-ascon.

[3] https://www.nist.gov/news-events/news/2018/04/nist-issues-first-call-lightweight-cryptography-protect-small-electronics.

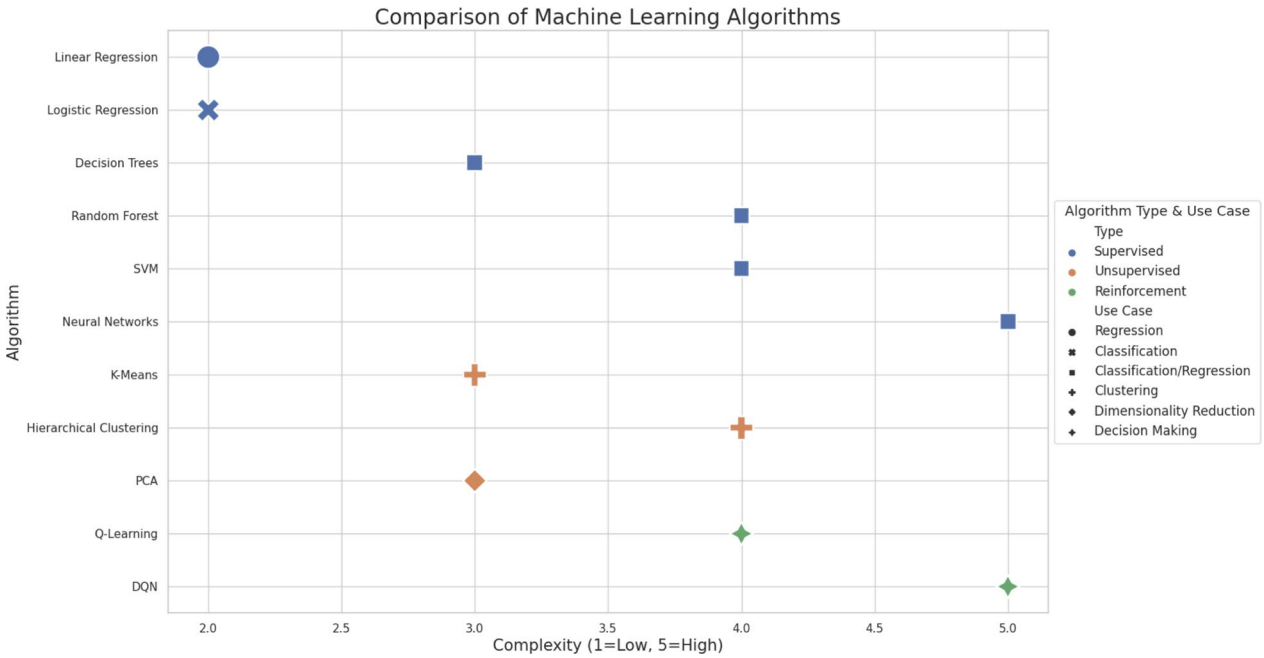

Fig. 1 Navigating through popular and traditional ML algorithms

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

The foundation of quantum cryptography can be traced back to the early twentieth century. Quantum mechanics raised challenges and opportunities for information processing due to the counterintuitive properties of quantum systems, such as superposition and entanglement.

During the 1970s and 1980s, there were significant advancements made in quantum information theory. Charles Bennett and Gilles Brassard introduced the quantum key distribution (QKD) concept in 1984 with the BB84 protocol, based on previous quantum mechanics and information theory research. This protocol utilised quantum mechanics principles to allow two parties to create a shared, secret random key that was secure due to physical laws.

In the years that followed, there was a significant development in both theoretical and practical aspects

of quantum cryptography. Besides crucial distribution, quantum cryptographic protocols have expanded their scope to include quantum digital signatures and secure direct communication. With the progress in photonics and quantum technologies, these protocols have been implemented and tested in real-world scenarios, opening doors for commercial quantum secure communication networks.

Although originating from different scientific traditions, AI and quantum cryptography have converged through fundamental insights, technological advancements, and a continuous pursuit of understanding and innovation. This convergence presents numerous opportunities and challenges, potentially transforming information security and computational intelligence.

Review of integration in AI with quantum cryptography

The technological advancements in AI and quantum computing have been monumental, leading to significant changes in various domains, including cryptography. One of the primary objectives of integrating AI with quantum cryptography is to harness AI's computational prowess to enhance the efficiency, security, and robustness of quantum cryptographic systems. AI methodologies, with their ability to process vast amounts of data, recognise intricate patterns, and adapt to new scenarios, can significantly contribute to optimising quantum cryptographic protocols and addressing the complex challenges they face.

In parallel, quantum cryptography offers a unique avenue to safeguard AI systems, given its foundational security based on the laws of quantum mechanics. This integration is timely and relevant in our digital era, characterised by extensive data exchanges and escalating cybersecurity threats. Here, the role of AI becomes crucial. By analysing and interpreting large datasets, AI algorithms can play a pivotal role in elevating the security and effectiveness of quantum cryptographic practices.

However, the emergence of quantum computers has introduced a new and formidable challenge for cryptographic systems –the 'quantum threat.' This threat looms over traditional cryptographic methods, rooted in the fact that quantum computers have the potential to break many of the cryptographic algorithms currently in use. Thus, the synergy of AI and quantum cryptography is not merely an academic pursuit but a necessary evolution in our approach to digital security. AI-driven methodologies in quantum cryptography aim to anticipate, mitigate, and robustly defend against the quantum threat, ensuring a secure computational future.

This review delves deep into the interaction between AI and quantum cryptography, exploring their historical development, the challenges presented by the advent of quantum computing, and the transformative potential of their integration. By doing so, it aims to provide a comprehensive understanding of the current landscape and the exciting prospects this interdisciplinary fusion offers for the future of secure computation.

Review of the quantum threat

The 'quantum threat' refers to the potential vulnerability of existing cryptographic systems in the face of advanced quantum computing capabilities. Cryptographic methods like RSA and ECC (Elliptic Curve Cryptography) depend on the computational difficulty of specific mathematical problems. For example, RSA relies on the challenge of factoring large prime numbers, and ECC depends on the complexity of solving the elliptic curve discrete logarithm problem. These problems, currently considered difficult for classical computers, could potentially be solved efficiently by quantum computers using algorithms such as Shor's algorithm.

Quantum computers operate on principles of quantum mechanics, such as superposition and entanglement, to process information differently than classical computers. This capability allows them to perform specific calculations much more efficiently than traditional computers. Shor's algorithm demonstrates that a quantum computer could factor large numbers exponentially faster than the best-known algorithms running on a classical computer. As a result, the encryption systems that depend on the difficulty of these problems for security would become vulnerable once sufficiently powerful quantum computers are developed.

The quantum threat is not just a theoretical concern but a near-future reality. The advent of quantum computing thus necessitates the development of new cryptographic systems that are secure against quantum attacks, often referred to as 'quantum-resistant' or 'post-quantum' cryptography. These systems aim to use algorithms and cryptographic methods that quantum computers cannot efficiently break.

Integrating AI with quantum cryptography is a strategic response to this threat. AI's advanced pattern recognition and predictive capabilities can aid in developing, testing, and optimising quantum-resistant algorithms. Moreover, AI can contribute to the real-time assessment and adaptation of cryptographic systems, making them more resilient against the rapidly evolving landscape of quantum computing. This makes the convergence of AI and quantum cryptography a critical area of research for ensuring data security and privacy in the forthcoming quantum computing era.

Research methodology

This research employs a qualitative approach within an interpretive paradigm to comprehensively investigate the intricate relationship between AI and quantum cryptography. With the emergence of standardised tools and ontologies that strive to enhance information exchange and automate vulnerability management, the cybersecurity landscape is evolving rapidly. One such tool is the 'Reference Ontology for Cybersecurity Operational Information' (Takahashi and Kadobayashi 2015). This tool provides a structured framework for cybersecurity information and facilitates its exchange within the domain of cybersecurity operations. This approach proposes a reference ontology for cybersecurity operational information that promotes collaboration and information exchange among organisations. The ontology structures cybersecurity information and aligns with industry specifications. The authors worked with cybersecurity organisations to develop the ontology and demonstrated its usability by discussing industry specification coverage. They also established an adaptable information structure that complements industry specifications and outlines a prototype cybersecurity knowledge base that facilitates information exchange. This article explores the potential usage scenarios of the ontology and knowledge base in cybersecurity operations. The proposed ontology aims to advance the exchange of cybersecurity information.

The CYBEX framework (Rutkowski et al. 2010) is a significant step towards establishing a global standard for exchanging cybersecurity information. As an ITU-T initiative, CYBEX aims to standardise how cybersecurity entities communicate and ensure the integrity of this exchange. Introducing CYBEX will reduce the fragmentation of cybersecurity information availability, allowing for a more uniform defence posture worldwide. This paper outlines the framework's specifications, practical applications, and progress. CYBEX is uniquely structured around five functional blocks: Information Description, Information Discovery, Information Query, Information Assurance, and Information Transport. Together, these blocks enhance the automation and efficiency of cybersecurity operations, potentially reducing human error and operational costs. While these works provide valuable insights and contribute to the overarching goals of security information exchange and vulnerability management, they are not the central focus of this survey. As such, our research does not delve into these areas in detail but acknowledges their significance in the broader context of cybersecurity.

This research aims to enhance our understanding of the impact of these two technological advancements on cybersecurity. This study is informed by global efforts to develop, refine, and establish a range of quantum-safe cryptography algorithms (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.

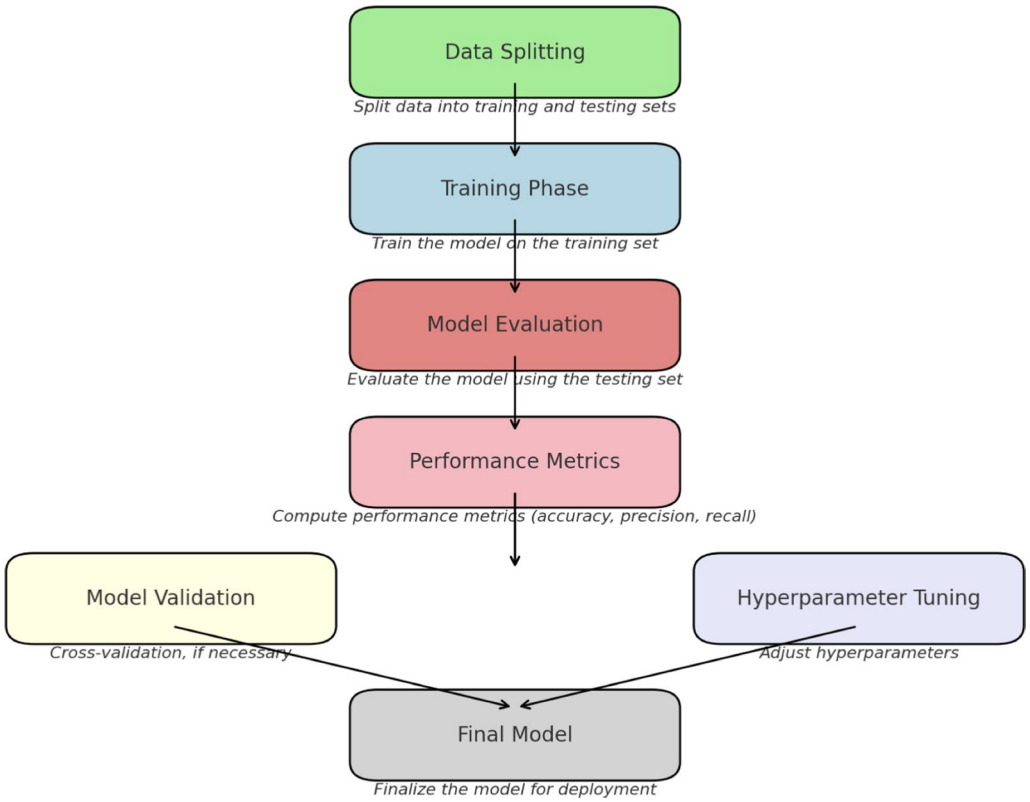

Fig. 2 AI model evaluation and validation

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 esteemed International Organization for Standardisation (ISO) and the International Electrotechnical Commission (IEC) have taken on the critical task of launching projects aimed at standardising quantum cryptographic protocols. This includes the crucial essential establishment procedures vital for the secure transmission of sensitive and confidential information. These projects ensure that quantum cryptography is widely accepted as a trusted and reliable method for secure communication in various industries, including finance, healthcare, and government. With the standardisation of these protocols, organisations can have greater confidence in the security of their communication systems, which is essential in today's increasingly interconnected world.

The National Institute of Standards and Technology (NIST) (NIST 2023a, b), a federal agency within the United States Department of Commerce, has extensively developed benchmarks and standards for quantum cryptographic systems. This ensures these systems meet rigorous security requirements for safeguarding sensitive information in the quantum computing era. NIST's efforts aim to promote a secure and reliable framework for quantum communication and cryptography, which are expected to play a vital role in the future of cybersecurity.

AI regulation presents a unique set of challenges. While standardisation issues arise in the quantum realm, AI faces its regulatory obstacles. These include concerns about data privacy, ethical considerations, and

transparency in decision-making. Addressing these concerns requires global conversations on how best to regulate AI. For instance, the General Data Protection Regulation (GDPR) in the European Union provides precise guidelines for AI decision-making processes. This ensures transparency and accountability, thereby guaranteeing the responsible use of AI. The challenges of regulating AI are complex and multifaceted, but they are necessary to ensure safe and responsible development and use of this technology.

The merging of AI and quantum cryptography presents a promising future, but obstacles exist to successfully executing, refining, and adhering to legal requirements. It is essential to adopt a collaborative methodology that involves scholars, policymakers, and industry professionals to achieve the full potential of this unification. We must acknowledge and work together to overcome the challenges as we progress.

Challenges and opportunities: integrating AI and quantum cryptography

The intersection of AI and quantum cryptography presents exciting possibilities. However, the intersection of these two ground-breaking fields is challenging. This chapter delves into the significant challenges and opportunities resulting from their integration. For example, Neural network-based AI has shown considerable promise in enhancing cryptographic systems, with several practical applications demonstrating its potential. For instance, neural networks have been successfully employed in the development of cryptographic algorithms themselves. One notable example is using machine learning techniques to design and optimise S-boxes (substitution boxes) in symmetric key cryptography. These S-boxes are critical components in many cryptographic algorithms, such as AES (advanced encryption standard), where they introduce nonlinearity and confusion into the encryption process. AI-driven methods can analyse the properties of S-boxes, such as nonlinearity and differential uniformity, to develop more secure and efficient cryptographic algorithms.

Another application is in the field of cryptanalysis. AI algorithms and profound learning models have been used to perform automated cryptanalysis on various cryptographic algorithms. By training neural networks with examples of plaintext and corresponding ciphertext, these models can learn to predict the key or decipher the messages without the key, thereby identifying potential vulnerabilities in cryptographic algorithms.

In addition to enhancing traditional cryptographic systems, neural network-based AI plays a pivotal role in addressing the challenges of quantum computers. Quantum computers exploit specific vulnerabilities in widely used cryptographic algorithms. For instance, Shor's algorithm takes advantage of quantum computers' ability to efficiently factor large numbers, thereby breaking the RSA encryption, which relies on the difficulty of factoring the product of two large prime numbers. Similarly, quantum computers can efficiently solve the discrete logarithm problem, undermining the security of ECC and Diffie-Hellman key exchange.

These vulnerabilities stem from the quantum principle of superposition, which allows quantum computers to evaluate multiple possibilities simultaneously, and quantum entanglement, which enables them to correlate the properties of separated particles. These characteristics enable quantum computers to perform specific calculations much faster than classical computers, rendering current cryptographic methods vulnerable.

Integrating AI with quantum-resistant cryptographic research is essential to developing new algorithms that can withstand the capabilities of quantum computers. For example, AI can simulate quantum attacks on cryptographic algorithms, helping researchers understand and mitigate vulnerabilities. Furthermore, AI-driven optimisation techniques can aid in the creation of more efficient and secure post-quantum cryptographic algorithms, ensuring the continued protection of digital information in the quantum era.

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

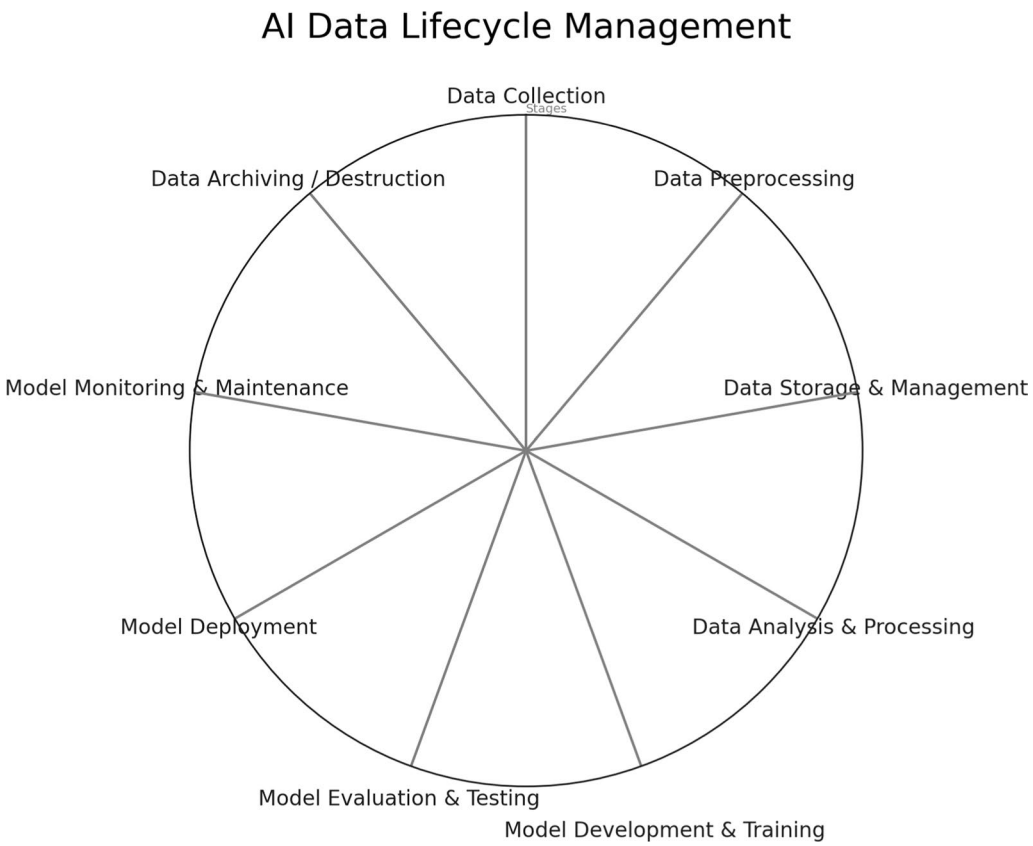

Fig. 3 Data challenges in the AI data lifecycle management caused by quantum cryptography

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.

Integrating AI with quantum cryptography is feasible, leading to significant advancements in cryptographic security. AI algorithms enhance quantum cryptographic protocols, making them more adaptable and efficient. The AI-driven approaches have effectively mitigated the quantum threat, providing a pathway to develop and optimise quantum-resistant cryptographic algorithms. Despite challenges, AI's successful implementations and potential applications in enhancing quantum cryptographic systems indicate a promising future. This includes secure communication channels, enhanced data privacy, and robust security solutions for various industries.

Continued research and development are crucial to address the challenges in real-time applications, improve scalability, reduce latency, and ensure compatibility with existing systems. The results underscore the necessity for policy development and industry engagement to facilitate the transition to quantum-secure cryptographic systems. This involves standardising practices, investing in infrastructure, and promoting collaboration among academia, industry, and policymakers. This process can be visualised in Fig. 3.

The successful implementation of AI in the context is seen in Fig. 3, requires using post-quantum cryptographic methods, particularly considering the imminent arrival of quantum computers (Aldoseri et al. 2023). However, the transition to these methods must be carefully considered and prepared, as standardisation and widespread acceptance may pose significant challenges. As such, it is crucial to prioritise the development of robust and reliable solutions that can effectively address these issues and ensure the safety and security of sensitive data.

Opportunities for enhanced security mechanisms and AI-driven quantum systems

The potential integration of AI's impressive data processing capabilities with the unassailable security of quantum cryptography could give rise to ultra-secure communication channels impervious to classical and quantum threats. With the rapid advancements in quantum computation, mounting evidence suggests that quantum systems will soon outstrip classical systems regarding computational capabilities (Ayoade et al. 2022). AI has the potential to significantly enhance quantum systems leading to faster algorithms and streamlined cryptographic protocols with far-reaching implications. Such developments could revolutionise secure communication and data transfer. The merging of quantum concepts with artificial intelligence has a potential for new research areas, attracting more significant funding in quantum cryptography and pushing the boundaries of both fields.

There are significant challenges when merging AI and quantum cryptography, but the potential rewards are vast. Researchers can unlock a wealth of possibilities that lay the foundation for new advancements in computation and security. These advancements can revolutionise how we approach these fields and significantly impact society.

Public key (PK) cryptography plays a vital role in this effort. Asymmetric cryptography, or public key (PK) cryptography, uses two mathematically linked keys: public and private. Unlike symmetric cryptography, which relies on one key for encryption and decryption, PK cryptography uses separate keys for each operation. This enhances security and ensures that sensitive data remains secure, even if an adversary intercepts the public key. PK cryptography enables secure communication and cryptographic features such as critical exchanges, digital signatures, and data encryption. It is a crucial component of modern cryptographic systems, offering enhanced security, scalability, and adaptability across various applications.

A crucial concept in cryptography is digital signature generation. To generate a digital signature, the signatory must first create a key pair consisting of a private key and a public key. The private key is kept confidential and never shared, whereas the public key is made available. A unique hash of the document or message to be signed is generated using a hash function. This hash value uniquely represents the content of the document. Hash signing occurs when the signer encrypts the generated hash value using their private key. This links their signature to a particular document. Upon encrypting the hash value, a cryptographic digital signature is generated, unique to both the document and the signer.

The combination of AI and quantum cryptography presents exciting opportunities. Despite the significant challenges that must be overcome, the potential rewards are vast, and the implications could be far-reaching. Merging these two fields can unlock a wealth of possibilities that lay the foundation for new advancements in computation and security. This could revolutionise secure communication and data transfer, leading to new research areas and pushing the boundaries of both fields.

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

Quantum key distribution (QKD) is a secure method that utilises quantum mechanics concepts to create and distribute cryptographic keys between two parties (Gyongyosi and Imre 2020; Tsai et al. 2021). The BB84 protocol is one of the most widely used protocols in QKD. The critical feature of QKD is that it can detect any attempts at eavesdropping. If a third party tries to intercept the exchanged quantum keys, the transmitted quantum states would be disrupted. This would immediately alert the communicating parties of a possible security breach (Diamanti et al. 2016).

Quantum cryptographic protocols

There are various applications of quantum cryptographic protocols aside from QKD. For instance, quantum digital signatures, quantum coin tosses, and quantum secure direct communication. These protocols use quantum mechanics to perform tasks that are impossible with traditional cryptography, thus ensuring more robust security measures (Broadbent et al. 2015).

Challenges and solutions

The concept of quantum cryptography presents new possibilities for secure communication, but it also comes with its own set of challenges. In the real world, implementing QKD networks is difficult due to issues such as quantum channel loss, noise, and technological limitations (Lovic 2020). However, researchers are actively working to overcome these obstacles. Post-quantum cryptography (PQC) offers algorithms that can withstand quantum adversaries, bridging the gap between classical and quantum cryptography techniques (Tsai et al. 2021).

Intersection of AI and quantum cryptography

Synergistic approaches

The convergence of AI and quantum cryptography presents unprecedented opportunities for secure computations and improved cryptographic protocols. As AI models become more complex, quantum-secure algorithms are of paramount importance. Quantum computing provides a platform for AI algorithms that can process vast amounts of data in polynomial time, enabling AI operations to be performed more quickly and effectively.

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

Quantum AI has significantly improved data protection and transaction security in the banking industry. AI methods have changed encryption techniques, leading to more advanced security measures that can counter constantly evolving threats. Traditional security measures have limitations that make detecting advanced and insider threats difficult. Cyber attackers have been using AI, data poisoning, and model theft to automate attacks, making it necessary to use cybersecurity techniques based on artificial intelligence.

The CS-FSM method and the K-nearest neighbour (KNN) algorithm are two such methods. The CS-FSM method uses the enhanced encryption standard (EES) algorithm to encrypt and decrypt data, ensuring information security in the financial sector. The KNN algorithm detects and prevents malware attacks by making predictions using training data. These methods enhance the performance of cybersecurity systems, improving their resistance to cyberattacks, data privacy, scalability, risk reduction, data protection, and attack prevention.

Quantum artificial intelligence has also been adopted in retail to provide more secure and efficient transactions. By leveraging quantum AI's power, retailers can safeguard their customers' data and ensure seamless transactions. This technology offers a highly reliable solution to protect customers' sensitive information.

The fusion of AI and Quantum Mechanics can lead to significant advancements in cryptographic systems. While shifting to quantum cryptographic systems has

numerous benefits, it also presents implementation challenges that can be overcome with careful planning and execution. The benefits of incorporating quantum artificial intelligence into cryptography are evident, particularly in sectors such as retail, where customer data protection and transaction security have been significantly improved.

Discussion

Integrating AI and quantum mechanics in cryptographic systems has tremendous potential to revolutionise data protection and transaction security in various industries. This intersection creates more robust and secure systems that can withstand evolving cyber threats, crucial for safeguarding sensitive information. It also allows for the development of innovative cryptographic techniques and quantum-resistant algorithms.

To advance this field, researchers must continue to innovate and explore these technologies' ethical implications and sustainability. Policymakers should support research and development while ensuring data privacy and security by creating policies that promote best practices. Industry professionals should invest in research and development, stay updated with the latest advancements, and train the workforce to adapt to these new technologies. They should also participate in shaping policies and standards that affect the deployment of these technologies.

The potential benefits of integrating AI and quantum cryptography are vast and exciting, and it holds the promise of creating a secure computational environment in an era where quantum computing is set to become a significant player. By enhancing data security, industries could increase consumer trust and transform online banking, e-commerce, healthcare, national security, and telecommunications transactions.

Overall, the intersection of AI and quantum cryptography is a dynamic and evolving field that can future-proof cryptographic systems and enhance global digital security. With international collaboration in establishing global standards and practices, we can realise the full potential of these technologies and take data security to a whole new level.

The future of AI-powered quantum cryptography

We must delve deeper into the various sectors utilising AI-powered quantum cryptography. By doing so, researchers can gain a better understanding of the practical challenges and advantages that arise within each sector. This, in turn, can lead to the development of more effective and efficient applications of AI-powered quantum cryptography.

Considering recent technological progress, it is imperative to thoroughly analyse the ethical considerations, particularly concerning data privacy and the possibility of abuse. We must take these concerns seriously and ensure that measures are in place to safeguard against any potential negative consequences of using innovative technologies. As such, it is crucial to consider the implications of any new developments and approach them cautiously, always considering the potential impact on individuals and society.

It is imperative to thoroughly scrutinise the sustainability and flexibility of these mechanisms, particularly considering the constant advancements in both AI and quantum mechanics. This careful examination will enable us to ensure their long-term effectiveness and potential for adaptation to future developments.

The potential for increased research capabilities can be achieved by collaborating with AI and quantum physics professionals. By combining their expertise, a more comprehensive approach can be taken towards advancing scientific inquiry. The potential of AI and quantum cryptography is highly promising. Through dedicated research, this technology can be fully unlocked in the future.

Conclusion

Our discussion has explored the intricate relationship between AI and quantum cryptography, revealing that combining these two domains can effectively enhance cryptographic systems and fortify security measures. Integrating AI and quantum cryptography has led to remarkable advancements in sectors such as banking and e-commerce, facilitating the development of robust security protocols and bolstering users' trust in these sectors.

The field of AI-driven quantum cryptography is rapidly evolving, with ongoing research and expected advancements that have the potential to revolutionise the field. Hybrid cryptographic systems, automated cryptographic protocol design, quantum key distribution enhancements, post-quantum cryptography development, quantum machine learning for cryptanalysis, and secure multi-party computation (MPC) are hotspots for innovation and breakthroughs.

Researchers are actively exploring the integration of quantum-resistant algorithms with traditional cryptographic methods. AI-powered optimisation and analysis can be crucial in developing and fine-tuning these hybrid systems for maximum efficiency and security. These hybrid systems leverage the strengths of both quantum and classical cryptography, providing enhanced security against both classical and quantum threats.

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.

Research is underway to use AI to improve the performance and reliability of QKD systems. AI algorithms can help optimise the QKD process, reduce errors, and enhance key generation rates. This includes the use of AI in adaptive QKD, where the parameters of the QKD system are dynamically adjusted in response to changing environmental conditions and potential security threats.

AI is expected to accelerate the development of post-quantum cryptography algorithms. By simulating quantum attacks, AI can help identify potential weaknesses in current algorithms and guide the design of new quantum-resistant cryptographic schemes. This could lead to the creation of a new generation of cryptographic algorithms that can secure data against classical and quantum computational threats.

The emerging field of quantum machine learning, which combines quantum computing with machine learning algorithms, has potential applications in cryptanalysis. Quantum-enhanced machine learning could analyse encrypted data more efficiently, leading to faster and more effective cryptanalysis. This research could provide insights into the resilience of cryptographic algorithms against advanced quantum computing techniques.

With the advancements in AI and quantum cryptography, secure multi-party computation (MPC) is expected to become more robust and efficient. AI can assist in optimising the protocols and algorithms used in MPC, ensuring secure, collaborative computation among multiple parties without revealing individual data inputs.

However, as these research areas develop, it is essential to consider ethical implications and ensure that advancements in AI-driven quantum cryptography are aligned with global data protection standards and privacy concerns. The future of AI-driven quantum cryptography promises enhanced security and efficiency while posing challenges and responsibilities regarding ethical use and global regulation.

To advance our understanding of AI-driven quantum cryptography, companies that depend on secure data transmissions should allocate resources towards research and development that combines artificial intelligence and quantum mechanics. This could result in more resilient and adaptable cryptographic systems, ultimately improving data security. Additionally, organisations should prioritise training their employees to adapt to these cutting-edge technologies.

In conclusion, combining AI and quantum cryptography is a promising field with significant potential in enhancing data security and privacy. Ongoing research and advancements in hybrid cryptographic systems, automated cryptographic protocol design, quantum key distribution enhancements, post-quantum cryptography development, quantum machine learning for cryptanalysis, and secure multi-party computation are expected to revolutionise the field. However, it is crucial to consider ethical implications and ensure that advancements in AI-driven quantum cryptography are aligned with global data protection standards and privacy concerns.

Acknowledgements
Eternal gratitude to the Fulbright Visiting Scholar Project.

Author contributions
Dr PR—sole author—was responsible for reviewing the researched literature, conceived the study, was involved in protocol development, gaining ethical approval, patient recruitment and data analysis, wrote the first draft of the manuscript and reviewed and edited the manuscript and approved the final version of the manuscript.

Funding
This work has been supported by the PETRAS National Centre of Excellence for IoT Systems Cybersecurity, which has been funded by the UK EPSRC under Grant Number EP/S035362/1, and ESRC Grant Number: ES/V003666/1.

Availability of data and materials
All data and materials are included in the article.

Declarations

Ethics approval and consent to particiapte
The University of Oxford ethical committee has granted ethical approval under reference R51864/002.

Competing interests
The author declares no conflict of interest, nor competing interest.

Received: 12 December 2023 Accepted: 28 January 2024
Published online: 09 February 2024

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-management/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/selected-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/getting-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

Publisher's Note

Dr. Petar Radanliev is a Masters Projects Supervisor at the University of Oxford's Department of Computer Science and a Post-Doctoral Researcher at the University of Bath School of Management. Dr. Radanliev completed his PhD in 2013/14 and has since engaged in postdoctoral research at several prestigious institutions, including Imperial College London, the University of Cambridge, the Massachusetts Institute of Technology, and the Department of Engineering Science at the University of Oxford for 7 years, before moving to the Department of Computer Science. Specialising in Artificial Intelligence, Cybersecurity, Quantum Computing, and Blockchain Technology, Dr. Radanliev has established himself as an expert in these cutting-edge fields. Prior to his academic career, he amassed a decade of experience as a Cybersecurity Manager at RBS, the world's largest bank, during his tenure. Additionally, he has a significant background in cybersecurity, evidenced by 5 years spent as a Lead Penetration Tester for the Ministry of Defence.