

Review Article

The Integration of Quantum Key Distribution and Zero Trust Security in 5G Networks: A Comprehensive Review

Md Rayhan Uddin¹, Nur Ziadah Harun^{1*}

¹Faculty of Computer Science and Information Technology, Universiti Tun Hussein Onn Malaysia, Johor, Malaysia.

*Corresponding Author : nurziadah@uthm.edu.my

Received: 10 February 2026

Revised: 01 July 2026

Accepted: 18 August 2026

Published: 30 September 2026

Abstract - With the rapid growth of 5G networks that introduce better speed, connectivity, and scalability than previous generation networks, new security threats have also started to arise, especially from quantum computing. Quantum Key Distribution (QKD) and Zero Trust (ZT) have emerged as viable solutions to overcome these security issues. Previous literature has discussed the independent implementation of these two frameworks in 5G networks. However, several new studies have been proposed and examined the integration of QKD and ZTA together in the same network in order to enhance the security against quantum threats, which leaves room for a new comprehensive review that will encompass the current research and development of QKD and ZTA in 5G networks. Therefore, this paper aims to address this gap by reviewing state-of-the-art progress, implementation approaches, and drawbacks of QKD and ZTA in 5G. This review also recommends future research direction by discussing the potential implementation of QKD and ZTA integration together in 5G networks.

Keywords - Authentication, Cryptography, Dynamic Polarization, QKD, Quantum networks.

1. Introduction

The Fifth Generation (5G) network has become an integral part of every aspect of modern lives. With the integration of New Radio and Long-Term Evolution technologies in 5G, it focuses on low latency communication, enhanced mobile broadband and massive machine type communication [1]. Conventional perimeter-based security in 5G network architecture is not viable anymore, as it considers any users within the perimeter trustworthy [2]. This method presumes the network parameter to be a trusted area, and users who operate within this zone are considered trustworthy after one-time verification. Nevertheless, the identification of this perimeter is exceedingly difficult as a result of the 5G network users' mobility and the agile radio environment. Additionally, as an enterprise's reliance on a network becomes more vital to operations like automated manufacturing, autonomous vehicles, and IoT devices, the necessity for communication system assurance has increased, with a major interest in securing telecommunication networks [3]. To confront these obstacles, Zero Trust Architecture (ZTA) has been proposed and developed. It offers a security framework that does not rely on any resources or users, in spite of them being within the range of the network, without continuous authentication. ZTA functions by enabling secure network access to data, devices, and services exclusively for authorized and approved entities (users, devices). Zero Trust (ZT) functions on the

principle of "never trust, always verify". It considers that internal and external threats might sneak into the system, and it reinforces strong identity verification, network segmentation, and least-privilege access [4]. The presumption that all network elements are secure allows an intruder to move between systems after breaching and gaining access [5]. ZTA, which aims to secure all resources, perform continuous authentication, and limit access to resources, was developed as a potential solution to overcome these issues.

Despite the significant development of 5G networks, the evolution of quantum computing in the post-quantum era has brought imminent security threats and consumer privacy issues. Quantum Key Distribution (QKD) has emerged as a feasible resolution to overcome these cyber threats. It utilizes the principles of quantum mechanics and allows authorized users to transmit symmetric keys securely while being alert against invaders [6].

Therefore, the incorporation of QKD in 5G and 6G architectures is considered to safeguard applications and services from quantum attacks [7]. Furthermore, the advancement of quantum computers will make the current encryption technologies inefficient, necessitating the adoption of QKD to safeguard the data transmission [6]. By means of a quantum channel, QKD allows the exchange of keys between



two endpoints without the infiltration of an eavesdropper, as this would alter the state of the information communicated between authorized parties [8].

The integration of QKD and ZTA independently in 5G networks has been studied and implemented by several researchers as promising approaches to overcome the security issues [9-14]. However, the existing literature only focuses on either QKD or ZTA independently, while there have been recent studies that explore how to integrate these two protocols together to improve security and authentication [15-18]. The secrecy of QKD and secure authentication of ZTA together have the potential of becoming a dual layer of defense on top of a network/system to prevent breaches in the network. There still remains a lack of a comprehensive review that explores the recent developments of QKD and ZTA in 5G networks, the recently proposed models of QKD and ZTA integrated together, the outcome of that research, etc.

Therefore, this study aims to present a comprehensive review of 5G networks as well as the incorporation and advancement of QKD and ZTA in 5G settings. It also provides insights and suggestions for future research directions for enhancing the security and resilience of 5G networks. The remainder of this paper is structured as follows: Section 2 elaborates on the current 5G network architecture, implementation, and the challenges that arise. Section 3 provides a background on QKD, its fundamental processes, current advancements, implementation in 5G networks, and the associated challenges.

Section 4 elaborates on the ZTA, its logical components, advancements, integration in 5G networks, and related challenges. Section 5 discusses the current development of integrating both QKD and ZTA together and the potentiality of implementing such an integrated framework within 5G networks. Section 6 summarizes with a review of the observations and proposals for future research.

2. Overview of 5G Network

5G utilizes mechanisms like high-density antenna-construct Multi-Input Multi-Output (MIMO) to enhance connectivity routes [19]. This feature makes the connection more reliable and speeds up the data transfer, which keeps critical communication and control safe. 5G is anticipated to address six challenges existing in previous generations: increased capacity, increased data rate, reduced latency, massive device connectivity, steady quality of service, and reduced cost [1]. Simultaneously, the capabilities of attackers expanded in comparison to those of previous generations [9]. Additionally, the malware and attacks that are generated are more efficient and effective. This results in attacks that are motivated by more ambitious objectives than those of previous generations, such as large cybercrime organizations that have explicit financial, political, and personal motivations

[9]. Consequently, it has a broad attack surface that could result in a serious interruption in the operation of the connected networks.

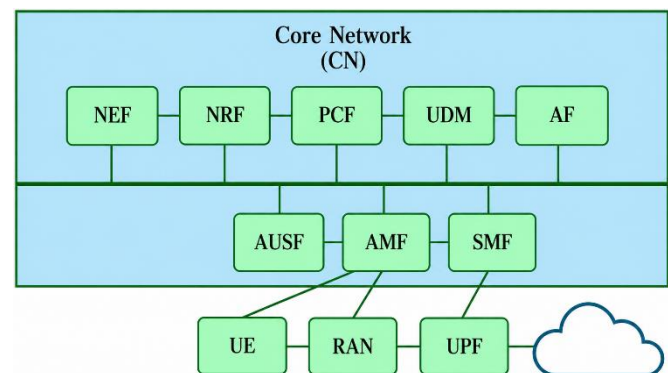


Fig. 1 5G architecture

2.1. 5G Security Architecture

A typical 5G architecture, as shown in Figure 1, comprises the User Equipment (UE), Core Network (CN), and the Radio Access Network (RAN). Any end-user device, like a smartphone or laptop, can be considered a UE in 5G. The UE is capable of establishing a wireless connection to the RAN. The transport network connects the Next Generation Node B (gNB) at RAN to the core network. The entrance for UE is the Access and Management Mobility Function (AMF) within this architecture. The Session Management Function (SMF) is selected by AMF to manage the session's user in accordance with the UE request. Additionally, the User Plane Function (UPF) enables data transfer. Finally, the UE and the 5G services are authenticated by the Authentication Server Function (AUSF). The policy control framework comprises functions such as Application Function (AF), Policy Control Function (PCF), SMF, and Unified Data Management (UDM) that are used to regulate network behavior, policy decision application, and subscription information [10]. The association, Next Generation Mobile Networks (NGMN), identified several challenges of previous generation networks, including vulnerability to DOS attacks, high network traffic, user plane integrity, etc. 5G architecture is able to tackle these issues by employing a stratified security framework consisting of six principal security domains [2].

2.2. Emerging Challenges in 5G Networks

In contrast to the previous generations, 5G networks are more robust due to the implementation of various security protocols and practices that encompass technical measures (encryption, anomaly detection, authentication) and process-oriented measures (vulnerability management) [9]. However, the broader scope and architectural changes of 5G result in a greater and more diverse threat landscape, albeit with these innovations. The primary security challenges are the following, as per a meta-review of current literature [9, 11, 20, 21]:

- **Increased Attack Surface:** The heavy use of SDN and virtualization technologies increases the attack surface in 5G networks.
- **Advanced Persistent Threats (APT):** These are complex and prolonged attacks that are composed of adversaries who are very skilled and motivated. These threats are devised to interrupt, steal data, or gain unauthorized entry to specific organizations by exploiting 5G networks' entry points and vulnerabilities.
- **Unrestricted Lateral Movements:** This is defined as the capability of attackers or malicious software to travel around in a network once they first gain access. Such lateral moves are far more difficult to trace since they tend to utilize genuine access.
- **Threat Detection:** High volume, velocity, and variety of data generated present a significant 5G cybersecurity challenge because threat detection is a key component. It can be a difficult task to identify threats from this huge amount of data in real time, particularly if there is no adequate number of human analysts.

In order to tackle these growing security demands, particularly ones further complicated by the decentralized and dynamic nature of 5G networks, researchers and industry stakeholders are investigating next-generation security paradigms that supersede conventional approaches. QKD and ZTA are two of the most promising approaches, since each of them was designed to enhance the trust, integrity, and confidentiality of next-generation networks. The next sections present a comprehensive review of the literature on theoretical or practical implementation of both these methods towards making 5G networks more secure.

3. Quantum Key Distribution (QKD)

QKD, unlike conventional key distribution algorithms that are based on the difficulty of mathematics as their strength basis for security, has been theoretically proven to offer unconditional security through the combination of three elements: the use of quantum mechanics laws exploitation, a one-time pad, and a hashing scheme [8].

The strength of the key is determined by the factorization problem in conventional cryptography. Numerous cryptographic algorithms have been demonstrated to be unsafe when subjected to a Quantum Computer (QC). QKD addresses the established secret key exchange of symmetric encryption in an information-theoretically secure manner. QKD allows two authorized users to generate and distribute shared symmetric keys securely, with the ability to detect eavesdroppers, with the application of quantum mechanics principals [6]. QKD provides a supplementary layer of security for the secure distribution of cryptographic keys in an existing network. It is a critical component in the establishment of secure communications in sensitive networks such as 5G.

3.1. Basic Process of QKD System

Bennett and Brassard [22] developed an innovative approach for QKD utilizing photons governed by the principles of physics. Recent years have witnessed substantial progress in QKD protocols, systems, devices and communication channels. Secure transmission over a Quantum Network (QN) has also been the subject of numerous QKD protocols [23, 24]. A secret key is created and shared between Alice and Bob in a fundamental QKD system through the use of a QKD protocol. Following the generation of the key, the encryption block encrypts the data and subsequently transmits it to Bob. The ciphertext is converted to plaintext by Bob using the same secret key to read the secret information [8, 25]. The following phases illustrate the procedure of a basic QKD, as shown in Figure 2:

- Quantum Phase:** Alice randomly selects a measuring basis between Rectilinear (R) and Diagonal (D) for each bit in a random string of bits. The quantum channel is used to transmit the string of qubits, the string of bits, and polarization states to Bob. Then Bob picks a measuring basis for each of the received qubits at random, and he commences the measurement of the received bits using the selected basis. If Alice and Bob's measuring bases are identical, the result is perfectly correlated; otherwise, it is uncorrelated. After measuring all of them, Bob records all the received bits, known as the Raw key (Kraw).

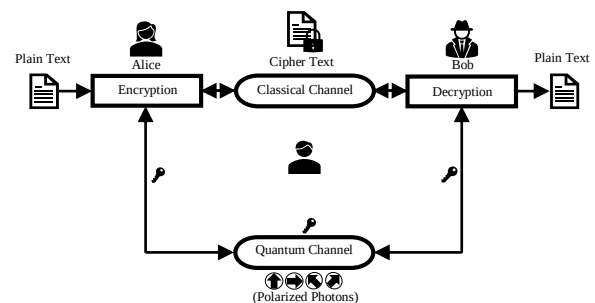


Fig. 2 Basic QKD mechanism

- Classical Phase:** Alice and Bob communicate in the classical channel to extract secret keys from the measurement outcomes. Following the steps illustrated in Figure 3, the process of extracting the secret key is as follows:
 - **Sifting:** Alice and Bob's random measuring bases are assessed, and the bits that correspond to the same bases are retained, while the bits that correspond to different measuring bases are rejected. The retained bits are referred to as the sifted key (Ksifted).
 - **Error estimation:** Alice and Bob establish a threshold value for the Quantum Bit Error Rate (QBER) in order to prevent eavesdropping on the communication medium. They calculate the estimated QBER by comparing a random subset of Ksifted bits based on that value.

- Error correction: This stage is necessary to reduce the possibility of error even more during the sifting process. The key that is generated after this process is referred to as the corrected key ($K_{corrected}$).
- Privacy amplification: Privacy amplification is a fundamental process that reduces the information content of the secret key to a negligible level with respect to an unauthenticated party and generates a new, shorter key using universal hash functions known as the final key (K_{final}).

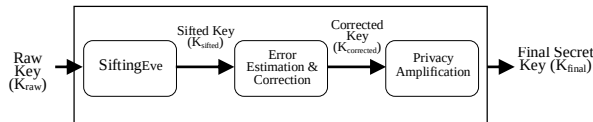


Fig. 3 Post quantum PROCESS

- c) Encryption Phase: During this phase, Alice and Bob utilize the secret key that was established for encrypting and decrypting confidential data. To facilitate secure communication among end-users and successfully encrypt and decrypt the data, this phase uses a symmetric encryption algorithm such as AES, coupled with the one-time pad encryption technique. The data that is encrypted and then sent by Alice is referred to as ciphertext. Afterwards, using the same secret key, Bob decrypts the data in plain text format.

3.2. Current Development & Implementation of QKD

QKD has the ability to secure the integrity of transactions and defend against possible cyber-attacks through unsurpassed security for transmitting sensitive information in the healthcare, finance, space technology, government industries and banking industry. Aside from establishing QKD interconnections during the FIFA World Cup in 2010 [26], it can also be applied in securing essential networks for governmental entities and financial foundations. The following are examples of typical QKDN application areas:

- Space and mobile applications: Among other services, QKD offers secure access to satellites, communication between ground stations, and satellite-to-satellite facilitation for space-based communications [27]. Additionally, the Tokyo QKDN [28] has implemented QKD to safeguard cell phones within a multi-user mobile network.
- Healthcare: In order to guarantee sustainable security of confidential human genomes and medical records, a storage system that offers exceptional storage longevity was implemented in [29]. Through the use of QKD, Toshiba and ToMMo were able to successfully transmit genome sequence data in real-time in 2020.
- Government and Defence: The strictest data security policies are found in governmental organizations, especially when it comes to safeguarding official sensitive information. In 2007, QKD was successfully

implemented by the Swiss government to safeguard a designated line for the purpose of tabulating national election votes. Numerous government employees have implemented a QKD metropolitan network in Jinan [30] to safeguard their data.

- Cloud and Data Centres: The protection of data confidentiality and security has transformed increasingly critical as an increasing number of organizations utilize data centres and the cloud to store, recover, and backup data. KPN has established end-to-end QKD within its network connecting the KPN data centres in The Hague and Rotterdam. Researchers in [31] provided the description of QKD's implementation in safeguarding multi-source data security in the smart grid. The Beijing-Shanghai QKD link [32] was employed in China to safeguard the data centre backup between Beijing and Shanghai. Quantum-safe encryption is also being implemented by numerous corporations, including Alibaba and Acronis, in the corporate cloud security sector [33].

3.3. QKD vs PQC

Post-Quantum cryptography (PQC) aims to remain secure against both classical and quantum threats by designing new cryptographic systems. These systems are expected to be compatible with existing communication networks and protocols. PQC substitutes susceptible public-key primitives with algorithms considered resilient against quantum attacks, such as lattice- and code-based schemes. NIST has standardized essential PQC algorithms for key establishment and signatures, facilitating the deployment of PQC in current protocols like TLS, IPSec, and 5G SBA authentication. It is entirely software-based, facilitates long-distance and multi-hop networks without the need for trusted relays, integrates effectively with existing SDN/NFV and slicing frameworks, and offers economic scalability across extensive 5G deployments [34]. Nonetheless, PQC offers computational security rather than information-theoretic security and is based on hardness assumptions that, despite thorough evaluation, may be compromised by future cryptanalytic developments or implementation side-channels. In this case, QKD provides a significant advantage by utilizing information-theoretic key security while guarding against an eavesdropper. The survey [34] provides a comparison of both PQC and QKD and argues that QKD provides stronger security, whereas PQC provides temporary solutions. However, these analyses also point out the limitations that QKD faces regarding distance, scalability, secret-key rate, etc. It also relies on trusted-node or repeater infrastructure, which makes the wide-area implementation difficult. Thus, surveys emphasize the necessity of crypt agility and hybrid migration as continuous requirements [35].

3.4. Applications of QKD in 5G Networks

The authors in [36] argue that QKD is a crucial method for safeguarding 5G and 6G networks from quantum threats. Certain proposals in the literature illustrate the integration of

QKD into various components of the 5G architecture to enhance the security of communications among distributed network elements. For example, [12] proposes and validates, via simulation, a mechanism to secure transmissions within the Base Stations and the Data Unit Station of the 5G fronthaul utilizing QKD. A further contribution [13] presents a method for facilitating 5G slicing augmented with QKD between the aggregation node and the 5G core, meeting the rigorous security requirements of particular use cases. Additionally, [14] demonstrates and validates a communication system utilizing polarization entanglement-based QKD commercial equipment, integrating TLS and QKD to secure communications among the Network Functions (NFs) within the 5G core network. A QKDN testbed is under development in Eindhoven to offer quantum encryption as a service on demand, ensuring optimal end-to-end security, with connections to both optical access networks and 5G testbeds. The authors of [37] examined the integration of QKD into 5G/B5G fronthaul network segments to secure against quantum threats and achieved a high success rate. Another study [38] integrated CV-QKD into a WBM-based 5G fronthaul network. Their experiment resulted in high secret key rates, even in a noisy environment, over 10 Mbps within a 13.2 km distance.

3.5. Challenges & Limitations of QKD in 5G

Integrating QKD in 5G networks possesses several shortcomings [39-41]. The limited quantum key generation rate is a huge obstacle in high-speed and large scale 5G environments. The limited distance, which is usually 100-200 km due to photon loss in optical fibers, is another major issue that prevents the broad deployment of QKD in 5G networks. In the sequential setting, e.g. the framework of [42], the security proofs require Alice and Bob to process inputs and outputs in a certain order. While sequential proofs yield better security parameters, their performance in leakage scenarios, and especially in real-time, high-throughput 5G systems, is not clear.

The security of QKD does not rely on mathematical complexity, but it can be attacked because of technical and engineering imperfections. Technological limitations also restrict the practicality of QKD over 5G networks. Attacks like Photon Number Splitting, Trojan Horse and Fake States could leverage the flaws of the present QKD protocols. Backflash light was considered as a vulnerability in [39], where the photon emission during the Single-Photon Avalanche Diode (SPAD) detection process can leak the key information. Their methods involve the measurement and minimisation of backflash emissions.

Other vulnerabilities appear from the modulation leakage [43], coherent light states [44] and experimental inaccuracies [45]. Any encoding or experimental error may lead to information leakage in a QKD-integrated 5G network.

4. Zero Trust (ZT)

Zero trust model is focused on safeguarding resources founded on the principle that trust is not inherently given, but must be continuously verified. Traditionally, enterprise networks have been built around perimeter defence, granting authorised users access to a broad spectrum of assets once they entered the internal network. Thus, unauthorised lateral movement within the setting has become a major challenge for federal agencies [5].

The definition emphasises the goal of preventing unauthorised access to data and services and implementing the most comprehensive enforcement of access control possible. ZT security frameworks assume that there could be an invader within the environment and that the enterprise-owned environment is no more secure than a non-enterprise-owned environment.

In this new paradigm, an enterprise has to adopt a ZT approach and continuously assess and evaluate the threats to its resources and business operations and implement defences to mitigate such dangers. Such defences typically rely on restricting access to resources (data, computation, applications/services) to entities and assets as needed, while continuously authenticating and authorising the identity and security posture of each access request.

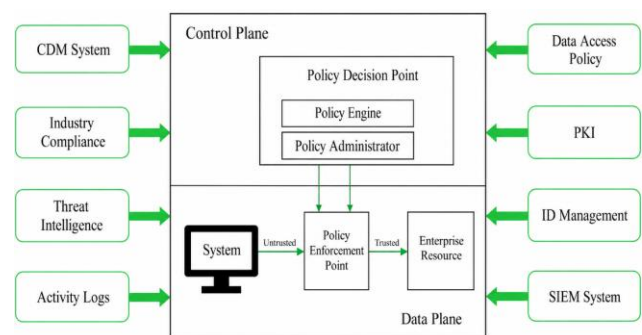


Fig. 4 Zero Trust Architecture

4.1. Zero Trust Architecture (ZTA)

ZTA is a zero trust principles-based framework for organisations to stop data breaches and restrict internal lateral movement. Authentication and authorisation for every request enables the system to precisely regulate and calibrate the security level required to access particular resources [46]. It is described as a framework that addresses both internal and external threats, preventing malicious adversaries from gaining access to unauthorised information and reducing the exposure of vulnerable systems. A ZTA is constructed and employed in accordance with the essential foundations of ZT [4].

4.2. Logical Components of ZTA

A ZTA network involves multiple logical components that operate either an on-premises service or a cloud-based

service. The ZTA logical components employ a separate control plane for communication, meanwhile application data is conveyed through a data plane. The essential components of a ZTA, illustrated in Figure 4, are as follows [46]:

- **Policy Engine (PE):** PE employs organization policy and external inputs to notify a trust algorithm that governs resource access by granting, rejecting, or withdrawing permissions. It is associated with the Policy Administrator (PA), formulating and recording the decision (as permitted or denied), while the PA implements the decision.
- **Policy Administrator (PA):** This component facilitates the initiation and termination of the communication link between a subject and a resource. After session authorization and request authentication, the PA configures the policy enforcement point to permit session initiation. If the session is denied or the previous authorization is revoked, the PA instructs the PEP to abort the connection. This interaction occurs through the control plane.
- **Policy Enforcement Point (PEP):** This component enables, overrules, and ultimately concludes connections between an individual and an organizational asset. PEP cooperates with the PA to communicate requests and obtain policy updates from the PA. Behind the PEP lies the trust zone that contains the enterprise resource.

Besides fundamental elements of a ZTA, multiple data sources provide input and policy rules employed by the PE in access decision-making. This includes both inner and outsider data sources. This may involve, but is not restricted to, Data access policies, Threat intelligence, Security Information and Event Management (SIEM) system, PKI, Continuous Diagnostics and Mitigation (CDM) system, ID management, Industry Compliance and Activity logs [46].

4.3. Recent Advancements & Implementation of ZT

The emergence of ZT has been influenced by the rise in threat levels and the advancements in technology, including cloud computing. The most significant enhancement to ZTA may be the modern Identity and Access Management (IAM) tools, which are significantly stronger and more scalable than previous solutions. These tools are now complemented by additional attributes, including Multi-Factor Authentication (MFA), biometrics, and behavioral analysis. In 2010, [47] introduced the notion of a ZTA framework and a practical technique for its implementation. In addition, the authors presented a new ZTA based on the Data Acquisition Network (DAN) in their work. DAN enables the network data extraction to a centralized management center, where it undergoes real-time inspection and analysis, thereby achieving the ZT model. For safeguarding sensitive information, [48] suggested a secure medical image sharing system that is compliant with the principles of ZT and blockchain technology.

The research in [49] introduced an artificial intelligence-driven ZTA in 2021. The framework utilizes artificial intelligence to facilitate intelligent detection, analysis, and decision-making, thereby improving the effectiveness of ZTA components in handling big data. Additionally, researchers in [50] introduced a ZT framework that entails a thorough trust assessment of various system components, encompassing users, devices, communication channels, files, and applications. This method necessitates secrecy and credibility, assigning different weights to ensure optimal protection of object confidentiality and integrity. Nevertheless, it neglects to consider the initial trust value allocation mechanism for users, terminals, environments, objects, and other entities, and it is incapable of adequately mitigating human-factor errors in establishing initial trust. To attain economical fine-grained access control, alongside performance, scalability, and security for actual organization networks, [51] proposed an advanced ZTA that employs generalized attribute relation extraction to automate fine-grained access control.

ZTA research is in its early phases, and the limitations of inheritance systems have prompted a more advanced method to cyber threats. The study [52] proposed a trust model for bridging the trust gap in cloud environments using the ZTA framework. The model presented a comprehensive strategy for enhancing trust in an enterprise's information system, indicating that the allocation of trust-based nodes could be utilized to regulate intrusions.

To address the limitations of existing cybersecurity protocols in virtual power plants, [53] instituted the ZTA to improve privacy and data protection within the energy sector. They used the ZTA framework to construct their model, and its efficacy presented a viable solution to theft of data and intrusions. [54] Conducted research on ZTA for healthcare industry transitions and reached the conclusion that medical devices could be safeguarded through the integration of firewalls and the model. As a result, network performance will be impacted by the cessation of all unnecessary traffic.

The influence of ZTA within a university setting was examined by [55]. They found that the existing security framework is inadequate for preventing invasions and cyber-attacks, as well as supporting the deployment of ZTA, after considering the components and policies. Another study [56] examined the current security architecture and concluded that it is incapable of mitigating the most recent security trends and challenges.

Consequently, they suggested a hybrid security architecture that is based on blockchain technology and a ZTA, which would serve as a framework for IoT. This framework would facilitate secure access to devices and resources and facilitate authentication.

Table 1. Advancements & implications of zero trust

Author	Technique	Findings	Limitations
[48]	Integration of blockchain technology and zero trust.	Blockchain technology protects data by keeping a record of all transactions, and zero-trust principles make sure that medical data is encrypted and that only trusted devices and users can connect to the network.	Poor network speed, high demand for node performance and causes waste of energy.
[49]	Intelligent Zero Trust Architecture (i-ZTA) and Machine Learning (ML).	Introduces an intelligent Zero Trust Architecture (iZTA) for the next generation of 5G and 6G tactical networks. It combines machine learning with traditional Zero Trust components to constantly check for trust and enforce access decisions. They proposed the MED model: Monitor assets, Evaluate risk per request, and Decide via AI-driven algorithms.	Conceptual, yet to be implemented.
[50]	New Zero trust method with the combination of Bell-LaPadula (BLP) and BIBA model.	The zero trust principle, through the integration of BLP and BIBA, enables enhanced and more precise enforcement of data confidentiality and integrity.	Does not account for the initial trust value granting method for users, terminals, environments, objects, and other entities, and does not prevent human factors from misallocating initial trust.
[51]	An advanced ZTA, leveraging an automated policy generation scheme.	Generalized attribute relation extraction is used to automate fine-grained access control, which makes designing and managing high-level policies much cheaper.	Requires evaluation of performance, scalability and security on a real enterprise network.
[52]	ZTA for cloud computing environments.	Feasible and useful as a defense against intrusion and a secure method to recover, which ensures that operations keep running.	Requires empirical validation at cloud scale, performance quantification, economic cost analysis and integration guidance with existing cloud providers and service meshes
[53]	ZTA transition framework using microsegmentation, Access Control Lists (ACLs), and firewall placements, tested through Cisco Modelling Labs (CML), and evaluated with packet flow analysis and latency measurement.	Presents a pragmatic roadmap and supported examples (CML) demonstrating feasibility and expected security enhancements for healthcare organizations.	Hypothetical, yet to be implemented in a real-life environment.
[55]	Implementation plan of ZTA using the West Point model.	Proposed model protects university resources and research from potential hackers.	Limited to the university environment.
[56]	A ZTA for Future IoT (FIoT).	Secures devices and incorporates a scalable device authentication and identification mechanism.	Theoretical, yet to be implemented.

4.4. Zero Trust Security Overview in 5G Networks

In 5G networks, which relies on virtualization and software-defined architectures, ZTA can enhance security by

enforcing strict access control and real-time monitoring. 5G uses network slicing, where each slice operates as a virtualized network for specific applications [20]. Zero Trust aligns well

with network slicing by applying micro segmentation to enforce security policies within and between slices, limiting the impact of a potential breach. Due to these measures, the implementation of ZTA in 5G is actively being researched in several sectors. The following are some implications of a ZTA-secured 5G system:

- **Smart Healthcare System:** The passive security measures, including data encryption and isolation, utilized in conventional medical platforms, insufficiently offer the required security for a healthcare system deployed in a distributed manner. The authors of [9] proposed a security awareness and protection system utilizing ZTA for a 5G-enabled smart medical platform.
- **Mobile Core Networks in 5G:** Implementing a virtualized mobile core network in a cloud setting presents considerable security concerns, involving both the interactions between the RAN and the mobile core network, along with those within the core network itself. The authors of [10] proposed a Vepc-vSDP framework to ensure secure communications within the mobile core network through an authentication-based method. The SDP components are virtualized and located inside the virtualized core network, establishing a ZT environment in which only authorized and authenticated core network components can communicate.
- **Minimizing Lateral Movement in IoT Networks:** It is crucial for 5G networks to switch from perimeter-based defense to a ZT security framework that emphasizes agent-centric trust assessment and access protocols for identifying adversaries. The authors of [11] proposed a Game-theoretic ZTA framework to formulate interdependent trust evaluation and authentication policies utilizing dynamic game models.

4.5. Challenges of Implementing ZTA in 5G

While ZTA offers robust security solutions, there are challenges in applying it to 5G networks [4, 57, 58]:

- **Scalability:** Enforcing ZT principles across thousands of interconnected devices is complex and may strain network resources, especially in dynamic 5G environments.
- **Latency and Performance:** Continuous authentication and monitoring could impact the performance of the network, especially for latency-sensitive applications.
- **Interoperability:** Due to the decentralised nature of 5G and 6G, ZTA needs to be compatible with diverse platforms, devices and standards. Enforcement of trust can break down at the edges of the network without seamless interoperability.
- **Privacy Concerns:** Monitoring and verifying user activity at all times may lead to concerns over user privacy and data protection.

5. Integration of QKD & ZT

Due to their individual potential in providing strong security against cyber and quantum attacks, several studies have explored the combination of QKD and ZTA as a stronger solution. A recent study [15] has demonstrated that the integration of QKD into ZTA improves secure identity verification, encrypted communication, and session-based access control.

The results show that QKD protocols, in combination with quantum-resistant algorithms, can reduce the risk of key compromise and enable continuous authentication in quantum attack scenarios, which is consistent with the ZT principles.

Another study by [16] proposed a ZT spatiotemporal diversification framework for QKD networks to enhance end-to-end key distribution security by dynamically shuffling transmission routes and excluding suspicious relay nodes through a penalty-based mechanism.

Simulation indicated that the attack success rate was reduced by up to 97.22% and greatly improved interception resistance, showing that the incorporation of ZT concepts into QKD routing is effective. [17] investigates the convergence of quantum technology with ZTA to fortify network security from emerging digital threats.

In this method, dynamically generated quantum keys are employed for every authentication request and also for encrypting data to be transmitted, making both identity verification and communication tamper-proof and eavesdropping-resistant.

The paper opines that innovation in quantum key studies provides practical opportunities for more secure implementation of ZT, building a future-ready cybersecurity ecosystem.

The author in [18] designed a ZT-QKD relay architecture based on fully homomorphic encryption to avoid dependency on trusted intermediaries. Another study by [59] proposed and simulated the integration of Q-EnergyDEX, a zero-trust framework and QKD to secure decentralized electricity markets from cyber-attacks. Their experiment showed a sub-second latency, fast finality and enhanced resilience against cyber threats, significantly outperforming standard protocols.

The authors of [60] proposed a crypto-agile zero-trust multi-cloud infrastructure that incorporated SDN, PQC and QKD to overcome inconsistent key management and fragmented trust boundaries. Their simulation output showed a 100% accessibility success rate, showcasing enhanced security control and affirming that crypto-agility is feasible in multi-clouds.

Table 2. Integration of QKD & zero trust

Author	Problem Statement	Technique	Findings	Research Gap
[15]	Current ZTA faces performance and scalability issues due to its complex architecture.	Integration of quantum computing, including QKD, Post-Quantum Cryptography (PQC) and Quantum Machine Learning (QML) into Zero Trust frameworks.	By utilizing quantum-enhanced decision-making mechanisms and quantum-resistant algorithms, quantum computing enhances Zero Trust Architectures by facilitating continuous authentication, secure access control, and adaptive threat detection.	Lack of a comprehensive, implementable framework combining Zero Trust and quantum tech remains undeveloped.
[16]	Trusted relay dependency in QKD networks is static and vulnerable to compromise.	A zero trust routing protocol using moving target defense: spatio-temporal path diversification, multipath multi-key distribution, recursive-penalty node exclusion.	Enhances resilience by dynamically shifting routes, isolating suspicious relays, and improving end-to-end key security.	Requires practical deployment at scale.
[17]	Zero Trust lacks future readiness against quantum threats.	Integration of quantum technology with Zero Trust Network Architecture	Quantum enhancement has the potential to expedite decision-making, increase visibility, and future-proof Zero Trust systems against emerging cyber threats.	Limited details on integrating actual quantum hardware and scaling across diverse infrastructures.
[18]	Traditional QKD relay nodes expose plaintext keys at each hop, requiring full trust in intermediaries.	Uses Fully Homomorphic Encryption (BFV scheme), external QRNGs, and ETSI-aligned design to shield key material even at untrusted relays.	Enables secure, privacy-enhancing QKD deployment over an untrusted relay, while simultaneously maintaining acceptable performance and scalability, by preserving key confidentiality and integrity.	Authentication mechanisms and multi-key management strategies within FHE-enhanced QKD require further development.
[59]	Existing blockchain-based solutions are vulnerable to quantum attacks.	Integrated Q-EnergyDEX, a zero-trust framework with QKD.	Improved latency, fast finality and enhanced resilience against cyber-attacks.	Requires practical deployment.
[60]	Inconsistent key management and fragmented trust boundaries in the cloud.	Crypto-agile ZT infrastructure integrated with SDN, PQC and QKD.	100% accessibility rate and stronger security control without compartmentalization.	Limited to theoretical and simulation experiments.

The findings of these studies indicate that the combination of QKD and ZTA can be potentially very effective against cyber-attacks. QKD ensures secure key exchange while ZTA verifies authentication continuously, making it difficult for infiltrators to breach into the systems. Moreover, many of these studies suggest that the overall performance and security have improved significantly. Based on the results of these QKD and ZTA integration studies, as well as their successful individual integration in 5G, this study suggests the integration of QKD and ZTA together in 5G networks. Individually, they have shown successful experiments and implementation when integrated in 5G, as discussed in sections 3.4 and 4.4. The combined implementation could further enhance the overall security of

5G networks. The integration will blend the quantum-secure key exchange capabilities of QKD with the continuous verification and strict access control concepts of ZTA. QKD ensures the distribution of secure cryptographic keys based on quantum mechanics, thereby rendering eavesdropping detectable and making intercepted keys unusable. While ZTA enforces a strategy of continuous authentication, limited access, policy enforcement, etc., at all network layers, which prevents unauthorized access even from sources within the network. QKD can generate and distribute encryption keys securely among the communicated nodes using the entanglement property, ensuring confidentiality and integrity in a ZTA network. Any attempt to intercept the key exchange alters the quantum state and gets discarded. The resulting

secure key can be used as a source for identity and communication protocols among the participants' nodes in the network. ZTA ensures that the using parties always verifies their authenticity before being given access to any form of data. If any unauthorized party attempts to access that data, the system will deny the access and revoke the session. Based on the findings and discussion above, the integration of QKD and ZTA together into 5G networks could potentially enhance the overall security of 5G networks and could be a possible future direction for further development.

One of the concerns of QKD-ZTA integration is the failure of QKD channels due to the detection of Eve. The studies on quantum channel interruptions show that QKD systems quickly resynchronize the phase and the time, then create new pairs of keys and restore the key flow in sub-second scales of recovery phases [61]. Studies on routing mechanisms in QKD networks show that key resource exhaustion and unreliable paths cause most quantum communications service failures, and rerouting and reliable multi-path routing decisions redistribute key flow along new trusted paths in case the initial trust in the first path gets degraded. The studies suggest that suspicious and untrustworthy routers will be penalized and excluded from the routing process, and the newly formed route paths will be reassigned to assist in the restoration of the end-to-end trust-based flow of the secure keys, enabling a safe and trust-based re-distribution of the keys due to envisioned eavesdropping events [16].

Recent articles demonstrate that the cross-layer mismatch between a fragile physical key source and software-driven continuous access control is another major obstacle to QKD-ZTA integration. QKD-network challenge surveys note that physical-layer effects, fiber loss, noise, hardware drift, and attack-induced disturbances cause large QBER and Secret Key Rate fluctuations and can even stop key generation, so higher-layer services cannot assume steady key availability [62]. Zero Trust literature emphasizes that ZTA engines require reliable, low-latency telemetry and continuous verification loops, which are harder to stabilize when the key supply is intermittent or rapidly changing [63]. Due to this incompatibility, SDN-enabled QKD architecture papers propose a dedicated software control/management plane that exposes quantum-link health and key-pool status via programmable interfaces to allow upper-layer controllers to adapt to physical conditions [64].

5G deployment-focused QKD articles suggest linking 5G core security functions to key-supply metrics to analyse interoperability and overhead. Securing Network Function (NF)-to-NF signalling with QKD-backed TLS allows standard 5G Service-Based Architecture (SBA) interfaces (e.g., AMF/SMF/UPF service communications) to use QKD keys via a KMS layer, according to a core network study [14]. This suggests that QKD-ZTA requires adding a key-service

endpoint to authentication and encryption workflows rather than redesigning 5G functions. Fronthaul and slicing experiments show that co-propagating classical traffic causes Secure-Key Rate (SKR) variability, Quantum Bit Error Rate (QBER) pauses, and even minutes-long SDN-orchestrated slice setup and teardown. These factors affect how often ZTA decision centres can complete inter-device authentications with session keys. ZTA performance in real deployments may be determined by quantifiable QBER/SKR and buffer-depletion dynamics, not just abstract latency. Recent works suggest the viability of QKD with ZT access in the 5G core networks following the SDN model and performing network slicing communications in the quantum realm without the need for any new control plane architecture to launch the entire process [13].

6. Conclusion & Future Directions

This study presents a comprehensive review of the current developments of QKD and ZTA in 5G networks. It also discusses the existing challenges for implementing these frameworks in 5G, as well as current research on exploring the potential of combining QKD and ZTA to enhance security against quantum threats. QKD and ZTA have been studied individually to address some of the security gaps in the 5G infrastructure, but new threats continue to appear due to the evolving and complex nature of the technological scenario. This supports the case for a more resilient and integrated security approach. Therefore, this study suggests the combined implementation of QKD and ZTA in 5G networks as a promising future direction for research. It is recommended to build a simulation environment based on SDN to evaluate the latency parameters of decision centres supporting a ZTA that uses QKD keys in inter-device authentication. The basis for the recommendation lies in the results of the current studies in the area of R&D in SDN and QKD, where the provision of quantum keys is exerted through the control/management plane that is made possible through the implementation of a software-defined network and is capable of co-simulation together with higher-level security decisions [64]. The experiments in QKD networks enabled by the SDN platform demonstrate the orchestration and fast reconfiguration supported by network control through SKR and QBER values and confirm that QKD-enabled ZTAs will make the proof-of-authentication latency a control-plane derived value based on the routing, transmission, and restoration of QKD-based keys in the decision center's architect [65]. Such an integrated framework is particularly vital in highly sensitive domains such as enterprise private networks, government services, and defence communications, where data confidentiality, integrity, and resilience against quantum-era threats are of utmost importance.

Conflicts of Interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

Funding Statement

This research was supported by the Ministry of Higher Education (MOHE) through a Fundamental Research Grant Scheme (FRGS/1/2024/ICT07/UTHM/03/1). We also want to

thank the Government of Malaysia, which provides the MyBrain15 programme's for sponsoring this work under the self-funded research grant and L00022 from the Ministry of Science, Technology and Innovation (MOSTI).

References

- [1] Nguyen Huu Phuoc Dai, Lourdes Ruiz, and Rajnai Zoltan, "5G Revolution: Challenges and Opportunities," *2021 IEEE 21st International Symposium on Computational Intelligence and Informatics (CINTI)*, Budapest, Hungary, pp. 211-216, 2021. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [2] Milica Pejanović-Djurišić, and Slawomir Kuklinski, "5G Security Landscape: Concept and Remaining Challenges," *2022 30th Telecommunications Forum (TELFOR)*, Belgrade, Serbia, pp. 1-4, 2022. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [3] S. Sullivan et al., "5G Security Challenges and Solutions: A Review by OSI Layers," *IEEE Access*, vol. 9, pp. 116294-116314, 2021. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [4] K. Sowjanya, Dhiman Saha, and Brejesh Lall, "Zero-Trust Security in 5G and Beyond Networks: An Overview," *2025 17th International Conference on COMMunication Systems and NETWORKS (COMSNETS)*, Bengaluru, India, pp. 1230-1234, 2025. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [5] Onome Christopher Edo et al., "Zero Trust Architecture: Trend and Impact on Information Security," *International Journal of Emerging Technology and Advanced Engineering*, vol. 12, no. 7, pp. 140-147, 2022. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [6] Miralem Mehic et al., "Quantum Key Distribution: A Networking Perspective," *ACM Computing Surveys*, vol. 53, no. 5, pp. 1-41, 2021. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [7] Asier Atutxa et al., "Authentication of the QKD Classical Channel Through Post-Quantum Cryptography in a Multi-Site 5G/6G Quantum-safe Communication Network," *2025 International Conference on Quantum Communications, Networking, and Computing (QCNC)*, Nara, Japan, pp. 648-654, 2025. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [8] Yuan Cao et al., "The Evolution of Quantum Key Distribution Networks: On the Road to the Qinternet," *IEEE Communications Surveys and Tutorials*, vol. 24, no. 2, pp. 839-894, 2022. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [9] Ashutosh Dutta, and Eman Hammad, "5G Security Challenges and Opportunities: A System Approach," *2020 IEEE 3rd 5G World Forum (5GWF)*, Bangalore, India, pp. 109-114, 2020. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [10] Abdul Manan et al., "Extending 5G Services with Zero Trust Security pillars: a Modular Approach," *2022 IEEE/ACS 19th International Conference on Computer Systems and Applications (AICCSA)*, Abu Dhabi, United Arab Emirates, pp. 1-6, 2022. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [11] Jinxin Liu et al., "A New Realistic Benchmark for Advanced Persistent Threats in Network Traffic," *IEEE Networking Letters*, vol. 4, no. 3, pp. 162-166, 2022. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [12] Yuyuan Tian, and Fengming Xin, "Establishment and Performance Evaluation of Quantum-Safe 5G Fronthaul Optical Architecture," *Computers and Electrical Engineering*, vol. 110, 2023. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [13] Paul Wright et al., "5G Network Slicing with QKD and Quantum-Safe Security," *Journal of Optical Communications and Networking*, vol. 13, no. 3, pp. 33-40, 2021. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [14] Asier Atutxa et al., "Towards a Quantum-Safe 5G: Quantum Key Distribution in Core Networks," *Computer Communications*, vol. 224, pp. 145-158, 2024. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [15] Temitope Adewale, "The Role of Quantum Computing in Advancing Zero Trust Architectures for Enhanced Cyber Defense," pp. 1-5, 2023. [[Google Scholar](#)]
- [16] Esraa M. Ghourab, Mohamed Azab, and Denis Gračanin, "A Quantum Key Distribution Routing Scheme for a Zero-Trust QKD Network System: A Moving Target Defense Approach," *Big Data and Cognitive Computing*, vol. 9, no. 4, pp. 1-23, 2025. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [17] Jun Lin et al., "Quantum-Enhanced Zero Trust Security: Evolution, Implementation, and Application," *2024 International Conference on Quantum Communications, Networking, and Computing (QCNC)*, Kanazawa, Japan, pp. 211-215, 2024. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [18] Aitor Brazaola-Vicario et al., "Privacy Enhanced QKD Networks: Zero Trust Relay Architecture based on Homomorphic Encryption," *Computer Networks*, vol. 280, pp. 1-13, 2026. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [19] Noamen Ben Henda, "Overview on the Security in 5G Phase 2," *Journal of ICT Standardization*, vol. 8, no. 1, pp. 1-14, 2020. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [20] Hisham A. Kholidy et al., "Toward Zero Trust Security IN 5G Open Architecture Network Slices," *MILCOM 2022 - 2022 IEEE Military Communications Conference (MILCOM)*, Rockville, MD, USA, pp. 577-582, 2022. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]

- [21] Bhavjot Kaur, and K. Tony Joseph, "Security Challenges and Solutions in 5G Networks," *2024 IEEE International Conference on Interdisciplinary Approaches in Technology and Management for Social Innovation (IATMSI)*, Gwalior, India, vol. 2, pp. 1-5, 2024. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [22] Charles H. Bennett, and Gilles Brassard, "Quantum Cryptography: Public key Distribution and Coin Tossing," *Theoretical Computer Science*, vol. 560, pp. 7-11, 2014. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [23] Anastasija Trizna, and Andris Ozols, "An Overview of Quantum Key Distribution Protocols," *Information Technology and Management Science*, vol. 21, pp. 37-44, 2018. [[Google Scholar](#)]
- [24] Mandeep Kumar, and Bhaskar Mondal, "A Brief Review on Quantum Key Distribution Protocols," *Multimedia Tools and Applications*, vol. 84, no. 27, pp. 33267-33306, 2025. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [25] Purva Sharma et al., "Quantum Key Distribution Secured Optical Networks: A Survey," *IEEE Open Journal of the Communications Society*, vol. 2, pp. 2049-2083, 2021. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [26] Hoi-Kwong Lo, Marcos Curty and Kiyoshi Tamaki, "Secure Quantum key Distribution," *Nature Photonics*, vol. 8, no. 8, pp. 595-604, 2014. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [27] Robert Bedington, Juan Miguel Arrazola and Alexander Ling, "Progress in Satellite Quantum key Distribution," *npj Quantum Information*, vol. 3, no. 1, pp. 1-13, 2017. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [28] A. Tajima et al., "Quantum key Distribution Network for Multiple Applications," *Quantum Science and Technology*, vol. 2, no. 3, pp. 1-22, 2017. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [29] Masahide Sasaki, "Quantum Key Distribution and its Applications," *IEEE Security and Privacy*, vol. 16, no. 5, pp. 42-48, 2018. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [30] Qiang Zhang et al., "Large Scale Quantum key Distribution: Challenges and Solutions [Invited]," *Optics Express*, vol. 26, no. 18, pp. 24260-24273, 2018. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [31] Licheng Wang et al., "Research on Multi-Source Data Security Protection of Smart Grid based on Quantum Key Combination," *2019 IEEE 4th International Conference on Cloud Computing and Big Data Analysis (ICCCBDA)*, Chengdu, China, pp. 449-453, 2019. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [32] Qiang Zhang et al., "Quantum Information Research in China," *Quantum Science and Technology*, vol. 4, no. 4, pp. 1-8, 2019. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [33] Leilei Huang et al., "Quantum Random Number Cloud Platform," *npj Quantum Information*, vol. 7, no. 1, pp. 1-7, 2021. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [34] Savo Glisic, "Quantum vs Post-Quantum Security for Future Networks: Survey," *Cyber Security and Applications*, vol. 2, pp. 1-19, 2024. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [35] Marel Alvarado et al., "A Survey on Post-Quantum Cryptography: State-of-the-art and Challenges," *arXiv preprint*, pp. 1-16, 2023. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [36] Chonggang Wang, and Akbar Rahman, "Quantum-Enabled 6G Wireless Networks: Opportunities and Challenges," *IEEE Wireless Communications*, vol. 29, no. 1, pp. 58-69, 2022. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [37] Dimitris Zavitsanos et al., "On the QKD Integration in Converged fiber/Wireless Topologies for Secured, Low-Latency 5G/B5G Fronthaul," *Applied Sciences*, vol. 10, no. 15, pp. 1-21, 2020. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [38] Dinka Milovančev et al., "High Rate CV-QKD Secured Mobile WDM Fronthaul for Dense 5G Radio Networks," *Journal of Lightwave Technology*, vol. 39, no. 11, pp. 3445-3457, 2021. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [39] Ivan Vybornyi, Abderrahmen Trichili and Mohamed-Slim Alouini, "Backflash Light as a Security Vulnerability in Quantum Key Distribution Systems," *Physical Layer Security*, pp. 83-97, 2021. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [40] Miralem Mehic et al., "Quantum Cryptography in 5G Networks: A Comprehensive Overview," *IEEE Communications Surveys and Tutorials*, vol. 26, no. 1, pp. 302-346, 2024. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [41] Thu A. Pham, and Ngoc T. Dang, "Quantum Key Distribution: A Security Solution for 5G-based IoT Networks," *2022 International Conference on Advanced Technologies for Communications (ATC)*, Ha Noi, Vietnam, pp. 147-152, 2022. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [42] Rahul Jain, and Srijita Kundu, "A Direct Product Theorem for Quantum Communication Complexity with Applications to Device-Independent QKD," *2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS)* Denver, CO, USA, pp. 1285-1295, 2022. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [43] Nitin Jain et al., "Modulation Leakage Vulnerability in Continuous-Variable Quantum key Distribution," *Quantum Science and Technology*, vol. 6, no. 4, pp. 1-12, 2021. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [44] A.S. Trushechkin et al., "Security of the Decoy state Method for Quantum key Distribution," *Physics-Uspekhi*, vol. 64, no. 1, pp. 88-102, 2021. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [45] Rupesh Kumar et al., "Experimental Vulnerability Analysis of QKD based on Attack Ratings," *Scientific Reports*, vol. 11, no. 1, pp. 1-12, 2021. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]

- [46] Scott Rose et al., “Zero Trust Architecture,” *NIST Special Publication*, vol. 800, no. 207, pp. 1-52, 2020. [[Google Scholar](#)]
- [47] John Kindervag, “Build Security into Your Network’s DNA: The Zero Trust Network Architecture,” *Forrester Research, Inc*, vol. 27, pp. 1-16. 2010. [[Google Scholar](#)]
- [48] Maliha Sultana et al., “Towards Developing a Secure Medical Image Sharing System based on Zero Trust Principles and Blockchain Technology,” *BMC Medical Informatics and Decision Making*, vol. 20, no. 1, pp. 1-10, 2020. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [49] Keyvan Ramezanzpour, and Jithin Jagannath, “Intelligent Zero Trust Architecture for 5G/6G Networks: Principles, Challenges, and the role of Machine Learning in the Context of O-RAN,” *Computer Networks*, vol. 217, pp. 1-17, 2022. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [50] Xiaopeng TIAN, and Haohao SONG, “A Zero Trust Method based on BLP and BIBA Model,” *2021 14th International Symposium on Computational Intelligence and Design (ISCID)*, pp. 96-100, 2021. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [51] Nakul Ghate et al., “Advanced Zero Trust Architecture for Automating Fine-Grained access Control with Generalized Attribute Relation Extraction,” *International Conference on Emerging Technologies for Communications*, vol. 68, pp. 1-4, 2021. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [52] Luca Ferretti et al., “Survivable Zero Trust for Cloud Computing Environments,” *Computers and Security*, vol. 110, 2021. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [53] Annamalai Alagappan, Sampath Kumar Venkatachary, and Leo John Baptist Andrews, “Augmenting Zero Trust Network Architecture to Enhance Security in Virtual Power Plants,” *Energy Reports*, vol. 8, pp. 1309-1320, 2022. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [54] Dan Tyler, and Thiago Viana, “Trust no one? A Framework for Assisting Healthcare Organisations in Transitioning to a Zero-Trust Network Architecture,” *Applied Sciences*, vol. 11, no. 16, pp. 1-18, 2021. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [55] Erik Dean et al., “Toward a Zero Trust Architecture Implementation in a University Environment,” *The Cyber Defense Review*, vol. 6, no. 4, pp. 37-48, 2021. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [56] Shan Li, Muddesar Iqbal, and Neetesh Saxena, “Future Industry Internet of Things with Zero-trust Security,” *Information Systems Frontiers*, vol. 26, no. 5, pp. 1653-1666, 2024. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [57] Moyan Lyu, and Junaid Farooq, “Zero Trust in 5G Networks: Principles, Challenges, and Opportunities,” *2024 Resilience Week (RWS)*, Austin, TX, USA, pp. 1-8, 2024. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [58] Mahnsuk Yoon et al., “Design and Implementation of a 5G Security Testbed Based on Zero Trust Architecture,” *2024 15th International Conference on Information and Communication Technology Convergence (ICTC)*, Jeju Island, Korea, pp. 2190-2192, 2024. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [59] Ziqing Zhu, “Q-EnergyDEX: A Zero-Trust Distributed Energy Trading Framework Driven by Quantum Key Distribution and Blockchain,” *arXiv preprint arXiv*, pp. 1-11, 2025. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [60] Venkatesh H, and Sashikanth Reddy Avula, “Crypto-Agile Zero-Trust Access for Multi-Cloud via SDN, with PQC-QKD Key Orchestration,” *2025 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS)* Kolhapur, India, pp. 1-5, 2025. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [61] Jan Krause et al., “Dynamic Rerouting and Interruption Resilience of Quantum Communication via Single-Photon-Based Resynchronization,” *arXiv preprint arXiv*, pp. 1-9, 2025. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [62] Chia-Wei Tsai et al., “Quantum key Distribution Networks: Challenges and Future Research Issues in Security,” *Applied Sciences*, vol. 11, no. 9, pp-1-15, 2021. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [63] Yongjun Ren et al., “Zero Trust Networks: Evolution and Application from Concept to Practice,” *Computers, Materials and Continua*, vol. 82, no. 2, pp. 1593-1613, 2025. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [64] Hua Wang, Yongli Zhao, and Avishek Nag, “Quantum-Key-Distribution (QKD) Networks Enabled by Software-Defined Networks (SDN),” *Applied Sciences*, vol. 9, no. 10, pp. 1-12, 2019. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [65] R.S. Tessinari, R.I. Woodward, and A.J. Shields, “Software-Defined Quantum Network using a QKD-Secured SDN Controller and Encrypted Messages,” *Fiber Optical Communication Conference Optica*, pp. 1-3, 2023. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]