future internet

MDPI

Review

Quantum Key Distribution for 5G Networks: A Review, State of Art and Future Directions

Mohd Hirzi Adnan [1,*], Zuriati Ahmad Zukarnain [1,*] and Nur Ziadah Harun [2]

[1] Department of Communication Technology and Network, Faculty of Computer Science and Information Technology, University Putra Malaysia, Seri Kembangan 43400, Selangor, Malaysia
[2] Department of Web Technology and Information Technology, Faculty of Computer Science and Information Technology, University Tun Hussein Onn Malaysia, Batu Pahat 86400, Johor, Malaysia; nurziadah@uthm.edu.my
* Correspondence: gs55435@student.upm.edu.my (M.H.A.); zuriati@upm.edu.my (Z.A.Z.)

Abstract: In recent years, 5G networks and services become progressively popular among telecommunication providers. Simultaneously, the growth in the usage and deployment of smartphone platforms and mobile applications have been seen as phenomenal. Therefore, this paper discusses the current state of the art of 5G technology in the merger of unconditional security requirements referred to as Quantum Cryptography. The various domain of Quantum Cryptography is illustrated including the protocols available, their functionality and previous implementation in real networks. This paper further identifies research gaps covering critical aspects of how Quantum Cryptography can be realized and effectively utilized in 5G networks. These include improving the current technique in Quantum Cryptography through efficient key distribution and message sharing between users in 5G networks.

Keywords: quantum communication; QSDC; QKD; 5G

Citation: Adnan, M.H.; Ahmad Zukarnain, Z.; Harun, N.Z. Quantum Key Distribution for 5G Networks: A Review, State of Art and Future Directions. *Future Internet* **2022**, *14*, 73. https://doi.org/10.3390/fi14030073

Academic Editors: Savio Sciancalepore, Giuseppe Piro and Nicola Zannone

Received: 10 January 2022
Accepted: 14 February 2022
Published: 25 February 2022

1. Introduction

The 5G networks are rapidly adopting various developing technologies to provide high-speed data delivery. The 5G technology is being used in a variety of applications such as smart city, Industrial Internet of Things (IIoT), and smart grid to meet the user needs and provide faster connection speed with high reliability and low latency for remote access to routine services. The 5G architecture intends to utilize various nodes to offer secure and on-demand connectivity to other devices. The 5GPPP mobile networks prefer to use high-frequency technology to strengthen many devices faster with fewer interruptions. With applications involving a phenomenally vast number of IoT devices and BSNs, improving the network's security at all layers becomes a major goal. When many devices are running simultaneously, it becomes difficult to detect the security threats and adversaries who can obscure the vast amounts of data transmitting across the network. Security enhancement is needed since larger spectrum space is accessible on 5G networks that can support heavy bits without reducing transmission range. Consequently, the security improvement demands an advanced set of protocols that consider the operation and architecture of 5G networks.

Moreover, 5G communication systems are prone to security vulnerabilities, and various existing studies show the types of attacks that can significantly affect network performances. Furthermore, since these systems must operate instantly, the presence of contaminated codes, malware, wormhole, Trojans, and viruses in 5G devices can disrupt the entire network. Different technology enablers that support the 5G networks are software-defined networks (SDNs), network function virtualizations (NFV), multiple-input multiple-output (MIMO), non-orthogonal multiple access (NOMA), radio access networks (RAN), Massive-MIMO, device-to-device communications (D2D), simultaneous wireless information and power transfer (SWIPT), low-power wide-area networks (LPWAN), network slicing, orthogonal frequency division multiple access (ODFMA), etc.

In the information security areas, cryptography is not considered a new field. One of the most classical concepts in cryptography is to combine a message with another piece of information when converting a bit of information. The cryptography techniques can be categorized as classical cryptography and quantum cryptography. The classical techniques can be divided into two categories: Symmetric and Asymmetric cryptographic, where the suitable categories rely on the required number of keys for encryption. However, both types are determined by the complexity of the mathematical factorization. With high technological computing such as quantum computing, any complex problems can be solved within a few minutes. Furthermore, there is a new cryptography category derived from quantum physics, which is called Quantum cryptography. As part of its physical characteristics, the researchers utilized it in cryptographic development to guarantee information security. Quantum cryptography is an upgrowing technology that uses the quantum mechanical system to process, secure, and transmit information instead of using a classical computational method. This method relies on mathematical algorithms that encrypt, secure communication, and transmit information between different parties using symmetric or asymmetric key distribution [1]. However, some advanced mathematical constraints and the massive technology growth are threatening the traditional cryptography protocols. Nowadays, as the intensity of software applications, websites and web browser is growing, it will introduce cybersecurity and cryptography implications [2]. However, when using QKD, the needs for communication and requirements of security collide physically. Furthermore, the engineering that is necessary to balance these challenges has a very narrow margin for error. As a result, rather than being guaranteed by physical laws, the security of QKD is largely implementation-dependent. Currently, sector such as governments, military and healthcare are not implementing QKD solutions in their applications due to these limitations. Consequently, QKD techniques must be implemented in conjunction with cryptographic authentication systems to prevent any security regression.

To use quantum cryptography efficiently, researchers proposed a Quantum Key Distributed (QKD), a fundamental technology based on the law of physics that ensures a secure exchange of symmetric encryption keys. Even though the concept of QKD was proposed in early 1980 [3], it took many years to be accepted and implemented. Since then, the progress in QKD shows remarkable improvement. The concept of Quantum Key Distribution is based on the principles of key distribution. The theory is that the sender and the receiver share the public key using a channel to ensure that the public key is not tempered. Consequently, the most crucial part of the encryption process is the key distribution. QKD is based on transmitting secure quantum cryptographic keys between different parties [4]. The main concept of communication in QKD relies on enabling two parties to share random keys based on their private polarization angles, which are used as an encryption and decryption mechanism, as mentioned in Figure 1. A sender will send a stream of photon-based on a private polarization pattern which the receiver will receive a stream of photons and then passing it through his private polarization. After that, the sender and receiver will establish a secure classical communication in which they will compare all the photons, keeping the matched photons and destroying the rest. The matched photons are considered thoroughly accurate and safe. Therefore, QKD is regarded as a secure key for data distribution between parties. Using the same session output, the secure key can establish future secure sessions between the same parties. Moreover, QKD can provide future security proof, which means that even if the cryptographic system crashed for any reason, the prior data communications and session remains secure.

The 5th generation or 5G network is launched in 2019 to enhance and overcome some of the limitations in the previous network generations such as enhances broadband mobile services and wireless access services. It works to improve mobility by providing great capacity and faster data speed that offers more excellent connectivity for people on the move. 5G promises to lower the communication latency, opens the possibility of real-time control of devices, industrial robotics, vehicle to vehicle communications and safety systems, autonomous driving, and safer transport networks. Those new features

contributed to the possibility to connect more devices than ever before which ensure the opportunity of massive machine-to-machine communications without human intervention. 5G also will be mainly involved in manufacturing, industrial, agricultural revolutions. 5G is expected to bring a drastic change in recent technology. As a result, several reviews and research were conducted in 5G [5–7]. Although security was one of the main requirements in 5G, however, limited research was proposed in that domain such as [8–10] are some of few a survey that emphasizes on the security challenges and communications security of 5G. In the 5G security model, the main security domain such as confidentiality, integrity and availability are ensured [11].

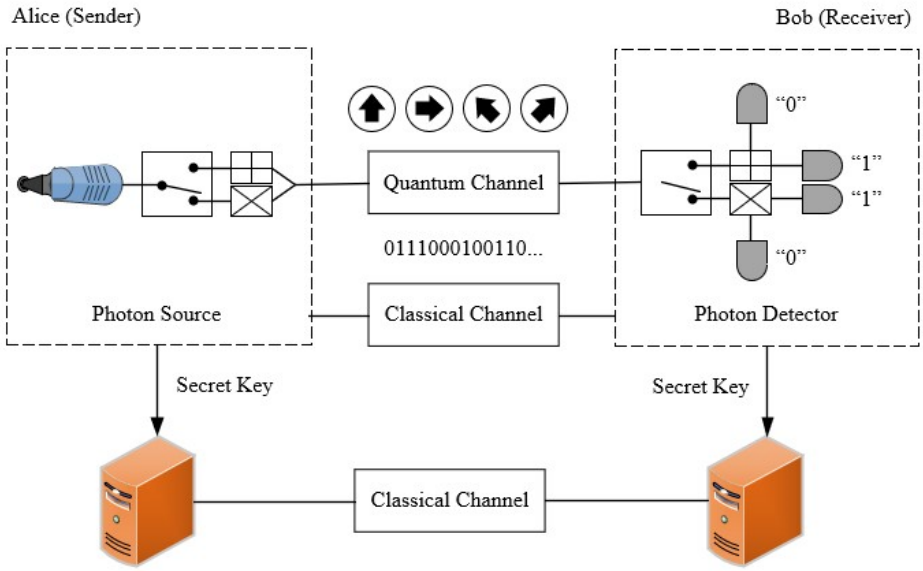

Figure 1. Classical QKD Mechanism (Polarization-encoding BB84 protocol).

Therefore, it is critical to emphasize the security challenges that exist in the 5G communication systems. This paper focuses our research on the 5G security challenges that need immediate security measures. We further examined the quantum key distribution (QKD) as the potential security solution for the threats illustrate in this paper. The main contributions of this paper are:

- We discuss the challenges in 5G networks in terms of privacy and security.
- We provide classification of QKD for 5G networks into three types of categories, including, single photon, multiphoton, and entanglement approach.
- We present the challenges of QKD implementation in 5G networks.

The remainder of this paper is organized as follows. Section 2 discusses the security challenges in 5G. The importance of QKD is demonstrated in Section 3, while Section 4 presents the QKD classifications. Lastly, the conclusion and future works are discussed in Section 5.

2. Security Challenges in 5G Network

Due to the global service demands the number of connected machines as mobiles, IoT, and IIoT devices, has been immensely increased. This improvement has a great impact on the regular network efficiency and capacity for that matter a 5G network technology is proposed to provide an efficient network that can cope with the recent technology revolution.

Some of the 5G benefits is providing a quality of services based on user requirements and also 5G ensure the validity of peer-to-peer communication [12]. It promises the world with a heterogeneous network that focuses on individual reliability and integrity. Moreover, 5G proposed unlimited wireless connectivity. That depends on the high speed of data with low latency. It considers as the core foundation of the future of IA technology. Nevertheless, 5G encounter different security major issues in main security characteristics. Several of

those vulnerabilities are in confidentiality as the risk of eavesdropping, a man in the middle, side channel, stalking attacks, other vulnerabilities affecting the availability such as jamming attacks and DDOS, DOS attacks [13]. As mentioned earlier, 5G provide a proper quality of services (QOS) for end-users. However, the primary end-user's private information such as location, personal data, activities are vague in data maintained, data storage, and the data storage conditions.

The privacy issues in 5G can be divided into two aspects: user and network aspects. From the user aspect, end-to-end data privacy is one of the privacy issues that can evoke 5G. Since a 5G network is mostly connected to a cloud system, which supports several stakeholders in the network, such as service providers, operators, and any new technologies that are connected to business models. Most stakeholders will depend on cloud computing to store and process user's data and make the data accessible. Sharing this data between different parties can lead to privacy breaches. Thus, the end-to-end security in 5G should be handled instantly [14,15]. Another issue is the different trust objectives between the data owner and the cloud stakeholders. This conflict can raise a different perspective on privacy. Such as losing data ownership in the 5G network, which is one of the coming issues. The 5G network provides a shared network infrastructure to run many applications together such as health care smart homes or IoT devices those shared access programs can manipulate and forge access by attackers thus 5G insecure data ownership bounders rise the chance of unauthorized access, exchange, and retrieving confidential data [16]. Another issue that is facing by 5G is the trans-border information since the global digitalization and excessive data exchange all the information will be traveled across borders as free flow this flow will be mandate based on government consent of data transfers, data storage, and data processing [17,18].

Meanwhile, the security issues in 5G can be divided into several key areas such as authentication, access control, communication, and encryption.

2.1. Authentication

Authentication is a crucial security aspect in every communication channel to validate the users' identity. Every generation of mobile communication has developed various methods and frameworks for the authentication process. Consequently, this section focuses on the authentication scheme designed by 3rd Generation Partnership Project (3GPP) specifically for the 5G communication system. Generally, there are two categories of authentication that is primary and secondary. 3GPP has released the evaluation standard of 5G Phase 1 in the 3GPP Release 15. Network and device mutual authentication that supports both 4G and 5G is provided in the primary authentication. However, primary authentication also has some limitations because of the evolved 5G environment. Home automation authentication system manages the information and device authentication. 5G Authentication and Key Agreement (5G-AKA) and Extensible Authentication Protocol (EAP-AKA) are two primary mutual authentication techniques in 5G Phase 1. EAP-based authentication is allowed for a particular scenario, such as private networks. Since primary authentication is not dependent on the Radio Access Technology (RAT), it can be used with non-3GPP technologies. Secondary authentication is used to authenticate data networks outside of a mobile network operator's area.

EAP based authentication and associated credentials methods can be applied to this method. Supplying key material to be used between the network and UE along with mutual authentication can be achieved using primary authentication and key management. The serving network-specific anchor key (KSEAF) are provided by key agreement procedures and the primary authentication. In the serving network, KSEAF is sent to Security Anchor Function (SEAF) by the home network's Authentication Server Function (AUSF). Based on technical specifications published by ETSI and 3GPP, AUSF works as a Network Function (NF) Service Provider that offers UE authentication to the requester NF. Furthermore, AUSF gives the NF service customer access to the Access and Mobility Management Function

(AMF) for UE authentication. During the authentication process, NF supplies AUSF with the UE's identification and serving network name.

For EAP-based authentication or 5G-AKA, AUSF will utilize the information supplied by AMF. Various research on security threats and security mechanisms for heterogenous 5G has been conducted for different scenarios and threats. Formal analysis on the 5G-AKA authentication protocol is shown in [19], where the security goals weaknesses are highlighted, and the requirements of 3GPP standards for 5G networks are discussed. Hussain et al. proposed a public-key infrastructure (PKI) based authentication scheme deployed above the asymmetric cryptography to authenticate the base station in the 5G network. Moreover, the analysis of 5G-AKA is presented by authors in [20]. The research shows that the 5G-AKA depends on the core network. Borgaonkar et al. discussed the challenges and threat model for 5G-AKA protocols, where the author demonstrated the logical vulnerabilities that require dedicated fixes [21]. Behrad et al. investigated the vulnerabilities of 4G and 5G-AKA protocol to understand the weaknesses of Authentication Authorization and Accounting (AAA) [22]. Authors in [23] presented the 3GPP-AKA protocol with perfect forward secrecy for the session key. The proposed protocol focused on the compatibility of perfect forward secrecy with the current Universal Subscriber Identity Module (USIM) 5G-AKA protocol.

Moreover, Giustolisi-Gerhmann in [24] offers a group-based authentication threat model for a heterogeneous 5G network. In [25], the authors studied the 5G-AKA protocol for the 5G mobile communication network. The proposed protocol utilized asymmetric randomized encryption to provide better privacy and secure communication. Furthermore, the proposed protocol shows that all possible attack against 5G-AKA privacy still applies except the IMSI-catcher attack. The authors also modified the existing 5G-AKA protocol for prevention strategies. The authors in [26] developed an advanced authentication and key agreement protocol for the 5G mobile network. The proposed scheme applies random numbers, which resulting robust security and decreased communication cost. The authors utilized public-key cryptography to encrypt the SUPI and generating the SUCI.

Furthermore, since current USIMs can execute random asymmetric encryption procedures, a random number can be used in the 5G-AKA protocol. Moreover, the proposed solutions guarantee forward security and post-compromise security. An efficient and seamless vertical handover authentication protocol for a 5G wireless mobile network is presented in [27]. The proposed mechanism offers fast, strong, and mutual authentication. Furthermore, the authors suggested using a certificate-based approach called Extensible Authentication Protocol-Transport Layer Security (EAP-TLS). Ma-Hu in [28] investigated handover authentication schemes using cross-layer collaborative techniques for a 5G heterogeneous network. The proposed method offers reliable and secure services by utilizing the cross-layer such as physical layer to implement the EAP-AKA authentication.

Moreover, the proposed scheme executed the physical layer authentication using the non-parametric Kolmogorov-Smirnov (K-S) test. In [29], the authors considered the 5G security model in their proposed protocol. They developed a 4G+ relative authentication protocol (4G + RAM) that depends on 4G+ frequency re-authentication protocol (4G + FRP) and privacy-protected authentication and key agreement protocol (PEPS-AKA). Wang et al. presented two protocols to provide anonymity and secure device-to-device (D2D) group communications [30]. The first protocol is the privacy-preserving authentication protocol (PPAKA-HMAC), where the session key is created and combined with the hash-based message. The second protocol is the key agreement protocol (PPAKA-IBS) where it protects against internal attacks by utilizing IBS instead of HMAC. Shin-Kwon in [31] introduced a two-factor authentication scheme in heterogeneous WSN for IoT to provide anonymity, mutual authentication, and protection against various attacks.

2.2. Access Control

Performing selective limitation of the access for the network is the main purpose of access control. Since access control is the main component for any network security system,

securing and providing a safe network to end-users is crucial for network providers. The authentication of user access is confirmed in the access control environment. The concept of access control strategies shows at the implementation-independent level before applying to real-time systems using accessibility policies systems. Several current access control systems show that network decentralization can upgrade the security of the network system environment. Research in [32] investigates access selection schemes for device-to-device physical layer security with different eavesdroppers. Taking distance threshold into consideration, the authors proposed sharing the spectrum between D2D devices and cellular users. The interference generated is used to confuse the eavesdroppers using jamming. The authors use the D2D protection pair to secure a single user and optimal throughput access selection scheme to increase securities.

Furthermore, in [33], the authors introduced an automated framework called ConfigSynth to synthesize network security configurations and provide affordable network configuration. The author improved the security framework by designing a refinement mechanism. The algorithm is used to offer better security device distribution, isolation, and improved traffic flow. In [34], the authors update LTE pseudonyms by utilizing the current pseudonym-based solutions to prevent International Mobile Subscriber Identity (IMSI) downgrade attacks using fake base stations. Various access control solutions have been proposed based on authentication, encryption, authorization, and secret sharing. The authors in [35] proposed a privacy-preserving and accountable access control to guarantee user privacy. The validity of the protocol is authenticate using restricted experimental resources.

Meanwhile, the authors in [36] introduced a biometric and password-based authentication scheme for Telecare Medicine Information System (TMIS). The proposed solution works by offering anonymity, authentication, forward secrecy, and lower computational cost without the involvement of a remote server. Moreover, a general verification scheme for access control policies is proposed to expand the current management and policy specification [37]. An access control scheme for IoT based on the computer outsourcing and ciphertext update is presented by authors in [38]. The proposed method uses attribute-based encryption (ABE) to encrypt the user's data before storing the data into cloud storage.

Qinlong et al. offered an efficient and secure data sharing scheme for Online Social Networks (OSNs) that are developed using secret sharing and Ciphertext-Policy Attribute-Based Proxy Re-Encryption (CPABPRE) [39]. The authors also reduced the computational overhead by introducing partial decryption construction. The construction distributes the decryption process to OSNs, examine the ability mechanism to ensure decrypted data by OSNs, attribute revocation technique to attain forward and backward secrecy. Moreover, authors in [40] proposed a node admission protocol using secured ephemeral mobile ad-hoc network (MANET) using bi-variate polynomial secret sharing. The proposed scheme is a secure admission method to ensure sharing, efficiency, and non-interactive. MANETs are permitted to distribute efficiently and secretly pairwise secret keys without any assistance from a centralized system. The authors also develop a method for creating fast and spontaneous secure communication links from the pair of nodes. Castiglione et al. introduced shared encryption-based construction (SEBC) access control schemes based on general hierarchical access control [41]. The proposed scheme used symmetric encryption and secret sharing to add authorized users to the system. The scheme allows the management of access to different users and details other methods of accessing the system. The authors also developed a secure and efficient key assignment protocol based on threshold public-key encryption.

In ad-hoc networks, unique characteristics exposed the system to potential vulnerabilities. Access control such as ad-hoc network group is important because it can prevent any unauthorized individual or group from accessing the system. Authors in [42] investigated a robust access control protocol attack that depends on a new proactive RSA signature scheme. The authors emphasize that the adversaries can recreate the shared secret using

the information obtained in the RSA signature scheme. Wang et al. studied the cooperative relaying using multiple-input single-output (MISO) for multiple distance vehicles [43]. Techniques such as signal superposition and cooperative jamming are used where an adjacent user decodes the signal and performs as a remote user relay. After a detailed examination of the eavesdropping security threats, the authors propose an improved secure transmission scheme.

In [44], the authors examined the reliability and security in the downlink of cloud radio access network (C-RAN) practical scenario with channel estimation (CE) errors as consideration and remote radio heads (RRHs) node selection. Cheminod et al. presented a novel framework in implementing semiautomatic verification for access control policy [45]. The proposed technique developed for Industrial Network Systems (INS) applies a twofold model that considers two system views: access control policies abstract requirement and specific details of physical target scheme. Furthermore, the authors also used role-based access control (RBAC) in the proposed framework to determine the policies. The utilization of micro 5G operators or local 5G networks can lead to frequent roaming events in 5G networks because most of the 5G operators have a lower level of security compared to main mobile network operators [46–48]. Therefore, the probability of running into malicious 5G operators that work as a serving network is highly possible [26]. Consequently, a strong authentication process in a 5G network is required to prevent the connection with such networks.

2.3. Communication Security

The goals of 5G communications are to offer connectivity, low latency communication, high data bandwidth, and extensive signal coverage to any type of device in the 5G ecosystem. Consequently, the integration of 5G technologies and architectural changes will be updated in the 5G communication. However, some threats and challenges need to be mitigated in 5G mobile networks [49]. An efficient and reliable mobile network requires secure communication among various control entities. Enabling secure 5G communication will require integrating 5G core network elements and efficient key management entities.

Furthermore, security parameters and key exchanges need to be frequently updated along with 5G core security network elements. In a 5G network, the overhead cost of security maintenance such as communication cost, battery life, bandwidth and processing power significantly increase because of the additional control entities such as core network elements, number of base stations, and subscribers. Therefore, a proper solution needs to be proposed to solve these challenges for future secure communication systems in the 5G network. The adversaries use various attack segments such as access networks, user equipment, and mobile operators core networks to launch an attack on 5G communication [50]. To help comprehend the challenges and security issues affecting on 5G network, Table 1 shows the security issues related to the 5G communication channel and the point of impact for each security issue. There are two categories in 5G core networks: user data traffic and control traffic. Both types are vulnerable to various security threats. However, the main security issue of control traffic is the inadequate IP level security.

The security protocol in the application layer, such as Secure Sockets Layer (SSL) or Transport Layer Security (TLS), is used to secure the communication channel in the SDN-based 5G core network. The network has known TCP/IP security threats such as TCP sequence number attack, TCP session hijacking, SYN flooding, IP spoofing, eavesdropping attacks, TCP reset attacks [51]. Consequently, the use of an IP security mechanism that combines with a multilayer security mechanism is necessary. Securing the control channel using IPSec based security framework has been proposed by authors in [2,52,53]. Different SDN controllers are used to manage different network segments in SDN mobile networks [54]. The east/west traffic interface is utilized to initiate inter-controller communication (ICC) channel connecting various SDN controllers. The interface supports performing multiple network functions such as traffic and mobility management, network monitoring, and security policy synchronization by sharing control information. Therefore, securing the ICC

channel is important in guaranteeing the appropriate operation of the network functions. The entire system will be compromised if the core ICC channel is penetrated despite the condition of the rest of the network.

Table 1. Security issues of 5G communication.

Attack Segment	Challenge/Threat	Effected Technology				Privacy
		SDN	NFV	Channels	Cloud	
Device Threats	Bots	*				
	DDoS Attacks	*	*		*	
	MitM Attacks	*				*
	Firmware Hacks					*
	Device Tampering					*
	Malware					*
	Sensor Susceptibility			*		
Air Interface Threats	Jamming	*		*		
	MitM Attacks	*		*		*
	Eavesdropping		*			*
Edge Network Threats	MEC Server Vulnerabilities	*	*			
	Rouge Nodes	*	*	*		*
	Authentication Issues					*
	Side Channel Attacks	*				
	Improper Access Control	*	*		*	*
Backhaul Threats	DDoS Attacks		*	*		
	Control and User Plane Sniffing		*	*		*
	MEC Backhaul Sniffing		*	*		
	Flow Modification Attacks			*		
5G Core Network Threats	Software Issues				*	
	API Vulnerabilities	*				
	Network Slicing Issues	*	*			
	DoS and DDoS Attacks	*	*		*	
	Improper Access Control					*
	Virtualization Issues		*		*	
External Network Threat	Application Server Vulnerabilities					*
	Cloud Service Vulnerabilities					*
	BoTs and other IP-based Attacks	*				*
	Application Vulnerabilities					*
	API Vulnerabilities	*				
	Roaming Partner Vulnerabilities	*	*		*	

The current SDN inter-controller channel is vulnerable to various web-based and IP-based attacks such as DNS hijacking, replay attack, DDoS, and IP port scan [55,56]. 5G ICC will be imminently vulnerable to cyber-attacks and extensive physical threats such as human errors, technical failures, and disaster failures. Additionally, the only consideration for the current SDN communication system is the cyber-attacks impact. Authors in [56] introduced identity-based cryptography (IBC) based secure key exchange scheme in a multi-controller SDN network to secure the east/west-bound data transmission. However, the authors did not emphasize current physical threats and cyber-attacks. Recent advances in adaptive security provide a more resilient and flexible approach than industrial 5G security.

Furthermore, the security solutions are mostly developed by different vendor proprietary solutions. Consequently, real-time synchronization and mix-and-match security systems are nearly impossible and difficult in current existing networks [57]. Therefore,

new flexible and resilient security systems for 5G network are needed since it is impossible to change the existing system to prevent potential adversaries' attacks.

2.4. Policies

New technologies, stakeholders, regulations, verticals, businesses, and end-users will be included in the extremely large 5G networks. The 5G are considered the best platform for the new generation of networks such as industries, smart cities, vehicles, and IoT. The applications, devices, users, and machines will produce a large quantity of data. This enormous data will be collected, analyzed, processed, combined, and stored for various purposes such as cross-border data flows. Furthermore, the data belong to the applications, organizations, societies, citizens, individual consumers, etc. In the classical network, the risk of user privacy mostly originates from the plaintext communication of the application data in the network. There is a high risk that user privacy is exposed to data leaks.

Consequently, one of the challenges in 5G network is to secure end-user privacy. Solving privacy issues for all the stakeholders is a complex task since there are multiple interests at risk. However, some privacy issues are highlighted from the cloud computing perspective because of the relevance of cloud computing concepts to various 5G network technologies, for instance, NFV, SDN [17].

- End-to-End data privacy issues: Stakeholders such as service providers, mobile operators, businesses, and new technologies utilizing new business models are currently supported by 5G networks. Most of the stakeholders use cloud computing technology to store and access users' data. These personal data will then be managed and shared among various stakeholders for multiple purposes, leading to privacy breaches. Consequently, methodology for end-to-end data confidentiality must be considered to secure user privacy [14,15].
- Personal data ownership and shared environment issues: The 5G network can assist application controls such as smart grid and healthcare running on virtual networks and providing shared network infrastructure. However, these network infrastructures are vulnerable to unauthorized data access [16]. Thus, effective functions of share network infrastructure without affecting users' privacy are needed. Furthermore, the party responsible for the data losses in shared network infrastructure is still a major concern for the users. Therefore, different stakeholders such as service providers, network operators and other third parties must be assigned licensing and ownership of personal information.
- Various trust objectives issues: For classical 5G network, communication service providers and mobile operators might joint ventures and migrate some segment of their network into the cloud. For such cases, these stakeholders may decide the trust objectives based on their regulations and policies [17]. Consequently, these stakeholders may not take all the aspects of user data privacy into consideration.
- Cross-border data flow issues: As a result of global digitalization, personal data is considered an essential commodity of the modern market. The information is expected to flow freely across the borders. Therefore, it is crucial to require consent from the government and individuals for any data transfers, including the methodology for storing and processing across the border [17,18].
- Issues of the third party in the 5G network: 5G and IoT offer a new opportunity to the application developers to develop immersive applications that employ various communication protocols. Since the application developers can access the 5G network, the developers can sell or disclose the private data to a third party. In [58], the author explained that by using the mobile application, "the health insurance portability and accountability act (HIPPA) allow a share out of individual's health data". Furthermore, the cloud network policies for information sharing can consequently invoke the issues of data privacy.

As for the future directions, various potential future research can be conducted to mitigate the data privacy issues since 5G technologies can be designed to offer privacy

protection for a data source or privacy embedded for application, device, or service. Privacy-by-Design (PbD) is one of the general architectures for 5G privacy that future researchers can define and focus on. Other wide areas can be investigated, such as location-privacy based on multi-access edge computing (MEC). Data processing for MEC occurs at the edge nodes, where the operators will monitor and control the nodes. Moreover, some examples of 5G applications that will directly impact the privacy solutions are healthcare, IoT, transportation, and smart cities.

Furthermore, other methods such as software-defined privacy (SDP) also can be used in the 5G network [17]. SDP allows privacy officers to define and implement an IaaS Cloud Customer privacy policy [59]. The methods in managing and storing data under different policies are still at an early stage. The author in [60] proposed PADRES, an open-source tool to examine web applications and aid in the compliance process for securing data, privacy, and security. The proposed tools can be extensible by adding questions related to general data protection regulation and more cookie and vulnerability analysis tools. However, the tools' limitations include that the breadth and scope of the questions must be expanded, as well as more case studies and end-user input.

Since 5G network contain various stakeholders (such as ISP, mobile network, CSP) and different connected verticals (such as smart cities, data centres, power distribution) that may have different objectives, effective regulation on the privacy policies for various entities such as user, government, and other industries level are needed.

To summarize, 5G is the iteration of cellular technology and is designed to improve the speed and quality of services of wireless networks. 5G technology plays an important part in securing the communications. Thankfully, as technology advances, so do the tools available to protect it. Nowadays, secure communications are widely utilized; they are incorporated into any web browser that communicates over the Internet, and they allow users to connect physically mobile devices or different corporate networks to private networks. Quantum keys can make 5G communications significantly more secure by physically transferring secret key sharing between two entities. To generate the shared key, QKD can be used instead of asymmetric key agreement systems, which is subsequently employed in symmetric schemes to safeguard messages.

3. The Importance of Quantum Key Distribution (QKD)

The importance of quantum is derived from its high security and reliability compared to the classical key distribution. The classical key distribution is deployed and tested using cryptography techniques that are widely used. A classical key distribution is based on mathematical equations and computational complexity, which used two different fundamental distribution techniques namely symmetric techniques and asymmetric techniques. The symmetric techniques are applied when both sender and receiver share the same secure, and access protected key. On the other hand, the asymmetric technique provides both public and private key that is preserved and protected. The private key is used to keep the confidentiality and authenticity of each party in the communication. Those security methods were acceptable and widely used until Shor's algorithm was introduced which is the quantum cryptography technique that are used to enhance the security of any communication in the network. For that matter, quantum was proposed as an advanced and efficient mathematical operation that undermine the security of RSA. Furthermore, quantum can defeat the discrete logarithm problem consequently undermined the Elliptic Curve Cryptography method that is based on providing small key size with the same RSA cryptographic strength [61].

The quantum key distribution which based on quantum key distribution proves its reliability, privacy of security and high level of confidentiality by avoiding eavesdropping and providing holistic, different, and new concept on encryption mechanism that is based on the law of quantum mechanics and logic of physics. It can be considered as an innovative technology that proposing a new idea of transmitting photon lights between sender and receiver to establishing a secure connection [62]. There are two main principles of quantum

mechanics which quantum cryptography are based on namely the Heisenberg Uncertainty Principle and quantum no-cloning theorem. Some of the advantages of using QKD is related to the security that established secure communication that can replace the eventually breakable mathematical algorithm. Furthermore, QKD is virtually unbreakable. QKD prove its simplicity of use, regarding resource consumption, consume fewer resources compare to the classical key encryption. Finally, QKD can firmly detect and eliminate eavesdropping in any communication process.

The reason is that quantum mechanics prevents and will not replicate any alteration in a photon. This is due to the quantum properties are strengthened by the unconditional security as proved by the no-cloning theorem and Heisenberg Uncertainty theory. The polarization mode of the photon will change when the eavesdropper measures a photon, and eavesdropping will be observed according to quantum physics. The sending key is ignored when a photon is intercepted, and the rest of the key may be safe to send [63].

When it comes to a key agreement and asymmetric encryption methods, other options other than using QKD are using quantum-safe techniques if long-term security is required. Furthermore, the other option is to merge the existing mechanisms with the quantum-safe processes to prevent any security degradation caused by technical designs. In asymmetric signature techniques, replacing present algorithms is no longer necessary. Signatures, in contrast with encrypted messages, cannot be hacked after they have been sent. Moreover, signature systems based on known primitives currently exist that are unaffected by quantum computers. These schemes are suited in some scenarios even though it is not replacing the current methods completely.

A feature equal to QKD might be developed using purely symmetric methods unaffected by quantum computers in a theoretical world free from asymmetric key negotiation. When this type of solution is widely utilized, secure communication will revert to what they were before the mass acceptance of asymmetric mechanisms, which is expensive and complex while needing unified secret management and thus employed exclusively by large enterprises. They would, however, be simpler to implement than their QKD-based equivalents because they are suitable with current networks.

3.1. The Challenges of QKD in 5G Implementation

In general, 5G networking does not ensure encryption of data traffic. Rather it relies upon the top encryption sessions count on the end-user to ensure security maintenance and updates. Knowing that, end to end encryption will still be applied. A crucial prerequisite for unbreakable encryption is to secure the key exchange between different parties. However, nowadays, the well-known key exchange algorithms are believed to be vulnerable by large-scale quantum computers. There are two feasible routes to overcome this future risk namely quantum-resistant algorithms (QRAs) and quantum key dispersion (QKD). Each of the different approaches for QRA is based on robust mathematical proofs that reduce the power of the large-scale quantum computer. However, QKD is based on fundamental laws of quantum physics that provide strong communication security for any potential threats.

Currently, 5G takes advantage of public-key infrastructure (PKI). It affects both user equipment (UE) authentication to the network and how control and management plane services are securely interacting with each other. This embrace of PKI is happening just as advances in quantum computing begin to make cryptographers nervous about the longevity of workhorse ciphers such as Rivest-Shamir-Adleman (RSA) and Elliptic Curve Cryptography (ECC). To date, the density of qubits in quantum computers has matched a Moore's Law curve of doubling every 18 months. If these trends continue, ciphers such as RSA will be broken and unusable before 2030. QKD provide a promising encryption strategy that ensures security by using the concept of quantum physics. For that, QKD is a promising measure to provide secure communication for a large capacity 5G network. However, improving the transmission capacity has led to many problems such as the limited research on the impact of strong carrier and carrier-free signal in the secure key rate

in 5G networks. Moreover, there is limited research on the uncertainty of secret key rate effect on the QKD system in different bandwidths, cost, and power levels [64].

QKD is a sample of quantum cryptography that depends on a distributed classical key between legitimate users to achieving unconditional security. This concept was proposed using the form of the QKD protocol (BB84). However, BB84 can be hacked if the attacker uses a system of higher dimensions without the consent of legitimate parties. This limitation can be countermeasure using devices dependence DI which allow the QKD protocol to perform in a separate dependent device model that limits the analysis in the statistical form and the security based on those statistical experiments results [65]. A long-distance QKD implementation is considered one of the vital security challenges in quantum. Quantum cryptography is based on the strength of the photon length before it fades away in optical fiber. The problem was solved by place a repeater in the fiber optic to work as an amplifier that strengthens the photons before they are lost. This process depends on reboots the optical signal as if taking a copy of the signal to secure the transmission losses. However, QKD cannot trust the repeater to transmit the quantum data in the long-distance which means that the range of QKD is limited presents a contradictory dilemma in quantum cryptography between distance and efficient communication rete that explains basically as the longer the distance the weaker the photon signals becoming the fewer photons reaches the destination. In the past 10 years, many successful pieces of research contributions strengthen the signals to travel longer distances [66]. On the other hand, each repeater in the communication channel secures the key can be revealed thus the confidentiality can be easily exposed. Rebooting the signal will indeed reduce the number of repeaters along the communication channel, but it cannot eliminate it.

3.1.1. Implementation Cost

Firstly, the cost of specialist QKD communication hardware is expected to complicate the migration to quantum cryptography. Recently, many researchers were conducted toward using 5G with QKD to enhance the security of 5G with an attempt to limit the vulnerabilities on QKD. Due to the quantum communication over fiber optic has reached optimal performance caused by fixed loss related to fiber and the restriction of the device, it (fiber optic) can be replaced by free space channel that offers several advantages including flexibility of installation, broader geographical coverage, and cost-effectiveness in terms of infrastructure deployment [67].

3.1.2. Integration Issue

Secondly, in terms of integrating the QKD network with conventional telecommunication networks and also optical routing purposes [68,69], a technique such as wavelength division multiplexing (WDM) can be used in fiber-based QKD networks. Furthermore, the QKD integration scheme with conventional telecommunication data using a single fiber can considerably reduce the cost while able to increase the robustness of QKD applications. Townsend in 1997 [70] first introduced the scheme by concurrently transmitting a combination of QKD and conventional data. Later on, numerous QKD experiments are conducted to verify the feasibility in terms of QKD network integration with conventional telecommunication networks [71–74]. Moreover, an integration between 3.6 Tbsp. optical communication data and QKD over 66 km backbone fiber network has been conducted in 2018 [75].

3.1.3. Efficiency

The third challenge is efficiency. Efficiency can be justified by the number of classical and quantum resources used to transfer an amount of information. Currently, the QKD protocol only provides a steadiness key over 50 km with the only secure key rate of 1 Mb/s. With that, no QKD protocol can prove its efficiency to travel over 300 km using optical fiber. Thus, it is necessary to improve the efficiency over quantum channel. However, this approach is not able to guarantee end-to-end security.

3.1.4. Secure Secret Key Rate

The fourth challenge is the high channel loss and decoherence in long-distance due to the key rate of QKD that degraded over a long distance. For example, 1000 km fiber can detect merely 0.3 photons, even with the perfect source and detector for every single photon. Recently the distance recorded for QKD in fiber is only 412 km [76], and for that matter, a protocol was proposed to lengthen the distance to 500 km [77]. A proper solution for this challenge is to place a quantum repeater [78] that prove the proposed solution is able to expand up to 500 km. Even though the limitation of the application experiences limitations both in terms of performance and quantum memory [78,79], one of the temporary substitutions of the quantum repeater is the trustful relay scheme using the current technology along with proper protection on all related nodes [80]. Moreover, the satellite-based quantum communication recorded significantly less chancel loss and negligible decoherence in space and providing great achievable progress lately which makes it the promising solution [81–83]. Nowadays, enhancing the communication rate is the priority research area to prove the efficiency of QKD technology [84].

3.1.5. Number of Nodes

The fifth challenge is based on the number of end nodes in the network. Typically, the smart grid consists of different types of nodes with a massive number of nodes that have different capabilities. To control all nodes in the distributed network, the smart grid provides many sensors, energy and data storage, actuator, processors, transformer substations and renewable energy generators. Moreover, any network consumer is installed with a smart meter. Consequently, QKD is designed to function only in point-to-point pair communication nodes. The main challenge for QKD relies on allocating the secure key to many nodes where the nodes have different capabilities, and they are not all connected through fiber optic directly. The solution is to have a separate quantum channel for each control device. However, this solution is considerably expensive.

3.1.6. Real-Time Communication

The sixth challenge is associated with real-time communication. A system similar to a smart grid that supports a myriad number of applications such as load shedding applications and dynamic pricing applications, demands a fast response application. Several of those applications that provide a substantial protection mechanism would deny any communication delay if it exceeded 4 ms [85]. In cases such as in Unmanned Aerial Vehicle (UAV) application, traditional networks' communication latency and dependability are unsuitable for UAVs deployed in warfare operations. In those kinds of scenarios, the system cannot tolerate even a 1 ms delay or system downtime, which results in big catastrophe for both persons and property. The challenge relies on the QKD protocols features that support real-time communication. The QKD protocols approximately take hundred milliseconds to distribute the secure key which depends on the length of that key.

3.1.7. Big Data Handling

The seventh challenge is regarding the capability of handling a big amount of data. Several smart grid tools generate a flow of data stream based on the sampling period and it requires the accuracy of data. One of these tools is the synchronous phase measurement unit's tool. Mostly, the data stream records a few Mb/s. Consider the capacity of optical fiber that can transmit terabits per second or the capacity of 5G network that able to handle gigabit per second. QKD protocol encounters a challenge in supporting and coping with the requirements of data rate in each application where the secret key must be shorter than the data rate if it used with the OTP symmetric cryptographic algorithm. However, QKD can only produce a secret key at a rate of 1 Mb/s on 50 km. and it is rare for QKD implementation to generate a secret key at 10 kb/s over 100 km. In cases such as in UAV domain, due to the continuous data collection procedure, the data collected from UAV sensors is huge in volume. As a result, if there are insufficient resources to

managing the data, it will create a problem when the data processing and data handling occur simultaneously.

4. Quantum Key Distribution Categories

The fundamental of QKD is to use the non-cloning of the non-orthogonal single quantum state to accomplish the key distribution. Due to the usage of Heisenberg's uncertainty principle in the prepare-and-measure protocol, the measurement of the system's quantum state is hardly attainable without interrupting the quantum state. As discussed in the no-cloning principle [86], the possibilities to amplified or copy the qubit without disturbing them are impossible. Consequently, the QKD system can identify the adversaries by measuring the error parameter when transmitting the photons.

Figure 2 shows the classification of QKD protocol that can be divided into three categories based on their physical characteristics.

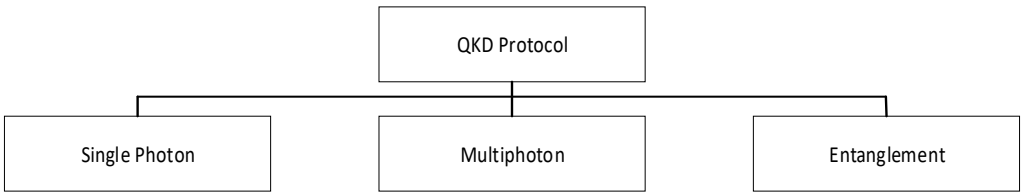

Figure 2. Categories of QKD Protocols.

4.1. QKD Based on Single Photon

Hilbert space is used in evaluating the criteria for classification for this category of protocols. For this category, quantum states are used to code the finite-dimensional of the entire QKD process. To distinguish the states, the information polarization direction that contains the photon or the phase of the photon is utilized. For example, BB84 is the most basic single photon protocol in this category. However, this protocol integrates Distributed Phase Reference (DPR) convention that is equal with the conventional correspondence protocols.

For this category, to convey the information, these protocols use different states of a single photon. Consequently, other various states are used for the coding and encoding of the key distribution process. Some of the protocols categorized in this QKD protocols class are as follows:

- BB84 protocol is proposed in 1984 by C.H. Bennett and G. Brassard [3]. BB84 is a QKD scheme that used quantum mechanics such as Heisenberg's uncertainty principle to share the secret key between sender and receiver. Furthermore, it is also the first QKD scheme that described the usage of photon polarization state in transmitting the secret key using a quantum communication channel. BB84 is considered as PM QKD protocol and used a single photon in transmitting and distributing the secret key's random bits. In BB84, the photon is polarized using either of the four polarization states, which is called rectilinear basis and choosing either of the two conjugate bases, which is called vertical polarization and horizontal polarization. The same principle applies to the diagonal basis polarization states and their conjugate bases, which are called diagonal polarization and anti-diagonal polarization. The polarization bases are shown in Figure 3. For the implementation of the BB84 protocol, there are four steps involved which is Quantum Exchange, Key Sifting, Information Reconciliation, and Privacy Amplification. BB84 is theoretically proven in providing complete security, as the author discussed in [87,88].
- B92 protocol is proposed in 1992 by C.H. Bennet [89]. This protocol is considered a prepare-and-measure-based QKD protocol. The B92 protocol is regarded as a simple protocol compares to the BB84 protocol, where the protocol can only choose either from two polarization states. In contrast, the BB84 protocol can choose either from four polarization states. For the B92 protocol, 0 degrees of the rectilinear basis is considered as bit 0, while 45 degrees of the diagonal basis is regarded as bit 1. Note

that, single non-orthogonal basis could be utilized to encode and decode the QKD protocol while not affecting the eavesdropper detection capabilities. Furthermore, the difference between BB84 and B92 protocol is that the B92 protocol will not obtain the measurement if the receiver chooses the wrong basis. The circumstances are called an erasure in quantum mechanics [90].

- Six-State Protocol (SSP) is proposed in 1998 by D. Bru [91]. This protocol is classified as a prepare-and-measure-based QKD protocol. The SSP protocol uses three measurement bases and six polarization states. This protocol can be assumed as advanced BB84 with additional measurement bases. The BB84 protocol utilizes four spin and half polarization states in the Poincare sphere that identical with $\pm$x and $\pm$y direction. Although the polarization state contains two additional states that correspond to $\pm$z, which makes it becoming six states, they are considered $\pm$x, $\pm$y, and $\pm$z in the Poincare sphere. The advantages of this protocol are that it has higher symmetrical compared to the BB84 protocol.
- SARG04 protocol is proposed in 2004 by V. Scarani et al. [92]. In terms of photon source, this protocol is developed by utilizing attenuated laser pulse rather than a single-photon source. This protocol is categorized as a prepare-and-measure-based QKD protocol. The similarity between SARG04 and BB84 is that it has an indistinguishable first phase scheme of the protocol. However, the second phase is different where Alice will apply either one of two non-orthogonal states when encoding the qubit instead of directly announcing her bases. The accuracy of the actual state and whether Bob will acquire the bit depends on him using the appropriate basis for the measurement. The length for the remaining key after the sifting stage in the no errors measurement is 0.25 from the raw key transmitted.

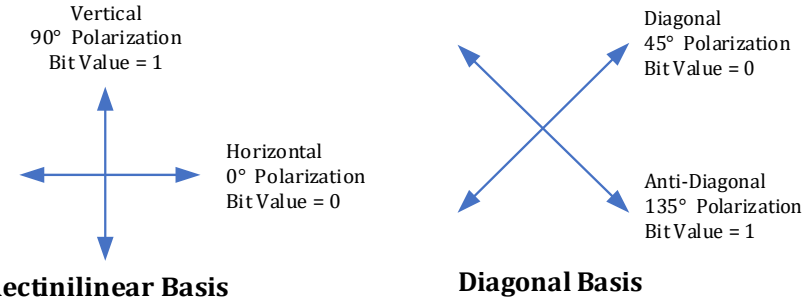

Figure 3. Classification of QKD Protocols.

4.2. QKD Based on Entanglement

Entanglement is an area of quantum physics that can be described as the correlation among particles that can't be separated despite their physical separation. When the state of one qubit is affected by the measurement of the other qubit, two qubits are said to be entangled. The disruption to the entangled qubits may cause them to lose their correlation. There are various states of entanglement, such as Greenberger-Home-Zeilinger (GHZ), Einstein-Podolsky-Rosen (EPR) and Bell state. The measurement is critical in quantum entanglement to determine whether the state is entangled or separable. There are two kinds of entanglement states: qubits spinning in the same direction and qubits spinning in different directions [93].

In quantum cryptography, especially in QKD, entanglement has widely been applied. The entangled state is applied to identify the existence of an eavesdropper and establish a secure key. The first QKD protocol using entangled state was proposed by Ekert in 1991 [94]. In entangled state QKD, the photon pairs entangled in the polarization degree of freedom are shared between Alice and Bob. One of the photons is transmitted to Alice whereas the other photon is transmitted to Bob. When they received the photons, the measurement will be conducted. After then, the entangled state is used to create a secure key and discover the existence of an eavesdropper. The states that have different results during

measurement will be eliminated. Next, Error Correction (EC) and Privacy Amplification (PA) will be conducted in the same procedure as BB84. In [95], EPR-QC is introduced where an entangled state in an EPR channel is used to perform an authentication procedure while the quantum channel transfers the shared key in QKD protocols. The process of authentication and key sharing is performed simultaneously to provide a sustainable flow of data. Semi-QKD was proposed in [96] where Charlie, as the third party prepares Green-Horne-Zeilinger (GHZ) states, divides them into a sequence and inserts decoy states into the sequence. Then, the quantum Alice requests the sequence of GHZ states and shares it with classical Bob. The security of Semi-QKD is preserved because Charlie cannot obtain the value of two particles by only knowing the value of one particle. However, the practical implementation of QKD should not rely on a third party. Therefore, Multi-party Bell state QKD [97] is introduced based on bi-directional communication. As a result, information leakage has been eliminated accordingly.

However, despite the benefits of entangled state QKD, the difficulty of efficiently creating, transmitting, and storing the entangled state make it impossible to implement in today's communication system. Furthermore, a research study conducted by [98] discovered that quantum cryptography based on entanglement is technically more cost than a single qubit. Due to the noise and error act independently in each qubit, the expensive quantum resource might be reduced using the single-qubit approach. In addition, entanglement suffers from photon source issues. Eve will try to split the copy of entangled states in case the photon laser source accidentally emits multiple simultaneous pairs of photons [99]. Consequently, Eve might be capable to measure the photons and obtain secret information.

The type of protocol in this category is a protocol that utilized the entanglement of photons for encryption and decryption instead of using the state of the photon. Some of the protocols that categorized as this type of QKD protocols class are as follows:

- E91 protocol is proposed in 1991 by Artur Ekert [94]. This QKD protocol is categorized as an entanglement-based protocol. E91 is developed by applying entangled photon pairs in the protocol. Since the protocol is using the principle of entanglement photon, the source of the photons can come from either Alice or Bob. The key point of using entanglement photons as the source for QKD is that the source can be untrusted. Which means, the security of QKD can be guaranteed even if the source is provided or controlled by opponents. Both Alice and Bob will acquire a particle from pair of entangled photons released by the entanglement photon source. The similarity of the E91 protocol and BB84 protocol is in the procedure of choosing the random basis for measuring purposes and reviewed it in the classical channel. Based on the principle of quantum, Alice and Bob will receive an opposite or identical result depend on the specific state of entanglement. Moreover, in the E91 protocol, detection of an eavesdropper can be performed using Bell's Inequality experiment.
- BBM92 protocol is proposed in 1992 by C.H. Bennett et al. shortly after the E91 protocol is proposed by Ekert [100]. This QKD protocol is also categorized as entanglement-based protocol. The similarity between BBM92 protocol and BB84 protocol is privacy amplification, key sifting, and raw key exchange procedure.

Some other DV Protocols

The proposed protocol can be divided into two categories: One-way protocols and Two-way protocols. Some of the proposed protocols that fall into the category are as follows:

One-way protocol:

- Differential Phase Shift (DPS) protocol is proposed in 2002 by Kyo Inoue et al. [101]. This protocol is categorized as an entanglement-based protocol. The principle of quantum entanglement is used in designing this protocol. The advantages of this protocol compare to other protocol is due to its simplicity of the configuration, efficient domain time usage, and the robustness against an attack such as photon number splitting (PNS) [102].

- Round-Robin Differential Phase Shift (RRDPS) protocol is proposed in 2014 by T. Sasaki et al. [103]. This protocol is attracting the researchers because of the protocol security characteristics; for example, the information leakage can be confined within the boundary without the knowledge of key bit error rate. However, there are still major doubts about the practicality of the implementation due to the difficulty in terms of the measurement device. Furthermore, from the theoretical aspect of security, the view on the optical attack remains unclear.
- The Coherent One-Way (COW) protocol is proposed in 2005 by D. Stucki et al. [104]. This protocol was developed by utilizing the principle of photon entanglement. This protocol is categorized as entanglement-based QKD protocol. Furthermore, this protocol has advantages where the protocol is robust against photon number splitting (PNS) attack, resistant to low interference visibility, and efficient with distilled secret bits per qubit. In this protocol, the time function is used to encode the information.
- S13 protocol is proposed by Eduin H. Serna [105]. The similarity of the S13 protocol and BB84 protocol is in terms of the mechanism of quantum. The only difference between each protocol is the usage of private reconciliation using asymmetric cryptography and random seed.

Two-way protocol:

- Ping-Pong QKD protocol [106] works by Bob, making sure that the Bell state is in specific pair of photons entangled inside freedom polarization degree where Bob will transmit one photon, which is supposed to be lossless and noiseless, to Alice by using the quantum channel. Next, Alice will perform the encoding of the travelling qubit and return the qubit to Bob. Bob received the qubit again from Alice. The remaining qubit that he will be accepted is either one of two encoded Bell states correlating with bit 0 or 1. Bob will differentiate using Bell measurement. In the default ping pong protocol, the security demands the control mode and the message mode to be rotated, in which the qubit is measured by Alice to check for error but will not return it. The ideal case for the Ping-Pong protocol is that Eve can only obtain the onward qubit and restore the photon to a maximum mixed state [107].
- LM05 protocol [108] is similar to BB84 protocol using four states obtained through two common unbiased bases. The protocol works by Bob forwarding the state to Alice, where Alice will then encode the state by utilizing unitary transformation. Next, Alice will send the encoded qubit to Bob, where the sharp measurement will be produced. A control mode is randomly executed to ensure security where the measurement of the received qubit will be performed. Then the comparison of the results will be conducted through a public channel. Nevertheless, quadratic scale losses occurred for the two-way channel of the protocol [109].

In QKD protocols, the aspect of distance must also be taken into considerations. Most current protocols do not provide a long-distance communication channel. According to Chen et al., the current distance record that the QKD protocol can cover is around 509 km [66].

4.3. QKD Based on Multiphoton

The enhanced approach where multiple photons are emitted from laser pulse or using a larger average number of photons is known as multiphoton approach [110]. The vulnerabilities in single-photon such as BB84 and protocol that derived from BB84 towards PNS attacks is significantly high since the difficulties for the photonic devices to periodically generating single photon at regular intervals due to a limited number of photons in the time slots [111]. A device that can produce single photons with periodicity on a consistent basis is technically difficult to be created. Multiphoton is claimed to be able to support long-distance photon and a higher rate of transmission compared to single-photon. In the multiphoton approach, information exchange is not limited to the single-photon source in a time slot, which means it allows transmitting the same quantum state more than once. The transmission of encoded bit between sender and receiver needs coherent non-decoying

quantum states with a mean number of photons greater than one [112,113]. Even though the laser pulse generates multiple photons, any unitary transformation and their complex conjugate transformation will have similar photons as long as all the photons are in the same phase [114]. Multiple photons can be delivered simultaneously to represent one bit of information to increase the transmission success rate.

The multiphoton approach is an enhanced version of a single photon with the benefits of high transmission rates and long photon travelling distance. In contrast, a single photon and entangled state are unable to do so [115]. In the multiphoton approach, information exchange is not limited to a single photon source in a time slot, allowing the same quantum state to be transmitted multiple times. Multiple photons could be transferred at the same time to represent one bit of information, increasing the transmission's success rate. To transfer the encoded bit from Alice to Bob, coherent non-decoying quantum states with a mean number of photons greater than one have been used [112,113]. Quantum communication using multiphoton approach are illustrated in Figure 4 where in the situation of Alice wants to transmit a photon, bit 1 will be encoded with 90° or bit 0 will be encoded with 0°, three photons were transferred, indicating of 90°, 90°, 90° or 0°, 0°, 0° denoting as one bit of information [116]. In this approach, if an error happens in one of the three photons, the original photon can be easily recovered. As a result, the beam-splitting attack does not affect the multiphoton approach.

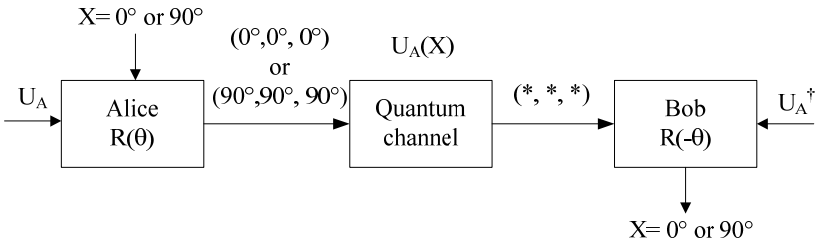

Figure 4. Quantum Communication using the multiphoton approach.

The multiphoton approach utilizes the arbitrary state of polarization using a rotation operator, which can secure the information from the MITM attack. The polarization of rotation operator [117] adopted in Figure 4 can be described as:

$$R(\theta) = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \quad (1)$$

where θ is the rotation angle. The secret unitary operation will be applied by Alice and Bob using U_A and U_B where $U_A U_B = U_B U_A$. The values of the rotation operator are $U_A = R(\theta)$ and $U_B = R(\Phi)$, where $R(\theta) = R(\Phi)$.

Despite the advantages of multiphoton in terms of multiple photon emission, Eve can easily syphon off multiphoton if only one stage is used. Therefore, it needs to be operated with the multi-stage transformation between sender and receiver. In theory, the Eve's capability to estimate the state of polarization might be improved as the numbers of photons in a beam increased. Therefore, the photon numbers and the stages must be carefully identified to make the protocols well utilized during their operations.

The Multiphoton QKD based on double-lock encryption has been introduced to overcome the weaknesses of a single photon and its variants [118]. The random secret key needs to be travel in a multi-stages step to make the transmission channel more secure and making the eavesdropper difficult to guess the state of the qubits. Same as BB84, the procedure of Error Concealment and Privacy Amplification is subsequently performed to minimize the knowledge of Eve towards the information. This protocol has significant benefits in increasing the distance's limit and provides higher SKR than the existing single-photon QKD. However, although any QKD protocols provide unconditional security, they still need an authentication procedure before the communication due to the key needs to be distributed to the right communication parties [119,120]. Therefore, implementing an

effective authentication procedure using a secure shared authentication key for multiphoton has been introduced to overcome the issue as mentioned earlier [121].

The advantages of the multiphoton approach are that it can solve the intricated heterodyne and homodyne detection and noise-sensitive problem. Thus, a detector with less efficiency is more appropriate when using multiphoton protocol. Furthermore, multiphoton implementation using multiple stages is designed to solve the security problem such as man-in-the-middle attack, photon splitting number attack, and Trojan Horse attack that occurred in the single-photon protocol. Currently, there is no involvement of the public channel in the multiphoton protocol as the exchanging keys process, and the entire procedure is performed only through a quantum channel.

The multiphoton protocol is initially designed for Quantum Secure Direct Communication (QSDC), where the protocol eliminates the key distribution process and directly shares the message using quantum channel [122,123]. Recently, the researchers have hotly discussed the works on improving QSDC. The quantum-memory-free version of the efficient-QSDC protocol is based on original work [123] was proposed by Hanzo and his collaborators [124]. As a result, the protocol is robust to individual attacks and produces high communication efficiency. Meanwhile, QSDC can be made into measurement-device-independent to create high communication distance [125]. QSDC can also be implemented with single-photon measurement to increase the secrecy of the protocol [126]. Furthermore, the two-step transmission can be further simplified by using hyperentanglement in one round. As a result, this protocol can improve transmission efficiency compared to standard quantum communication [127]. Furthermore, the concept of multiphoton QKD is to perform a key exchanging process by utilizing the polarization rotational in the multi-stages protocol [118,128].

Furthermore, multiphoton QKD is easily implemented in the administered network infrastructure. Multiphoton QKD are also not required to produce the same polarization states as in the BB84 protocol due to the generation of an arbitrary polarization state that can avoid the man-in-the-middle attack. Despite multiphoton successes, determining the number of stages and the optimal mean photon numbers to ensure that the protocols function correctly during operations remain critical concerns. Therefore, the works on enhanced multiphoton have been resolved the issue of increasing source redundancy [129], improved the authentication procedures [121] and improved the achievable secret key rate as well as distance coverage [130]. With the emergence of quantum technology, the chip-based QKD is introduced [131]. Chip-based technology can offer small size and low energy consumption for a low cost. Table 2 shows the QKD protocol based on Heisenberg's Uncertainty Principles.

Table 2. QKD Protocol based on Heisenberg's Uncertainty Principles.

Year	Name of Protocol	Citation
1984	BB84	[132–134]
1991	E91	[135,136]
1992	BBM92	[137–139]
1992	B92	[140–142]
1999	SSP	[143]
2002	GG02	[144,145]
2002	Ping-Pong	[146]
2003	DPS	[147–149]
2004	COW	[150]
2004	SARG04	[151–153]
2004	Coherent State Heterodyne	[154,155]
2005	LM05	[156,157]
2013	S13	[105]
2014	RRDPS	[158]
2015	Multiphoton	[159,160]

5. Conclusions and Future Works

As for the future directions, quantum security can be the solution that connects cryptography and network security areas. The existing signature schemes and public-key encryption could not guarantee secure connection once the adversaries are equipped with quantum level powers. The existing signature schemes and public-key encryption cannot provide a secure communication channel once the adversaries are equipped with quantum level powers. Without limiting any abilities of eavesdroppers, quantum cryptography security could be proven mathematically. Quantum cryptography techniques will generate and distribute longer symmetric keys, ensuring the security of many IoT devices over time. This approach will also reduce the network overhead and extend the device battery life by lowering the handshake frequency in the key establishment process. Moreover, quantum security can also be utilized in device authentication, power-efficient algorithms, certification, qualification, securing identity, and applying policies. Furthermore, MEC capabilities are used to implement the key management entities at the network edge and reduce the communication overhead related to security in the 5G backhaul network. This technique can also be used in other crucial areas such as smart grid, smart city, and IoT applications. For example, authors in [161] introduced integration software that combine IoT communication protocol to increase the security and resiliency of electricity grids. The proposed framework reduced overhead and allows 5G and IoT to be integrated.

Quantum cryptography has garnered a lot of attention from different organizations both industrial and academic communities. Over the last few years, significant progress in the quantum cryptography and development of optical equipment is shown by numerous successful research studies and testing of QKD technology. This research and testing produce significant results in quantum cryptography and underline the future works that need to be addressed and resolved.

This paper reviews and discusses the existing quantum cryptography protocol that has been identified in the literature to be implemented in the 5G networks. Trusted repeaters are required to extend the distance of secure transmission for quantum channels. Currently, the hot topic in optical research is to integrate the QKD networks into conventional telecommunication networks. The future works or the next breakthrough will be on employing quantum cryptography into the real-world information transfer applications. Since 5G is at the core of the future's heterogeneous network, QKD can also be implemented in the backbone network for a secure connection. Implementing QKD in the 5G backbone network will be the focus of our future works. Currently, the maximum key rate is correlated with the distance of the QKD links. One of the limitations of QKD links is length constraints. However, the development in optical equipment has significantly improved as discussed in this paper. In 2003, the DARPA QKD network achieved a key rate of 1 kbps. In 2007, the key rate in SECOQC or European QKD network are increased to 3 kbps and followed by the Tokyo QKD network in 2011 where the key rate is 300 kbps. This achieved key rate is adequate to initiate a secure video conferencing along with OTP cipher established by QKD. In terms of the correlating distance, the DARPA QKD networks have a connection distance of 29 km between Boston and Harvard Universities using the optical switch. For SECOQC network, the QKD link was between St. Pölten and BREIT for maximum distance of 82 km while for the Tokyo QKD network, the connection was between the Koganei-1 and Koganei-2 nodes with maximum distance of 90 km. Meanwhile, real-life application using QKD network that has been demonstrated in Hefei has the maximum distance of 85.1 km using the Hefei-Chaohu-Wuhu (HCW) intercity link.

Consequently, there is an expectation for a longer distance and a higher key rate in the upcoming years. Currently, QKD networks are merely accomplished using Trusted Repeater Approach (TRA), and it is expected that the optical quantum repeaters will ultimately be accessible for practical use. TRA is important in assisting routing for QKD networks and solving the distance limitations of QKD links. However, the are some restrictions that need to be resolved for a QKD network to be combined with conventional IP networks and used in everyday life. One method for extensive application of QKD

technology is by using an approach such as SDN-QKD to integrate QKD networks with telecommunication networks. Previous research [130] proved that the implementation of a new quantum technique for secret key transmission such as multiphoton approach in networks will improve the key transmission efficiency. Therefore, for future research, the implementation multiphoton approach during the interchanged of information are required to ensure that the key remains a secure between parties in the 5G networks.

Author Contributions: Authors contributed equally to this work . Conceptualization, M.H.A. and N.Z.H.; methodology, Z.A.Z.; validation, M.H.A., Z.A.Z. and N.Z.H.; formal analysis, M.H.A.; investigation, M.H.A. and N.Z.H.; writing—original draft preparation, M.H.A.; writing—review and editing, M.H.A. and N.Z.H.; visualization, N.Z.H.; supervision, Z.A.Z.; project administration, Z.A.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding. This research is self-funded by the authors since it is part of the requirement in University Putra Malaysia for postgraduate students.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: We thank the anonymous reviewers for their valuable comments and suggestions, which helped us to improve the content, organization, and presentation of this paper.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

3GPP	3th Generation Partnership Project
5G	5th Generation Network
ABE	Attribute-based Encryption
AMF	Access and Mobility Management Function
AUSF	Authentication Server Function
CE	Channel Estimation
C-RAN	Cloud Radio Access Network
CSP	Cloud Service Provider
D2D	Device-to-Device
DoS/DDoS	Denial of Service
DPR	Distributed Phase Reference
EAP	Extensible Authentication Protocol
ECC	Elliptic Curve Cryptography
HIPPA	Health Insurance Portability and Accountability Act
HMAC	Hash-based Message Authentication Code
IBC	Identity-based Cryptography
ICC	Inter-Controller Communication
IIoT	Industrial Internet of Things
IMSI	International Mobile Subscriber Identity
INS	Industrial Network System
ISP	Internet Service Provider
LTE	Long-Term Evolution
LPWAN	Low-Power Wide-Area Network
MANET	Mobile Ad-Hoc Network
MEC	Multi-Access Edge Computing
MISO	Multiple-Input Single-Output
MIMO	Multiple-Input Multiple-Output

NFV	Network Function Virtualization
NOMA	Non-Orthogonal Multiple Access
ODFMA	Orthogonal Frequency Division Multiple Access
PbD	Privacy-by-Design
PKI	Public Key Infrastructure
PNS	Photon Number Splitting
QKD	Quantum Key Distribution
QRA	Quantum-Resistant Algorithm
QoS	Quality of Service
QSDC	Quantum Secure Direct Communication
RAN	Radio Access Network
RAT	Radio Access Technology
RBAC	Role-based Access Control
SDP	Software-Defined Privacy
SEAF	Security Anchor Function
SEBC	Shared Encryption-based Construction
SSL	Secure Socket Layer
SWIPT	Simultaneous Wireless Information and Power Transfer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UAV	Unmanned Aerial Vehicle
USIM	Universal Subscriber Identity Module

References

1. Agiwal, M.; Roy, A.; Saxena, N. Next Generation 5G Wireless Networks: A Comprehensive Survey. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 1617–1655. [CrossRef]
2. Ahmad, I.; Kumar, T.; Liyanage, M.; Okwuibe, J.; Ylianttila, M.; Gurtov, A. 5G security: Analysis of threats and solutions. In Proceedings of the 2017 IEEE Conference on Standards for Communications and Networking (CSCN), Helsinki, Finland, 18–21 September 2017; pp. 193–199. [CrossRef]
3. Bennett, C.H.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. In Proceedings of the International Conference on Computers, Systems & Signal Processing, Bangalore, India, 9–12 December 1984; pp. 175–179. [CrossRef]
4. Ferrag, M.A.; Maglaras, L.; Argyriou, A.; Kosmanos, D.; Janicke, H. Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes. *J. Netw. Comput. Appl.* **2018**, *101*, 55–82. [CrossRef]
5. Khan, R.; Kumar, P.; Jayakody, D.N.K.; Liyanage, M. A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements, and Future Directions. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 196–248. [CrossRef]
6. Kumari, K.A.; Sadasivam, G.S.; Gowri, S.S.; Akash, S.A.; Radhika, E.G. An Approach for End-to-End (E2E) Security of 5G Applications. In Proceedings of the 2018 IEEE 4th International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing, (HPSC) and IEEE International Conference on Intelligent Data and Security (IDS), Omaha, NE, USA, 3–5 May 2018; pp. 133–138. [CrossRef]
7. Mitchell, C.J. The impact of quantum computing on real-world security: A 5G case study. *Comput. Secur.* **2020**, *93*, 101825. [CrossRef]
8. Mitra, R.N.; Agrawal, D.P. 5G mobile technology: A survey. *ICT Express* **2015**, *1*, 132–137. [CrossRef]
9. Zavitsanos, D.; Ntanos, A.; Giannoulis, G.; Avramopoulos, H. On the QKD Integration in Converged Fiber/Wireless Topologies for Secured, Low-Latency 5G/B5G Fronthaul. *Appl. Sci.* **2020**, *10*, 5193. [CrossRef]
10. Shang, T.; Tang, Y.; Chen, R.; Liu, J. Full quantum one-way function for quantum cryptography. *Quantum Eng.* **2020**, *2*, e32. [CrossRef]
11. Trinh, P.V.; Pham, A.T.; Carrasco-Casado, A.; Toyoshima, M. Quantum Key Distribution over FSO: Current Development and Future Perspectives. In Proceedings of the 2018 Progress in Electromagnetics Research Symposium (PIERS-Toyama), Toyama, Japan, 1–4 August 2018; pp. 1672–1679. [CrossRef]
12. Hasnat, M.A.; Rumee, S.T.A.; Razzaque, M.A.; Mamun-Or-Rashid, M. Security Study of 5G Heterogeneous Network: Current Solutions, Limitations & Future Direction. In Proceedings of the 2019 International Conference on Electrical, Computer and Communication Engineering (ECCE), Cox's Bazar, Bangladesh, 7–9 February 2019; pp. 1–4. [CrossRef]
13. Badoi, C.-I.; Prasad, N.; Prasad, R. Virtualization and Scheduling Methods for 5G Cognitive Radio Based Wireless Networks. *Wirel. Pers. Commun.* **2016**, *89*, 599–619. [CrossRef]
14. Li, S.; Da Xu, L.; Zhao, S. 5G Internet of Things: A survey. *J. Ind. Inf. Integr.* **2018**, *10*, 1–9. [CrossRef]
15. Chen, M.; Qian, Y.; Mao, S.; Tang, W.; Yang, X. Software-Defined Mobile Networks Security. *Mob. Net. Appl.* **2016**, *21*, 729–743. [CrossRef]

16. Taralika, A.; Challa, D.; Kumar, S.; Ojha, A.; Chung, L. Secure Authentication to Provide Mobile Access to Shared Network Resources. U.S. Patent 10,148,637, 4 December 2018. Available online: https://uspto.report/patent/grant/10,148,637 (accessed on 14 January 2022).
17. Liyanage, M.; Salo, J.; Braeken, A.; Kumar, T.; Seneviratne, S.; Ylianttila, M. 5G Privacy: Scenarios and Solutions. In Proceedings of the 2018 IEEE 5G World Forum (5GWF), Santa Clara, CA, USA, 9–11 July 2018; pp. 197–203. [CrossRef]
18. Aaronson, S. Data is different, and that's why the world needs a new approach to governing cross-border data flows. *Digit. Policy Regul. Gov.* **2019**, *5*, 441–460. [CrossRef]
19. Basin, D.; Dreier, J.; Hirschi, L.; Radomirovic, S.; Sasse, R.; Stettler, V. A formal analysis of 5G authentication. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, Toronto, ON, Canada, 15–19 October 2018; pp. 1383–1396. [CrossRef]
20. Cremers, C.; Dehnel-Wild, M. Component-based formal analysis of 5G-AKA: Channel assumptions and session confusion. In Proceedings of the Network and Distributed Systems Security (NDSS) Symposium, San Diego, CA, USA, 24–27 February 2019. [CrossRef]
21. Borgaonkar, R.; Hirschi, L.; Park, S.; Shaik, A. New privacy threat on 3G, 4G, and upcoming 5G AKA protocols. *Proc. Priv. Enhancing Technol.* **2019**, *2019*, 108–127. [CrossRef]
22. Behrad, S.; Bertin, E.; Crespi, N. Securing authentication for mobile networks, a survey on 4G issues and 5G answers. In Proceedings of the 2018 21st Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN), Paris, France, 19–22 February 2018; pp. 1–8. [CrossRef]
23. Arkko, J.; Norrman, K.; Näslund, M.; Sahlin, B. A USIM compatible 5G AKA protocol with perfect forward secrecy. In Proceedings of the 2015 IEEE Trustcom/BigDataSE/ISPA, Washington, DC, USA, 20–22 August 2015; Volume 1, pp. 1205–1209. [CrossRef]
24. Giustolisi, R.; Gerhmann, C. Threats to 5G group-based authentication. In Proceedings of the 13th International Conference on Security and Cryptography (SECRYPT 2016), Madrid, Spain, 26–28 July 2016; pp. 360–367. [CrossRef]
25. Koutsos, A. The 5G-AKA authentication protocol privacy. In Proceedings of the 2019 IEEE European Symposium on Security and Privacy (EuroS&P), Stockholm, Sweden, 17–19 June 2019; pp. 464–479. [CrossRef]
26. Braeken, A.; Liyanage, M.; Kumar, P.; Murphy, J. Novel 5G Authentication Protocol to Improve the Resistance against Active Attacks and Malicious Serving Networks. *IEEE Access* **2019**, *7*, 64040–64052. [CrossRef]
27. Ozhelvaci, A.; Ma, M. Secure and efficient vertical handover authentication for 5G HetNets. In Proceedings of the 2018 IEEE International Conference on Information Communication and Signal Processing (ICICSP), Singapore, 28–30 December 2018; pp. 27–32. [CrossRef]
28. Ma, T.; Hu, F. *A Cross-Layer Collaborative Handover Authentication Approach for 5G Heterogeneous Network*; IOP Publishing: Bristol, UK, 2019; Volume 1169, p. 12066. [CrossRef]
29. Baskaran, S.B.M.; Raja, G.; Bashir, A.K.; Murata, M. QoS-Aware Frequency-Based 4G+Relative Authentication Model for Next Generation LTE and Its Dependent Public Safety Networks. *IEEE Access* **2017**, *5*, 21977–21991. [CrossRef]
30. Wang, M.; Yan, Z. Privacy-Preserving Authentication and Key Agreement Protocols for D2D Group Communications. *IEEE Trans. Ind. Inform.* **2018**, *14*, 3637–3647. [CrossRef]
31. Shin, S.; Kwon, T. Two-Factor Authenticated Key Agreement Supporting Unlinkability in 5G-Integrated Wireless Sensor Networks. *IEEE Access* **2018**, *6*, 11229–11241. [CrossRef]
32. Wang, L.; Liu, J.; Chen, M.; Gui, G.; Sari, H. Optimization-Based Access Assignment Scheme for Physical-Layer Security in D2D Communications Underlaying a Cellular Network. *IEEE Trans. Veh. Technol.* **2018**, *67*, 5766–5777. [CrossRef]
33. Rahman, M.A.; Al-Shaer, E. Automated Synthesis of Distributed Network Access Controls: A Formal Framework with Refinement. *IEEE Trans. Parallel Distrib. Syst.* **2017**, *28*, 416–430. [CrossRef]
34. Khan, M.; Ginzboorg, P.; Järvinen, K.; Niemi, V. Defeating the downgrade attack on identity privacy in 5G. In Proceedings of the International Conference on Research in Security Standardisation, Darmstadt, Germany, 26–27 November 2018; pp. 95–119. [CrossRef]
35. He, D.; Chan, S.; Guizani, M. Accountable and Privacy-Enhanced Access Control in Wireless Sensor Networks. *IEEE Trans. Wirel. Commun.* **2015**, *14*, 389–398. [CrossRef]
36. Chatterjee, S.; Roy, S.; Das, A.K.; Chattopadhyay, S.; Kumar, N.; Reddy, A.G.; Park, K.; Park, Y. On the Design of Fine Grained Access Control With User Authentication Scheme for Telecare Medicine Information Systems. *IEEE Access* **2017**, *5*, 7012–7030. [CrossRef]
37. Jha, S.; Li, N.; Tripunitara, M.; Wang, Q.; Winsborough, W. Towards Formal Verification of Role-Based Access Control Policies. *IEEE Trans. Dependable Secur. Comput.* **2008**, *5*, 242–255. [CrossRef]
38. Huang, Q.; Yang, Y.; Wang, L. Secure Data Access Control With Ciphertext Update and Computation Outsourcing in Fog Computing for Internet of Things. *IEEE Access* **2017**, *5*, 12941–12950. [CrossRef]
39. Qinlong, H.; Zhaofeng, M.; Yixian, Y.; Xinxin, N.; Jingyi, F. Improving security and efciency for encrypted data sharing in online social networks. *China Commun.* **2014**, *11*, 104–117. [CrossRef]
40. Saxena, N.; Tsudik, G.; Yi, J.H. Efficient Node Admission and Certificateless Secure Communication in Short-Lived MANETs. *IEEE Trans. Parallel Distrib. Syst.* **2009**, *20*, 158–170. [CrossRef]
41. Castiglione, A.; De Santis, A.; Masucci, B.; Palmieri, F.; Castiglione, A.; Li, J.; Huang, X. Hierarchical and Shared Access Control. *IEEE Trans. Inf. Forensics Secur.* **2016**, *11*, 850–865. [CrossRef]

42. Jarecki, S.; Saxena, N. On the Insecurity of Proactive RSA in the URSA Mobile Ad Hoc Network Access Control Protocol. *IEEE Trans. Inf. Forensics Secur.* **2010**, *5*, 739–749. [CrossRef]
43. Wang, D.; Wang, Z.; Shen, B.; Alsaadi, F.E. Security-guaranteed filtering for discrete-time stochastic delayed systems with randomly occurring sensor saturations and deception attacks. *Int. J. Robust Nonlinear Control* **2017**, *27*, 1194–1208. [CrossRef]
44. You, J.; Zhong, Z.; Wang, G.; Ai, B. Security and Reliability Performance Analysis for Cloud Radio Access Networks with Channel Estimation Errors. *IEEE Access* **2014**, *2*, 1348–1358. [CrossRef]
45. Cheminod, M.; Durante, L.; Seno, L.; Valenzano, A. Semiautomated Verification of Access Control Implementation in Industrial Networked Systems. *IEEE Trans. Ind. Inform.* **2015**, *11*, 1388–1399. [CrossRef]
46. Siriwardhana, Y.; Porambage, P.; Liyanage, M.; Walia, J.S.; Matinmikko-Blue, M.; Ylianttila, M. Micro-Operator driven Local 5G Network Architecture for Industrial Internet. In Proceedings of the 2019 IEEE Wireless Communications and Networking Conference (WCNC), Marrakesh, Morocco, 15–18 April 2019; pp. 1–8. [CrossRef]
47. Prasad, A.; Li, Z.; Holtmanns, S.; Uusitalo, M.A. 5G micro-operator networks—A key enabler for new verticals and markets. In Proceedings of the 2017 25th Telecommunication Forum (TELFOR), Belgrade, Serbia, 21–22 September 2017; pp. 1–4. [CrossRef]
48. Ahokangas, P.; Moqaddamerad, S.; Matinmikko, M.; Abouzeid, A.; Atkova, I.; Gomes, J.F.; Iivari, M. Future micro operators business models in 5G. *Bus. Manag. Rev.* **2016**, *7*, 143. [CrossRef]
49. Sriram, P.P.; Wang, H.-C.; Jami, H.G.; Srinivasan, K. 5G security: Concepts and challenges. In *5G Enabled Secure Wireless Networks*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 1–43. [CrossRef]
50. Yao, J.; Han, Z.; Sohail, M.; Wang, L. A robust security architecture for SDN-based 5G networks. *Futur. Internet* **2019**, *11*, 85. [CrossRef]
51. Liyanage, M.; Abro, A.B.; Ylianttila, M.; Gurtov, A. Opportunities and Challenges of Software-Defined Mobile Networks in Network Security. *IEEE Secur. Priv.* **2016**, *14*, 34–44. [CrossRef]
52. Liyanage, M.; Braeken, A.; Jurcut, A.D.; Ylianttila, M.; Gurtov, A. Secure communication channel architecture for Software Defined Mobile Networks. *Comput. Netw.* **2017**, *114*, 32–50. [CrossRef]
53. Mämmelä, O.; Hiltunen, J.; Suomalainen, J.; Ahola, K.; Mannersalo, P.; Vehkaperä, J. Towards micro-segmentation in 5G network security. In Proceedings of the European Conference on Networks and Communications (EuCNC 2016) Workshop on Network Management, Quality of Service and Security for 5G Networks, Athens, Greece, 27–30 June 2016.
54. Dacier, M.C.; König, H.; Cwalinski, R.; Kargl, F.; Dietrich, S. Security Challenges and Opportunities of Software-Defined Networking. *IEEE Secur. Priv.* **2017**, *15*, 96–100. [CrossRef]
55. Yan, Z.; Zhang, P.; Vasilakos, A. V A security and trust framework for virtualized networks and software-defined networking. *Secur. Commun. Netw.* **2016**, *9*, 3059–3069. [CrossRef]
56. Lam, J.-H.; Lee, S.-G.; Lee, H.-J.; Oktian, Y.E. Securing distributed SDN with IBC. In Proceedings of the 2015 Seventh International Conference on Ubiquitous and Future Networks, Sapporo, Japan, 7–10 July 2015; pp. 921–925. [CrossRef]
57. Pasquale, L.; Ghezzi, C.; Menghi, C.; Tsigkanos, C.; Nuseibeh, B. Topology aware adaptive security. In Proceedings of the Proceedings of the 9th International Symposium on Software Engineering for Adaptive and Self-Managing Systems, Madrid, Spain, 18–24 May 2014; pp. 43–48. [CrossRef]
58. Edemekong, P.F.; Annamaraju, P.; Haydel, M.J. Health Insurance Portability and Accountability Act. *SAGE Encycl. Educ. Res. Meas. Eval.* **2018**. [CrossRef]
59. Kemmer, F.; Reich, C.; Knahl, M.; Clarke, N. Software defined privacy. In Proceedings of the 2016 IEEE International Conference on Cloud Engineering Workshop (IC2EW), Berlin, Germany, 4–8 April 2016; pp. 25–29. [CrossRef]
60. Pereira, F.; Crocker, P.; Leithardt, V.R.Q. PADRES: Tool for PrivAcy, Data REgulation and Security. *SoftwareX* **2022**, *17*, 100895. [CrossRef]
61. Clancy, T.C.; McGwier, R.; Chen, L. Post-Quantum Cryptography and 5G Security: Tutorial. In Proceedings of the ACM WiSec, Miami, FL, USA, 14–17 May 2019. [CrossRef]
62. Gandotra, P.; Jha, R.K. A survey on green communication and security challenges in 5G wireless communication networks. *J. Netw. Comput. Appl.* **2017**, *96*, 39–61. [CrossRef]
63. Gupta, A.; Jha, R.K. A Survey of 5G Network: Architecture and Emerging Technologies. *IEEE Access* **2015**, *3*, 1206–1232. [CrossRef]
64. Trizna, A.; Ozols, A. An Overview of Quantum Key Distribution Protocols. *Inf. Technol. Manag. Sci.* **2018**, *21*, 37–44. [CrossRef]
65. Bell, J.S. On the Einstein Podolsky Rosen paradox. *Phys. Phys. Fiz.* **1964**, *1*, 195–200. [CrossRef]
66. Chen, J.P.; Zhang, C.; Liu, Y.; Jiang, C.; Zhang, W.; Hu, X.L.; Guan, J.Y.; Yu, Z.W.; Xu, H.; Lin, J.; et al. Sending-or-Not-Sending with Independent Lasers: Secure Twin-Field Quantum Key Distribution over 509 km. *Phys. Rev. Lett.* **2020**, *124*, 070501. [CrossRef] [PubMed]
67. Aaron Lopez-Leyva, J.; Talamantes-Alvarez, A.; Ponce-Camacho, M.A.; Garcia-Cardenas, E.; Alvarez-Guzman, E. *Free-Space-Optical Quantum Key Distribution Systems: Challenges and Trends*; IntechOpen: London, UK, 2019. [CrossRef]
68. Chen, W.; Han, Z.-F.; Zhang, T.; Wen, H.; Yin, Z.-Q.; Xu, F.-X.; Wu, Q.-L.; Liu, Y.; Zhang, Y.; Mo, X.-F. Field experiment on a "star type" metropolitan quantum key distribution network. *IEEE Photonics Technol. Lett.* **2009**, *21*, 575–577. [CrossRef]
69. Wang, S.; Chen, W.; Yin, Z.-Q.; Zhang, Y.; Zhang, T.; Li, H.-W.; Xu, F.-X.; Zhou, Z.; Yang, Y.; Huang, D.-J. Field test of wavelength-saving quantum key distribution network. *Opt. Lett.* **2010**, *35*, 2454–2456. [CrossRef]
70. Townsend, P.D. Simultaneous quantum cryptographic key distribution and conventional data transmission over installed fibre using wavelength-division multiplexing. *Electron. Lett.* **1997**, *33*, 188–190. [CrossRef]

71. Chapuran, T.E.; Toliver, P.; Peters, N.A.; Jackel, J.; Goodman, M.S.; Runser, R.J.; McNown, S.R.; Dallmann, N.; Hughes, R.J.; McCabe, K.P. Optical networking for quantum key distribution and quantum communications. *New J. Phys.* **2009**, *11*, 105001. [CrossRef]
72. Choi, I.; Young, R.J.; Townsend, P.D. Quantum key distribution on a 10Gb/s WDM-PON. *Opt. Express* **2010**, *18*, 9600–9612. [CrossRef]
73. Eraerds, P.; Walenta, N.; Legr , M.; Gisin, N.; Zbinden, H. Quantum key distribution and 1 Gbps data encryption over a single fibre. *New J. Phys.* **2010**, *12*, 63027. [CrossRef]
74. Patel, K.A.; Dynes, J.F.; Choi, I.; Sharpe, A.W.; Dixon, A.R.; Yuan, Z.L.; Penty, R.V.; Shields, A.J. Coexistence of high-bitrate quantum key distribution and data on optical fiber. *Phys. Rev. X* **2012**, *2*, 41010. [CrossRef]
75. Mao, Y.; Wang, B.-X.; Zhao, C.; Wang, G.; Wang, R.; Wang, H.; Zhou, F.; Nie, J.; Chen, Q.; Zhao, Y. Integrating quantum key distribution with classical communications in backbone fiber network. *Opt. Express* **2018**, *26*, 6010–6020. [CrossRef]
76. Boaron, A.; Boso, G.; Rusca, D.; Vulliez, C.; Autebert, C.; Caloz, M.; Perrenoud, M.; Gras, G.; Bussières, F.; Li, M.-J. Secure quantum key distribution over 421 km of optical fiber. *Phys. Rev. Lett.* **2018**, *121*, 190502. [CrossRef] [PubMed]
77. Lucamarini, M.; Yuan, Z.L.; Dynes, J.F.; Shields, A.J. Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. *Nature* **2018**, *557*, 400–403. [CrossRef] [PubMed]
78. Sangouard, N.; Simon, C.; De Riedmatten, H.; Gisin, N. Quantum repeaters based on atomic ensembles and linear optics. *Rev. Mod. Phys.* **2011**, *83*, 33. [CrossRef]
79. Yang, S.-J.; Wang, X.-J.; Bao, X.-H.; Pan, J.-W. An efficient quantum light–matter interface with sub-second lifetime. *Nat. Photonics* **2016**, *10*, 381–384. [CrossRef]
80. Qiu, J. Quantum communications leap out of the lab. *Nature* **2014**, *508*, 441–442. [CrossRef] [PubMed]
81. Liao, S.-K.; Cai, W.-Q.; Liu, W.-Y.; Zhang, L.; Li, Y.; Ren, J.-G.; Yin, J.; Shen, Q.; Cao, Y.; Li, Z.-P.; et al. Satellite-to-ground quantum key distribution. *Nature* **2017**, *549*, 43–47. [CrossRef]
82. Ren, J.-G.; Xu, P.; Yong, H.-L.; Zhang, L.; Liao, S.-K.; Yin, J.; Liu, W.-Y.; Cai, W.-Q.; Yang, M.; Li, L.; et al. Ground-to-satellite quantum teleportation. *Nature* **2017**, *549*, 70–73. [CrossRef]
83. Yin, J.; Cao, Y.; Li, Y.-H.; Liao, S.-K.; Zhang, L.; Ren, J.-G.; Cai, W.-Q.; Liu, W.-Y.; Li, B.; Dai, H. Satellite-based entanglement distribution over 1200 kilometers. *Science* **2017**, *356*, 1140–1144. [CrossRef]
84. Diamanti, E.; Lo, H.-K.; Qi, B.; Yuan, Z. Practical challenges in quantum key distribution. *npj Quantum Inf.* **2016**, *2*, 16025. [CrossRef]
85. Fuloria, S.; Anderson, R.; McGrath, K.; Hansen, K.; Alvarez, F. The protection of substation communications. In Proceedings of the SCADA Security Scientific Symposium, Miami, FL, USA, 19–21 January 2010; pp. 1–13.
86. Wootters, W.K.; Zurek, W.H. A single quantum cannot be cloned. *Nature* **1982**, *299*, 802–803. [CrossRef]
87. Singh, S. *The Code Book: The Secret History of Codes and Codebreaking*; Fourth Estate: London, UK, 1999; Volume 366, ISBN 1857028899.
88. Shor, P.W.; Preskill, J. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.* **2000**, *85*, 441. [CrossRef] [PubMed]
89. Bennett, C.H. Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.* **1992**, *68*, 3121. [CrossRef] [PubMed]
90. Bruss, D.; Erdélyi, G.; Meyer, T.; Riege, T.; Rothe, J. Quantum cryptography: A survey. *ACM Comput. Surv.* **2007**, *39*, 6-es. [CrossRef]
91. Bruß, D. Optimal eavesdropping in quantum cryptography with six states. *Phys. Rev. Lett.* **1998**, *81*, 3018. [CrossRef]
92. Scarani, V.; Acin, A.; Ribordy, G.; Gisin, N. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Phys. Rev. Lett.* **2004**, *92*, 57901. [CrossRef]
93. Chen, C.; Zeng, G.; Lin, F.; Chou, Y.; Chao, H. Quantum cryptography and its applications over the internet. *IEEE Netw.* **2015**, *29*, 64–69. [CrossRef]
94. Ekert, A.K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **1991**, *67*, 661–663. [CrossRef]
95. Abushgra, A.A.; Elleithy, K.M. A Shared Secret Key Initiated by EPR Authentication and Qubit Transmission Channels. *IEEE Access* **2017**, *5*, 17753–17763. [CrossRef]
96. Zhu, K.-N.; Zhou, N.-R.; Wang, Y.-Q.; Wen, X.-J. Semi-Quantum Key Distribution Protocols with GHZ States. *Int. J. Theor. Phys.* **2018**, *57*, 3621–3631. [CrossRef]
97. Wang, J.-X.; Liu, N.; Wang, C.; Xu, J. Multi-party Quantum Key Distribution Protocol Without Information Leakage. *Int. J. Theor. Phys.* **2019**, *58*, 2654–2663. [CrossRef]
98. Sharma, V.; Thapliyal, K.; Pathak, A.; Banerjee, S. A comparative study of protocols for secure quantum communication under noisy environment: Single-qubit-based protocols versus entangled-state-based protocols. *Quantum Inf. Process.* **2016**, *15*, 4681–4710. [CrossRef]
99. Huang, A.; Barz, S.; Andersson, E.; Makarov, V. Implementation vulnerabilities in general quantum cryptography. *New, J. Phys.* **2018**, *20*, 103016. [CrossRef]
100. Bennett, C.H.; Brassard, G.; Mermin, N.D. Quantum cryptography without Bell's theorem. *Phys. Rev. Lett.* **1992**, *68*, 557. [CrossRef] [PubMed]
101. Inoue, K.; Waks, E.; Yamamoto, Y. Differential phase shift quantum key distribution. *Phys. Rev. Lett.* **2002**, *89*, 37902. [CrossRef] [PubMed]

102. Waks, E.; Takesue, H.; Yamamoto, Y. Security of differential-phase-shift quantum key distribution against individual attacks. *Phys. Rev. A* **2006**, *73*, 12344. [CrossRef]
103. Sasaki, T.; Yamamoto, Y.; Koashi, M. Practical quantum key distribution protocol without monitoring signal disturbance. *Nat. Photonics* **2015**, *509*, 475–478. [CrossRef]
104. Stucki, D.; Brunner, N.; Gisin, N.; Scarani, V.; Zbinden, H. Fast and simple one-way quantum key distribution. *Appl. Phys. Lett.* **2005**, *87*, 194108. [CrossRef]
105. Serna, E.H. Quantum Key Distribution from a random seed. *arXiv* **2013**, arXiv:1311.1582.
106. Boström, K.; Felbinger, T. Deterministic secure direct communication using entanglement. *Phys. Rev. Lett.* **2002**, *89*, 187902. [CrossRef]
107. Utagi, S.; Srikanth, R.; Banerjee, S. Ping-pong quantum key distribution with trusted noise: Non-Markovian advantage. *Quantum Inf. Process.* **2020**, *19*, 1–12. [CrossRef]
108. Lucamarini, M.; Mancini, S. Secure deterministic communication without entanglement. *Phys. Rev. Lett.* **2005**, *94*, 140501. [CrossRef] [PubMed]
109. Shaari, J.S.; Bahari, I.; Ali, S. Decoy states and two way quantum key distribution schemes. *Opt. Commun.* **2011**, *284*, 697–702. [CrossRef]
110. Verma, P.K.; El Rifai, M.; Chan, K.W.C. *Multi-Photon Quantum Secure Communication*; Springer: Singapore, 2019; ISBN 9789811086175.
111. Parakh, A.; Van Brandwijk, J. Correcting rotational errors in three stage QKD. In Proceedings of the 2016 23rd International Conference on Telecommunications (ICT), Thessaloniki, Greece, 16–18 May 2016; pp. 1–5. [CrossRef]
112. Khodr, M. Evaluations of Maximum Distance Achieved Using the Three Stage Multiphoton Protocol at 1550 nm, 1310 nm, and 850 nm. In Proceedings of the CYBER 2017: The Second International Conference on Cyber-Technologies and Cyber-Systems Evaluations, Barcelona, Spain, 12–16 November 2017; pp. 32–34.
113. Khodr, M. Evaluations of quantum bit error rate using the three stage multiphoton protocol. In Proceedings of the 2017 International Conference on Electrical and Computing Technologies and Applications (ICECTA), Ras Al Khaimah, United Arab Emirates, 21–23 November 2017; pp. 1–4. [CrossRef]
114. El Rifai, M.; Punekar, N.; Verma, P.K. Implementation of an m-ary three-stage quantum cryptography protocol. In Proceedings of the Proc.SPIE, San Francisco, CA, USA, 2–7 February 2013; Volume 8875. [CrossRef]
115. El Rifai, M. Quantum Secure Communication Using Polarization Hopping Multi-Stage Protocols. Doctor's Thesis, University of Oklahoma, Norman, OK, USA, May 2016. [CrossRef]
116. Hayashi, M. Finite-block-length analysis in classical and quantum information theory. *Proc. Jpn. Acad. Ser. B. Phys. Biol. Sci.* **2017**, *93*, 99–124. [CrossRef] [PubMed]
117. Chekhova, M.; Banzer, P. Polarization of Light. In *Classical, Quantum, and Nonlinear Optics*; De Gruyte: Berlin, Germany, 2015. [CrossRef]
118. Chan, K.W.C.; Rifai, M.E.; Verma, P.; Kak, S.; Chen, Y. Multi-photon quantum key distribution based on double-lock encryption. In Proceedings of the 2015 Conference on Lasers and Electro-Optics (CLEO), Munich, Germany, 21–25 June 2015; pp. 1–2. [CrossRef]
119. Miljkovic, N.N.; Stojanovic, A.D. Multiparameter QKD authentication protocol design over optical quantum channel. *Opt. Quantum Electron.* **2018**, *50*, 319. [CrossRef]
120. Hong, C.; Heo, J.; Jang, J.G.; Kwon, D. Quantum identity authentication with single photon. *Quantum Inf. Process.* **2017**, *16*, 236. [CrossRef]
121. Harun, N.Z.; Ahmad Zukarnain, Z.; Hanapi, Z.M.; Ahmad, I. Multi-Stage Quantum Secure Direct Communication Using Secure Shared Authentication Key. *Symmetry* **2020**, *12*, 1481. [CrossRef]
122. Deng, F.G.; Long, G.L.; Liu, X.S. Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block. *Phys. Rev. A At. Mol. Opt. Phys.* **2003**, *68*, 6. [CrossRef]
123. Long, G.L.; Liu, X.S. Theoretically efficient high-capacity quantum-key-distribution scheme. *Phys. Rev. A At. Mol. Opt. Phys.* **2002**, *65*, 3. [CrossRef]
124. Pan, D.; Li, K.; Ruan, D.; Ng, S.X.; Hanzo, L. Single-Photon-Memory Two-Step Quantum Secure Direct Communication Relying on Einstein-Podolsky-Rosen Pairs. *IEEE Access* **2020**, *8*, 121146–121161. [CrossRef]
125. Zhou, Z.R.; Sheng, Y.B.; Niu, P.H.; Yin, L.G.; Long, G.L.; Hanzo, L. Measurement-device-independent quantum secure direct communication. *Sci. China Phys. Mech. Astron.* **2020**, *63*, 1–6. [CrossRef]
126. Yang, L.; Wu, J.W.; Lin, Z.S.; Yin, L.G.; Long, G.L. Quantum secure direct communication with entanglement source and single-photon measurement. *Sci. China Phys. Mech. Astron.* **2020**, *63*, 1–8. [CrossRef]
127. Sheng, Y.B.; Zhou, L.; Long, G.L. One-step quantum secure direct communication. *Sci. Bull.* **2021**, *in press*. [CrossRef]
128. Chan, K.W.C.; El Rifai, M.; Verma, P.; Kak, S.; Chen, Y. Security analysis of the multi-photon three-stage quantum key distribution. *Int. J. Cryptogr. Inf. Secur.* **2015**, *5*, 1–13. [CrossRef]
129. Harun, N.Z.; Zukarnain, Z.A.; Hanapi, Z.M.; Ahmad, I. Hybrid M-Ary in Braided Single Stage Approach for Multiphoton Quantum Secure Direct Communication Protocol. *IEEE Access* **2019**, *7*, 22599–22612. [CrossRef]
130. Harun, N.Z.; Zukarnain, Z.A.; Hanapi, Z.M.; Ahmad, I.; Khodr, M.F. MQC-MB: Multiphoton Quantum Communication Using Multiple-Beam Concept in Free Space Optical Channel. *Symmetry* **2021**, *13*, 66. [CrossRef]
131. Kwek, L.; Cao, L.; Luo, W.; Wang, Y.; Sun, S.; Wang, X. Chip-based quantum key distribution. *AAPPS Bull.* **2021**, *31*, 1–8. [CrossRef]

132. Alshaer, N.; Nasr, M.E.; Ismail, T. Hybrid MPPM-BB84 Quantum Key Distribution Over FSO Channel Considering Atmospheric Turbulence and Pointing Errors. *IEEE Photonics J.* **2021**, *13*, 1–9. [CrossRef]
133. Alhussein, M.; Inoue, K.; Honjo, T. BB84 and DQPS-QKD experiments using one polarization-insensitive measurement setup with a countermeasure against detector blinding and control attacks. In Proceedings of the 2019 Conference on Lasers and Electro-Optics (CLEO), San Jose, CA, USA, 5–10 May 2019; pp. 1–2. [CrossRef]
134. Choe, J.-S.; Ko, H.; Choi, B.-S.; Kim, K.-J.; Youn, C.J. Integrated Polarization Beam Splitter Module for Polarization-Encoded Free-Space BB84 QKD. In Proceedings of the 2018 Optical Fiber Communications Conference and Exposition (OFC), San Diego, CA, USA, 13–15 March 2018; pp. 1–3.
135. Alshaer, N.; Moawad, A.; Ismail, T. Reliability and Security Analysis of an Entanglement-Based QKD Protocol in a Dynamic Ground-to-UAV FSO Communications System. *IEEE Access* **2021**, *9*, 168052–168067. [CrossRef]
136. Amer, O.; Krawec, W.O.; Wang, B. Efficient Routing for Quantum Key Distribution Networks. In Proceedings of the 2020 IEEE International Conference on Quantum Computing and Engineering (QCE), Broomfield, CO, USA, 12–16 October 2020; pp. 137–147. [CrossRef]
137. Zhou, C.; Bao, W.; Fu, X. Information-Disturbance Tradeoff of Individual Attack Against BBM92 Protocol. In Proceedings of the 2010 International Conference on Communications and Mobile Computing, Shenzhen, China, 12–14 April 2010; Volume 1, pp. 31–34. [CrossRef]
138. Honjo, T.; Nam, S.W.; Takesue, H.; Zhang, Q.; Kamada, H.; Nishida, Y.; Tadanaga, O.; Asobe, M.; Baek, B.; Hadfield, R.; et al. Entanglement-based BBM92 QKD experiment using superconducting single photon detectors. In Proceedings of the 2008 Conference on Lasers and Electro-Optics and 2008 Conference on Quantum Electronics and Laser Science, San Jose, CA, USA, 4–9 May 2008. [CrossRef]
139. Geng, J.; Jin, W.; Yan, X.; Cheng, Y. Performance on The Discrete Variable Based Satellite-to-Ground Quantum Key Distribution Links. In Proceedings of the 2019 IEEE International Conference on Signal, Information and Data Processing (ICSIDP), Chongqing, China, 11–13 December 2019; pp. 1–5. [CrossRef]
140. Miljković, N.N.; Stojanović, A.D.; Matavulj, P.S. Physical model for B92-QKD authentication based on analogy with optical chaotic systems. In Proceedings of the 2016 24th Telecommunications Forum (TELFOR), Belgrade, Serbia, 22–23 November 2016; pp. 1–4. [CrossRef]
141. Wijesekera, S.; Palit, S.; Balachandran, B. Software Development for B92 Quantum Key Distribution Communication Protocol. In Proceedings of the 6th IEEE/ACIS International Conference on Computer and Information Science (ICIS 2007), Melbourne, Australia, 11–13 July 2007; pp. 274–278. [CrossRef]
142. Xu, X.; Chen, X. Simulating B92 Protocol in Depolarizing Channel. In Proceedings of the 2010 6th International Conference on Wireless Communications Networking and Mobile Computing (WiCOM), Chengdu, China, 23–25 September 2010; pp. 1–3.
143. Guerreau-Lambert, O.L. *Multidimensional Quantum Key Distribution with Single Side Pulse and Single Side Band Modulation Multiplexing*; Georgia Institute of Technology: Atlanta, GA, USA, 2005; ISBN 0542433656.
144. Kim, Y.; Ko, Y.-C. Cramer-Rao lower bound of channel estimator in continuous variable quantum key distribution. In Proceedings of the 2016 International Conference on Information and Communication Technology Convergence (ICTC), Jeju Island, Korea, 19–21 October 2016; pp. 678–680. [CrossRef]
145. Ghalaii, M.; Kumar, R.; Razavi, M. Quantum-scissor amplified continuous-variable quantum key distribution. In Proceedings of the 2017 Conference on Lasers and Electro-Optics Europe & European Quantum Electronics Conference (CLEO/Europe-EQEC), Munich, Germany, 25–29 June 2017; p. 1. [CrossRef]
146. Kiktenko, E.O.; Malyshev, A.O.; Gavreev, M.A.; Bozhedarov, A.A.; Pozhar, N.O.; Anufriev, M.N.; Fedorov, A.K. Lightweight Authentication for Quantum Key Distribution. *IEEE Trans. Inf. Theory* **2020**, *66*, 6354–6368. [CrossRef]
147. Vokic, N.; Milovančev, D.; Schrenk, B.; Hentschel, M.; Hübel, H. Deployment Opportunities for DPS-QKD in the Co-Existence Regime of Lit GPON / NG-PON2 Access Networks. In Proceedings of the 2020 Optical Fiber Communications Conference and Exhibition (OFC), San Diego, CA, USA, 8–12 March 2020; pp. 1–3. [CrossRef]
148. Ranu, S.K.; Prabhakar, A.; Mandayam, P. Differential Phase Encoding Scheme for Measurement-Device-Independent Quantum Key Distribution. In Proceedings of the 2019 National Conference on Communications (NCC), Bangalore, India, 20–23 February 2019; pp. 1–5. [CrossRef]
149. Iwai, Y.; Honjo, T.; Inoue, K.; Kamada, H.; Nishida, Y.; Tadanaga, O.; Asobe, M. Polarization independent DPS-QKD system using up-conversion detectors. In Proceedings of the 2008 Conference on Lasers and Electro-Optics and 2008 Conference on Quantum Electronics and Laser Science, San Jose, CA, USA, 4–9 May 2008. [CrossRef]
150. Klicnik, O.; Munster, P.; Horvath, T.; Hajny, J.; Malina, L. Quantum Key Distribution Polygon. In Proceedings of the 2021 13th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), Brno, Czech Republic, 25–27 October 2021; pp. 263–266. [CrossRef]
151. Abushgra, A.A. SARG04 and AK15 Protocols Based on the Run-Time Execution and QBER. In Proceedings of the 2021 IEEE 5th International Conference on Cryptography, Security and Privacy (CSP), Zhuhai, China, 8–10 January 2021; pp. 176–180. [CrossRef]
152. Lopes, M.; Sarwade, N. On the performance of quantum cryptographic protocols SARG04 and KMB09. In Proceedings of the 2015 International Conference on Communication, Information & Computing Technology (ICCICT), Mumbai, India, 15–17 January 2015; pp. 1–6. [CrossRef]

153. Ali, S.; Mahmoud, O. Implementation of SARG04 decoy state quantum key distribution. In Proceedings of the 2011 6th International Conference on Telecommunication Systems, Services, and Applications (TSSA), Denpasar, Bali, 20–21 October 2011; pp. 86–90. [CrossRef]
154. Zheng, J.; Sun, W.; Wang, W.; Liu, J.; Zhu, N.; Chang, G.-K. Orthogonal polarization modulation based fully coherent self-heterodyne detection for future UDWDM-PON. In Proceedings of the 2015 International Symposium on Next-Generation Electronics (ISNE), Taipei, Taiwan, 4–6 May 2015; pp. 1–3. [CrossRef]
155. Hua, B.; Ju, C.; Zhang, Z.; Guo, Q.; Huang, X. Low Cost PAM4-TDM-PON Upstream Scheme Based on Electrical Nyquist Pulse Shaping and Heterodyne Coherent Detection. In Proceedings of the 2018 Asia Communications and Photonics Conference (ACP), Hangzhou, China, 26–29 October 2018; pp. 1–3. [CrossRef]
156. Khir, M.F.A.; Bahari, I.; Zain, M.N.M.; Ehsan, A.A. Erroneous signal detection and secure distance improvement in two way Quantum Key Distribution protocol with decoy state. In Proceedings of the 2012 IEEE 3rd International Conference on Photonics, Pulau Pinang, Malaysia, 1–3 October 2012; pp. 390–394. [CrossRef]
157. Khir, M.F.A.; Bahari, I. Secure communication with practical two way Quantum Key Distribution protocol and Weak+ Vacuum decoy state. In Proceedings of the 2013 IEEE 4th International Conference on Photonics (ICP), Melaka, Malaysia, 28–30 October 2013; pp. 281–283. [CrossRef]
158. Xu, Y.; Lin, J.; Li, Y.-H.; Dai, H.; Liao, S.-K.; Peng, C.-Z. Active Phase Stabilization for the Interferometer With 128 Actively Selectable Paths. *IEEE Trans. Nucl. Sci.* **2019**, *66*, 1076–1080. [CrossRef]
159. Harun, N.Z.; Zukarnain, Z.A.; Hanapi, Z.M.; Ahmad, I. Evaluation of Parameters Effect in Multiphoton Quantum Key Distribution Over Fiber Optic. *IEEE Access* **2018**, *6*, 47699–47706. [CrossRef]
160. Zhang, C.; Zhu, J.; Wang, Q. Reference-Frame-Independent Measurement-Device-Independent Quantum Key Distribution with Modified Coherent States. *IEEE Photonics J.* **2018**, *10*, 1–8. [CrossRef]
161. Viel, F.; Augusto Silva, L.; Leithardt, V.R.; De Paz Santana, J.F.; Celeste Ghizoni Teive, R.; Albenes Zeferino, C. An Efficient Interface for the Integration of IoT Devices with Smart Grids. *Sensors* **2020**, *20*, 2849. [CrossRef] [PubMed]