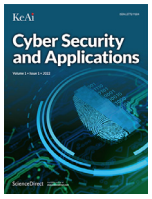
Cyber Security and Applications 1 (2023) 100019

Contents lists available at ScienceDirect

Cyber Security and Applications

journal homepage: http://www.keaipublishing.com/en/journals/cyber-security-and-applications/



Quantum communication with RLP quantum resistant cryptography in industrial manufacturing

Biswaranjan Senapati [a], Bharat S. Rawal [b,*]

[a] Computer Science Department, Capitol Technology University, Laurel, MD, USA
[b] Cybersecurity Department, Benedict College, Columbia, SC, USA

ARTICLE INFO

Keywords:
Cybersecurity
Cryptography
Quantum Machine Learning
RLP
Quantum Key Distribution
Quantum cryptography

ABSTRACT

This paper presents the best outcome of the Quantum communication use case of industrial manufacturing, using quantum theory to achieve secure data transfer between industrial production facilities and production units, especially in the most restricted industrial manufacturing facilities (i.e., Air and Defense production units). Quantum computing has several features to support manufacturing and production units within defense industrial products. Users must validate their user credentials and other essential information to access critical data from the source to the target system. We introduce Rawal Liang and Peter's (RLP) sequence for quantum key distribution to support the security and privacy of industrial manufacturing businesses.

1. Introduction

Quantum Computing also enhances the most critical digitalization business drives in industrial manufacturing practice and helps predict the performance optimization, operational excellence, and use cases of manufacturing excellence in industrial manufacturing business units. In a general statement, in the twenty-first century, most of the industrial manufacturing facilities and units, along with the operations facilities, are handling sensitive information, critical product information, Industrial manufacturing data(CAD, CAM, Manufacturing Products Information), Financial transaction information, exchanges of data in between designer and prototype builders across the industrial sites, data related to the confidential print documents, marketing (pictures, videos, printed flags, animations) across the industrial sites. These data and information are critically confidential and essential for industrial manufacturing sites while considering a defense product or a critical chip manufacturing contract. The production planning for the existing products/services or new products/services needs a robust environment with a strong identity, accessibility, and confidentiality guidelines within the manufacturing processing in industrial production sites [1].

In an industrial production operation, cryptography needs a public key infrastructure (PKI), which is the private root key that helps it operate within the units. It helps with user authentication, credential verification, and access control, along with signing the chain of certificates representing the identity of devices and controlling access to networks, preventing counterfeit protection, and ensuring customer data security. Through the public-key cryptography mechanism, data or information encryption and transmission could be easily achieved and possible to protect critical access control to authorized users in industrial units. During the entire communication, a private key is deployed while decrypting the data from the communication media [2].

In a general statement, in the twenty-first century, most of the industrial manufacturing facilities/units along with the operations facilities are still using paper, spreadsheets, excel sheet-based and phone calls to share information on predictive maintenance (PdM) with the plant shop floor from other departments, outside suppliers and customers to fulfill the demand and supply network [3]. In manufacturing and industrial facilities, data security and information exchange are key challenges while dealing with day-to-day operational activities. Most industrial operations require the exchange of sensitive files from users to factory managers, from factory managers to production unit planners, or as part of the exchange of communication between partners, vendors, suppliers, and external parties (i.e., consumers, manufacturers, vendors, or any service providers). The entire transaction requires the most secure, confidential, integrity, and authenticated communications among the associated parties, whether internal or external [4]. Per a Gartner report, there are 66% of users affected by cyber-attacks, 32% suffered a production or operation loss due to a cyber-attack, 7% suffered the theft of sensitive data by a cyber-attack, and more than 67% think that the measures taken to protect against cyber-attacks are inadequate and inappropriate due to a lack of "quantum computing" or "information theory." In quantum computing, communication theory can be the best option to manage the best communication mechanism while dealing with Industry 4.0 [5].

* Corresponding author.
E-mail address: bharat.rawal@benedict.edu (B.S. Rawal).

https://doi.org/10.1016/j.csa.2023.100019
Received 13 February 2023; Received in revised form 7 May 2023; Accepted 17 May 2023
Available online 26 May 2023

In industrial operations and large enterprises, industrial sites have been using the core SAP S/4 applications to perform the day-to-day enterprise-wide operations in sales, manufacturing, financial transactions, manufacturing, and production order management. S/4 Systems needs data security, confidentiality, and to be accessible to authorized users, and it offers the capability to perform digital transactions across the GUI and Fiori application [6]. It would be ideal to have cipher trust transparent encryption in the S/4 Hana system to protect and safeguard enterprise data and transactions in order to meet information security compliance and safeguard data security, data governance as per enterprise-wide application, and corporate compliance as suites in ISO 27,001-Information Security Management System (ISMS) [7].

In quantum computing, the Quantum Key Distribution (QKD) plays a vital role in cryptography in quantum computing networks, is extremely useful for quantum industrial applications, and offers a huge amount of opportunity to protect key critical security information in Industry 4.0. One of the most secure communication methods for exchanging encryption keys known only to senders and receivers is quantum key distribution (QKD). In quantum computing, the Quantum Key Distribution (QKD) plays a significant role in cryptography in quantum computing networks, which is extremely useful for quantum industrial applications because it provides better security information and safeguards critical industrial operational parameters across production sites. In QKD, the encrypted messages are shared with the communication parties (senders and receivers). Quantum key distribution is part of quantum physics, in which the exchange of cryptographic keys is transferred from senders to destinations with secure, achievable, guaranteed, and trusted communication information between senders and receivers. QKD has two key players (parties): the source and the destinations [8].

For secure communication, the QKD enables both parties to produce and share a common key that could be used to encrypt and decrypt messages while establishing the communication mechanism in the communication network at the network layer. In quantum cryptography, quantum key distribution (QKD) is the most trusted method of distributing the key, and the messages that can be sent enable users to send both sides (source and destination). Based on quantum mechanics, quantum cryptography generates and distributes symmetric cryptographic keys separately and efficiently between two geographical locations to avoid malicious attacks by hackers or unidentified individuals [9].

From a conventional key distribution standpoint, quantum communications and QKD are much more scalable and different, and they rely on the quantum laws of nature to protect critical data, information, and transactions securely and make them accessible to selective users who could communicate and own a private key. No one can attack or unauthorizedly access the data in the same way as per quantum laws [10].

The following is how the rest of the paper is structured: The introduction is covered in section I, and the related work is covered in section II. Then, section III describes quantum cryptography's application in industrial manufacturing. Section IV describes facts on quantum key distribution. Section V, talks about the RLP sequence. Section VI cryptography and quantum key distribution. Section VII talks about TS-quantum key distribution. Section VIII talks about the challenges of quantum key distribution. Finally, section IX concludes the research paper.

2. Related works

According to the quantum business report, venture capital financiers invested approximately US$ 147 million in quantum computing startups and governments worldwide in January 2019. Since 2017, they have also funded US$ 2.2 billion in research and development assistance. Quantum cryptography is a technique used to secure confidential information and data while transporting it from the source to the destination, which is the key combination of quantum mechanics and encryption. The quantum cryptography solution is incredibly useful to deploy for ensuring network security, application security, and the ability to offer security across the communication layer in the network as a service; it integrates both hardware and software technologies in any environment [11]. It is universally used in industrial automation, production, the automobile industry, data security, defense production, power management, and semi-conducting industrial manufacturing places. The below picture explains the global quantum cryptography solutions and service providers around the globe:

Decoy-state BB84 [12,13] is a well-known illustration of a DV-QKD[28] protocol, whereas Gaussian modulated coherent state CV-QKD [13] is the more widely applied protocol in the CV framework. The single-photon detectors are also necessary for distributed-phase-reference protocols like differential phase shift (DPS) [4], quantum key distribution (QKD) [13], and coherent one-way (COW) [4,14], where the key information is only stored on the phase shift between two adjacent poorly cohesive pulses and the photon arrival rate in both places.

Beyond these conventional protocols, there have been significant recent developments in QKD, most notably the proposed measurement-device-independent (MDI) QKD [6] (see also [7]) and the so-called Robin-Round (RR) DPS QKD protocol, which eliminates the need to monitor signal disturbance to establish security [15]. While the latter has an extremely high noise tolerance, the former offers a useful technique to stop security breaches caused by the receiver's detectors' flaws. Experimental proofs of both plans can be found, for example, in Refs. [11–13] and Photonic integration could be more beneficial and useful in industrial operations.

3. Quantum cryptography's application in industrial manufacturing

In Industry 4.0, the industrialization of smart metering and smart factories is highly demanded as compared to the traditional way of managing the factory and industrial operations. In terms of business demands, protecting industrial networks, and devices, and maintaining a secure, confidential communication network within industrial production sites is critical [10]. All these industrial equipment and communication devices are highly vulnerable, and it is critical to protect the data and information transactions within the combination and devices. With the help of cryptography, the quantum layer of cryptography adds an extra security measure to industrial networks and secures the data and information transactions access accessible networks.

The exchange of sensitive files and information could be easily achieved with the help of quantum computing and with the help of quantum communication theory [16]. It can be achieved through information security, data protection, availability, and ultimately operational security giving more quality for operational and industrial benefits. Here are a few industrial operations in production sites where cryptography and secure communication between sources and destinations are required:

- Industrial manufacturing design data (CAD, CAM, and manufacturing documents).
- Financing documents (auto banks, leasing companies).
- Exchanges of data between designers and prototype builders across the industrial sites.
- Exchanges of data in confidential printed documents (prospectuses before publication).
- Marketing (pictures, videos, printed flags, animations) across the industrial sites.
- Exchange of test data and information across the industrial production sites and restricted test zone.
- Production Pipeline data and future demand by manufacturing execution systems/ERP Systems.
- Exchange of personal information on digital platform.

Smart equipment in industrial manufacturing and production units includes IIoT devices, sensors, 5G, the Edge network, and other ERP-SAP applications. Most of the IoT, Industrial IoT, and 5G networks need quantum cryptography and the application of QKD to make industrial operations secure, confidential, and accessible to authorized network

participants in any critical communication [10]. Through secret keys and QKD, security and data privacy can be managed and optimized for a better smart factory's application in shopfloor activities, this could be a key aspect of managing industrial applications and operational planning concerning the production order, make-to-order, make-to-stock, and order fulfillment scenarios [10,17,18]. In 2009, a couple of Swiss researchers implemented the QKD system in a fiber optic network, and they used the coherent one-way (COW) protocol to implement it in an industrial operation. They successfully demonstrated the customized version of the BB84 protocol. When considering a defense or critical industrial product, quantum cryptography is the most important and critical for industrial operational planning [18]. Hybrid quantum-classical machine learning is used for near real-time space-to-ground communication of ISS lightning imaging sensor data [19]. Fadli and Rawal explored the practical realities of both quantum sensing for ultrasensitive measurements and quantum communications to provide unparalleled security, data rates, and efficiency [20].

4. Facts on quantum key distribution

In quantum cryptography, the process of encrypting the data and securing the information is done by applying a unique philosophy of "Quantum Mechanics/computing" which is to encrypt the data and transmit it to the destination from the source without even getting hacked by hackers. Quantum cryptography and QKD are the best methods to protect the data privacy, security, accessibilities, confidentiality, and availability of information to authorize resources in a digital manufacturing environment and would be best practices in industrial operation within Industry 4.0 [21,14,22]. Here are a few key principles of quantum mechanics within quantum cryptography:

- Photons are generated randomly in one of two quantum states during the transmission.
- Quantum entanglement or superposition could not be changed without any further functions.
- The cloning of some quantum properties can be possible partially, but not in their entirety
- Photons exist in multiple locations in quantum superposition to perform the superposition.

The QKD works by the philosophy of particles, photons, and light particles, or over the optic fibers to establish the communication mechanism between-source and between-destinations mechanism The photons delivered constitute a stream of (0, 1) which is the photon and have a random quantum state [8,11]. In the communication mechanism, when the photon or light particles reached their receiving end from senders, they will travel through the beam splitter.

In quantum computing, a beam splitter (BS) is used as the source of photon quantum entanglement, in which the statistics of photons change at the output ports of the beam splitter. In QKD, a beam splitter is used to divide the photons and polarize them, it divides beams of light linearly or diagonally. Both parties Alice and Bob can see bits as (0, or 1). An attacker can use the beam splitter to interrupt or eavesdrop on the key creation process. Eve may then be able to control what she sends to Bob, interfering with their secret quantum key distribution process. Alice and Bob no longer have a secure channel in which they can create a secret key. Security issues such as beam splitting attacks and other interferences like light injection must be addressed in quantum encryption systems. A beam splitter is an optical device that divides light into transmitted and reflected beams [6].

- Quantum coin flipping:

In cryptography, quantum coin-flipping is a cryptographic primitive in which two or more parties do not trust each other and want to establish a fair coin-flipping relationship. All these parties are not physically near each other, and they use quantum communication channels to interact. Protocol quality is determined by the best possible cheating strategy, which is the solution of a complex semidefinite optimization. It uses the principle of quantum mechanics to encrypt the message for secure communication. With the help of a low-level cryptographic algorithm can build a cryptographic protocol to establish computer security and network security [23].

- Strong coin flipping:

The strong coin flipping (SCF) is to be a coin flipping problem where each player is oblivious to the preference of others (Alice and Bob)

- Weak coin flipping:

Weak coin flipping (WCF) is to be a coin flipping where each player knows the preference of the other(Alice and Bob) [17], they both have an opposite preference.

- Bias:

In the case of the bias coin flipping, both the player (Alice and Bob), are intended to implement the protocol at the same time, and player 1(Alice) cheats using her best strategy against player 2(Bob) who honestly follows the protocol [24].

In BB84- QKD protocol, there are two users in this communication channel (Alice, and Bob). Alice prepares several qubits, sends them to Bob, and Bob measures the qubits. Alice and Bob exchange some information over the classical channel to ensure Bob measured correctly. Then Alice and Bob confirm all the choices made for a few of the circuits to confirm there is no eavesdropper, there is one third party user "Eve," on the line. The operations Alice and Bob perform as well as the information they share is dependent on the quantum key distribution protocol used.

The BB84 protocol uses single qubits that can be in either a $|0\rangle$ or a $|1\rangle$ state in the "Z" basis or the $|+\rangle$ or $|-\rangle$ state in the X-basis. Alice initializes qubits randomly between the four states and then sends them to Bob over the quantum channel. Bob measures the qubits on either the Z or X basis. Bob shares the bases he measured with Alice over classical channels and Alice confirms whether she measured the same. Alice and Bob also confirm some measurements to determine whether there was an eavesdropper on the line. Then they use the initialization or measurement of either a 0 or a 1 state in the respective basis as a bit in the key. For example, if Alice prepared a qubit in the $|+\rangle$ state and Bob measured on the X-basis, a "0″ would be added to the key. [21] Alice chooses to measure between 2 bases, so she has a $\frac{1}{2}$ chance of picking the same basis as Bob – either they both pick the Z-basis, or they both pick the X-basis.

In BB84 the probability of generating a correct circuit (both Alice and Bob measure on the same basis) is:

$$P\,correct = (Alice\,basis) \times (Bob\,same\,basis)$$

$$Pcorrect = 1/2 \times 1 = 1/2$$

Also note that for Eve to successfully infiltrate a circuit, she must guess the same circuit as Alice. Since there are two choices of the basis for Eve, this means the probability of Eve infiltrating a circuit without being detected is

$$P\,\mathrm{inf}\,iltrate = (Alicebasis) \times (Evebasis)$$

$$P\,\mathrm{inf}\,iltrate = (1/2) \times (1/2) = (1/4)$$

5. Rawal, Liang and Peter (RLP)

One of the unique properties of the RLP sequence is that the elements of the sequence are not derived from adding or subtracting from the RLP sequence. This makes a very unique sequence, and we can use it for encryption and decryption randomly on every attempt. RLP sequence is referred to as No Sum (NS) sequence. *Algorithm 1 RLP Cryptosystem*

Result:	one NS Sequence number N from N*
Input:	p,q are two unique large prime numbers NS_seq [] = Generate NS Sequence;
Start:	Sender Side: Encryption(Ciphertext, n, e) = RSA_encrypt (p,q); where e = public key of receiver and n = p*q
N1	= NS_seq[0]; //First NS Sequence number; Find Nn from NS_seq
N* =	Nn (as a public key) where n is the position of the element in the NS sequence and is shareable to a receiver.
Receiver Side:	Decryption
N =	retrieve (N*);
plaintext=	RSA_decrypt (ciphertext, n, d); where d = textbfEnd example sample sequences listed in Fig. 2 & 3.

NS sequence plays vital importance in QKD distribution by randomizing starting element as a secret key.

6. Cryptography and QKD

The QKD has the following facts and opportunities within the industrial manufacturing business

- Prepare-and-measure protocols: This is mostly useful for measuring unknown quantum states. Universally used in the detection of eavesdropping and understanding the data potentially intercepted.
- Entanglement-based protocols: Based on the quantum state of two objects which are linked together, forming a combined quantum state. The concept of entanglement means that the measurement of one object thereby affects the other. In this method, if an eavesdropper accesses a previously trusted node and changes something, the other involved parties will know [25].
- DV-QKD- It is called the discrete variable quantum key distribution, which is based on the photon detector to measure quantum states, the BB84 protocol is the best example.
- Continues variable QKD- continuous variable QKD (CV-QKD) [13]. It encodes quantum information on a laser's amplitude and phase quadrants, sending the light to a receiver.
- QKD: Establishing a public key in-between two parties.
- MQC: Little trust in one another (Alice and Bob) offer private input. Quantum Coin Flipping and Quantum commitment are the best examples.
- BNQSM: Works on commitment and unforgettable transfer procedure, it is easy to use and completely impenetrable.
- PBQC: Focus entirely on the player's location for verification and link to quantum teleportation protocol based on ports [26].
- DIQC: It is device independent and very noisy.

In Quantum Communication theory and system, these are few quantum protocols used widely while in Quantum Cryptography in digital transformation transactions (QKD protocols) are the following:

- BB84:

For the first time, this protocol was implemented by Bennett and Brassad, the cryptographic key was generated based on protocol BB84, by use of two different channels (classical and quantum computing) within free-space wireless communications.

This protocol can produce four states that can be part of a quantum state with two polarization states (i.e., $|H>$, $|V>$, $|45^\circ>$, $|135^\circ>$) [4,14,21]. Hacking in this protocol might not be as simple as we thought.

- Silber horn:

Post-quantum Cryptography and quantum key distributions

- B92 protocol:

This was invented by Bennett in 1992 and is the simplest version of the BB84 protocol, this has two nonorthogonal states [12,27]. The formula for this protocol is stated below.

$\varphi j >= \beta|0x> +(-1)\, j\alpha|1x>$ [22]

Where $j = \{0,1\}$, $\{|0x>,|1x>\}$ are the eigenstates of the X basis and $\beta = \cos\theta\ 2$, $\alpha = \sin\theta\ 2$ [4,14,22].

- Decoy state:

One of the widest protocols used in the QKD scheme. With the help of multiple intensity levels at the transmitter's source i.e., qubits are transmitted by Alice using randomly chosen intensity levels (one signal state and several decoy states), throughout the channel. Alice announces publicly which intensity level has been used for the transmission of each qubit. A successful PNS attack requires maintaining the bit error rate (BER) at the receiver's end, which cannot be accomplished with multiple photon number statistics. Useful for photon-number-splitting attacks.

- KMB09:

This is an alternative QKD protocol that is based on mutually unbiased bases. Due to the possible distance between Alice and Bob, this protocol allows more noise in the transmission line without any intermediate nodes [39].

The above diagram explains the quantum cryptography industrial application by geography, services type, by security types, and also considers the Key players.

Below Fig. 6 represents the type of attack along with the industrial device's parameter.

1. DDOS
2. Backdoor
3. Injection
4. Password and Ransomware
5. Scanning

7. TS-quantum key distribution (TS-QKD)

The time sensitive QKD is the synergy between time sensitive networking (TSN) and quantum key distribution (QKD), and it provides fast, deterministic, simple, and secure communication across the source and destination. All the QKD communications are compatible with communication cloning quantum states, and that is one of the greatest features of QKD.

In this paper, we analyze various eavesdropping techniques, which may be either translucent or opaque to the transmitted photons, and we estimate the error rate above which the key distribution is deemed unsafe and should be abandoned.

Key benefits of TS-QKD:

- Simpler, lower-cost, and more secure than classical cybersecurity solutions
- Deterministic (TSN-enforced) flow patterns with nanosecond resolution
- Reduced cybersecurity attack surface by restricting traffic injection
- Low-cost control of Measurement-Device-Independent (MDI) QKD
- Converged and fully characterized network
- Eavesdropper detection
- High key entropy

Application of Time-Sensitive Quantum Key Distribution (TSQKD):

The Time-sensitive quantum key distributions are used in the industrial network, IIoT, equipment, and data center to reduce the cybersecurity attack surface by restricting cyber traffic injections. Essentially it is the most cost-effective solution for the measurement-device-independent (MDI) QKD (Figs. 1, 3, 4, 5, 7, 8, 9, 10, Tables 1–4).

8. Challenges of QKD

In a quantum computer, there are a lot of challenges while establishing a secure communication path in-between the source and target. In the communication network, QKD faces a lot of challenges due to

Table 1
Quantum computing cryptography service provider around globe.

Service Provider (Quantum Computing)	Geography	Industries Focused by Quantum Technologies
Honeywell International Inc	USA	Pharma, Chemical, Aerospace, Finance, Logistics
Infineon Technology AG	Germany	Automotive, Communications, Consumers, Security and Financial solutions
IBM Corp	USA	Healthcare, Manufacturing, Finance, Industrial
MagiQ Technologies Inc	USA	QKD, PQC
Quantum Exchange	USA	QKD, Quantum Cryptography, PQC
Qubitekk Inc	USA	Defense, Financial and Utilities Industries
Quintessence Labs Pty Ltd	Australia	TSF, Quantum networks, Defense and Financial Applications
Raytheon Co	China	Quantum devices and sensors in Defense and Industrial manufacturing business
SK Telecom Co Ltd	South Korea	QKD, Network federation, and Infrastructure Industrial Applications
Toshiba Corp	Japan	QKD, Post Quantum Cryptography (PQC) to support telecom business, Defense, Financial and Utility Applications

Table 2
Quantum Computing value chain in Industrial manufacturing work sites.

Business Process	Quantum Computing tools Used	Future Applications
Design of Industrial Manufacturing Sites and Operational keys	Quantum AI, ML, QKD	Designing key products and prototyping, reduces the defects and bugs
Products designing and PIM	Quantum AI, ML, Optimizations	New Products and Manufacturing Industry Prints, Components and BoM's
Supply Chain and SOP	Quantum AI, ML, Optimizations	Predicts the supply chain, sales operational planning and IBP
Productions, and Manufacturing executions processing	Quantum AI, ML, Optimizations	Complex designing within manufacturing practices, QMS, IP
Marketing new products and Sales Customer Services	Quantum Optimizations	Sales and services of new products and solutions to business operational

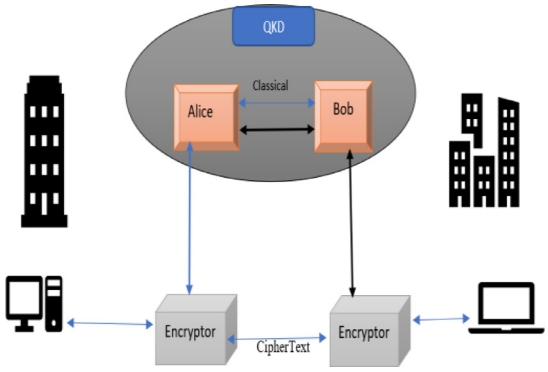


Fig. 1. Quantum key distribution network.

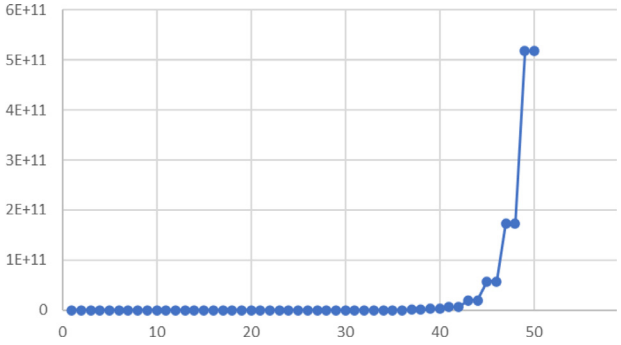


Fig. 2. RLP sequence with starting element numerical value 3.

Table 3
List of abbreviations used in this paper.

Abbreviations	Explanations	Uses
QC	Quantum Computing's	Network
QML	Quantum Machine Learning	Programming
QAI	Quantum Artificial Intelligence	Programming
QKD	Quantum Key Distribution	Cryptography
BNQSM	Bonded and Noise quantum storagemodel	Cryptography
QSDC	Quantum secure direct communication	Cryptography
MQC	Mistrustful quantum cryptography	Cryptography
PBQC	Position based Quantum Cryptography	Cryptography
DISK	Device-Independent Quantum Cryptography	Cryptography

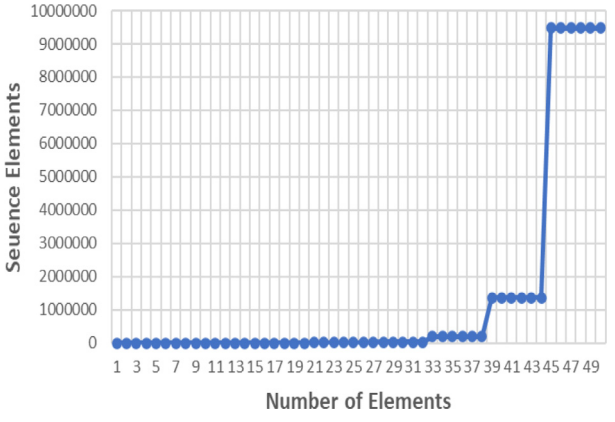


Fig. 3. RLP sequence with starting element numerical value 7.

secreting key rate (SKR), distance size, timeline, costs, and the security of information passing from source to destination. The most familiar challenges while implementing the QKD are the hardware, key rates,

Table 4
Quantum algorithm and industries.

Quantum Computing Models	Useful	Industries
Shor's Algorithm	Solves the discrete logarithm problem and the integer factorization problem in polynomial time	Finance and Banking Industrial Applications
Grover's Algorithm	Especially searches an unstructured database with N entries	Healthcare and Other industrial applications
Hamiltonian Simulation Algorithm	Simulating the dynamics of quantum systems	Cryptography and Security

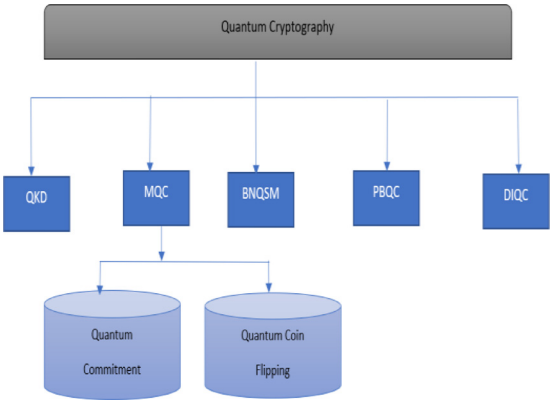


Fig. 4. Different types of cryptography in quantum computing.

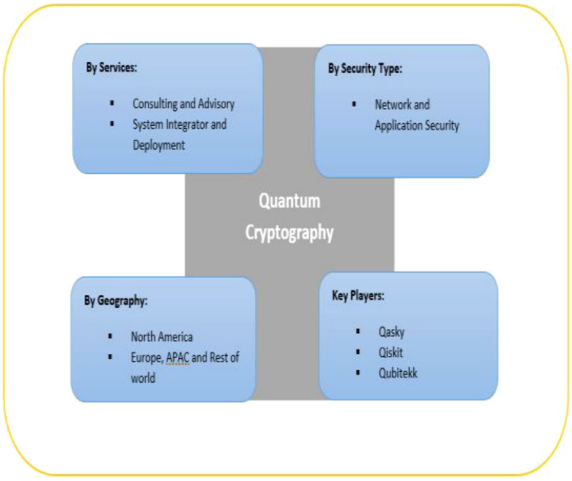


Fig. 5. Quantum Cryptography by service, Geography, security type, and key player.

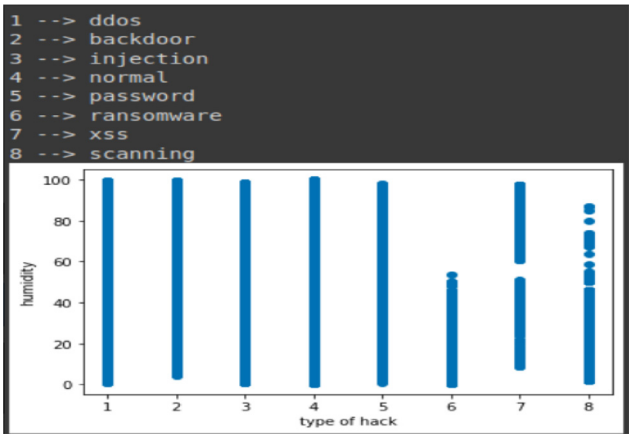


Fig. 6. Comparison of various attacks along with register inputs.

and cost factors. While considering practical network security within the QKD, it is advisable to consider the Device independent (DI), MDI-QKD, and network- QKD as the best practice to implement [8]. There are three main challenges concerning implementing the QKD into practice.

- Expensive and Infrastructure challenges
- Highly Interfacing with the existing landscape
- Need of an optical fiber as a photon carrying device

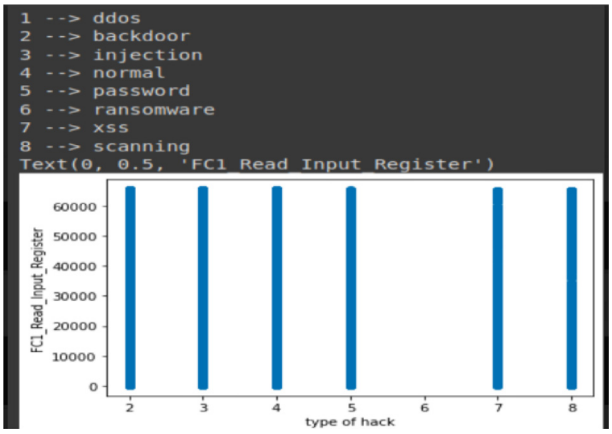


Fig. 7. . Comparison of various attacks along with register inputs.

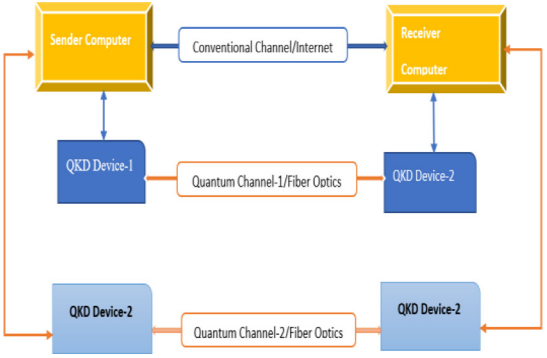


Fig. 8. Quantum Communications and Optical Network.

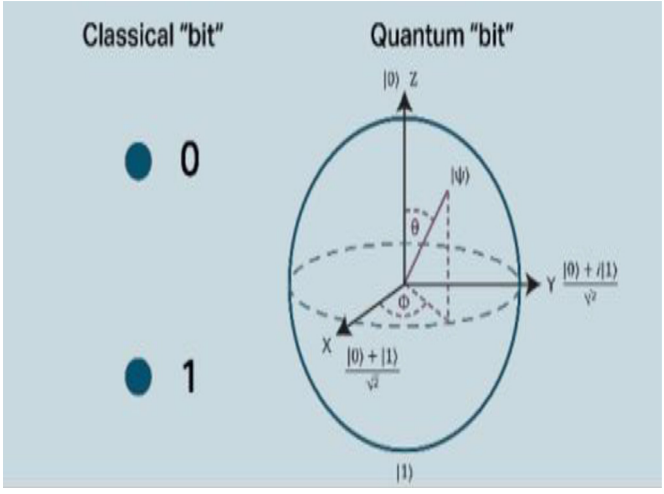


Fig. 9. Difference between classical “bit” and Quantum “Bit”.

A significant component of quantum cryptography is the Quantum Key Distribution (QKD) methodology, which uses quantum physics to produce and distribute symmetric cryptographic keys between two users who are separated by distance. Several effective QKD networks have been developed in previous years to evaluate the application and compatibility of various real-world solutions. This article examines previously used methodologies, demonstrating how to set up QKD networks and outlining the current difficulties with QKD networking. This analysis examines the network aspect by taking into account network organization, routing, and signaling protocols, simulation methodologies, and

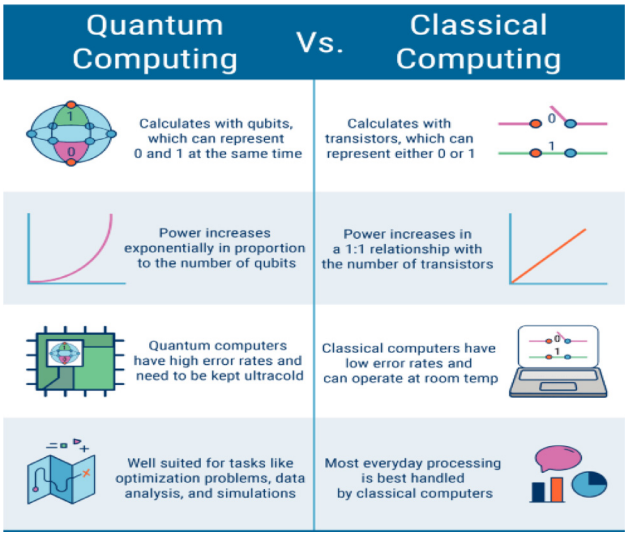


Fig. 10. key benefits of quantum computing.

software defined QKD networking strategy, in contrast to research that concentrates on optical channels and optical equipment [41].

Key Difference between Quantum Computing over Classical Computers:

In the computational world, there are a few key differences between Quantum Computing over classical computing and there is a huge amount of research and innovation is still in place to understand the benefits of quantum computing, network theory, and Quantum communication information sciences to solve a real-world problem.

1. Processing Capabilities.
2. Quantum Logic Gate.
3. Quantum Annealing.
4. Quantum Superposition.

9. Conclusion

This paper focuses on the implications of advanced technologies, digital twins, and the application of quantum cryptography in industrial operations, where quantum key distribution (QKD) protects smart factories, data centers, shop floors, and other manufacturing facilities. In the digital age, industrial manufacturing and smart factories are based on the application of smart technologies (e.g., AI, ML, quantum computing, sensors, IIoT, edge technologies, 5G, and SAP S/4HANA cloud database), which is critical to protect manufacturing operationally critical data, information, and security, which is critical to gain a successful enterprise business. Most manufacturing facilities rely on auto-control devices and sensors. To support the customer and supplier, industrial manufacturing sites obtained a continuity of innovative product designs, manufacturing efficiency, and order fulfillment in best-in-class conditions [13].

Quantum cryptography could save the most vital industrial product information, research and development information, product information and PIMs, and defense products related to key BOMs and components, as well as the most competitive challenges in qubits. Quantum computing and communications applications are used in industrial manufacturing facilities where key data, information, and sensitive industrial manufacturing information, as well as products and information related to key defense products and BOMs/components, are stored in secure, confidential locations accessible only to authorized users across the sites. Industrial cryptography and quantum cryptography were addressed, and the opportunity for quantum communication was handled in this article [28].

In today's digital manufacturing and smart factory sites, handling industrial manufacturing operations requires sensors, IIoTs, equipment, research and innovation centers, and industrial networks, which are highly connected with edge computing, clouds, and 5G interfaces. These challenges are impractical to address using traditional computing, as we require quantum computing and quantum-based cryptography to protect industrial production sites [29]. This paper analyzed the various aspects of quantum communication and information theory, along with quantum cryptography and various protocols associated with QKD. This could improve industrial manufacturing production efficiencies and optimize digital transformation best practices within Industry 4.0 [8,30]. We have explained various QKD theorems, and the protocol associated with the QKD within the various attributes of quantum cryptography and beyond with industrial digitalization (IIoT, MES, SAP S4, sensors, and 5G networks) to make the internet network more secure and confidential for industrial production business operations. We specifically included one of the quantum cryptographic algorithms, BB84, which is very safe and different from the existing traditional cryptographic algorithms. The above-proposed work is especially helpful for applications where the task is time-sensitive or the data is highly confidential, requiring special infrastructure at industrial manufacturing sites. We intend to develop a simulated or layered architecture and then implement it as quantum cryptography in the field of industrial and heavy industrial manufacturing sites using real quantum hardware (by quantum infrastructure providers such as IBM Risk it, AWS, and S/4 HANA along with other digital tools to make sure the better production efficiency in the industrial sites) [8,31]. Quantum cryptography could save the most vital industrial product information, research and development information, product information and PIMs, and defense products related to key BOMs and components, as well as the most competitive challenges in qubits.

Declaration of Competing Interest

The authors declare that they have no conflict of interest.

References

[1] Z. Ding-yi, W. Peng, Q. Yan-li, F. Lin-Shen, Research on Intelligent Manufacturing System of Sustainable Development, in: Proceedings of the 2019 2nd World Conference on Mechanical Engineering and Intelligent Manufacturing (WCMEIM), 2019.
[2] D.J. Bernstein, Post-Quantum Cryptography, Springer, Fiji, 2022 December 8-10.
[3] M. Fei, Z. Haiou, W. Guilan, Application of industrial robot in rapid prototype manufacturing technology, in: Proceedings of the 2010 the 2nd International Conference on Industrial Mechatronics and Automation, 2010.
[4] C.H. Bennett, G. Brassard, Quantum cryptography: public key distribution and coin tossing, in: Proceedings of the IEEE International Conference on Computers Systems and Signal Processing, Bangalore, 1984, pp. 175–179.
[5] N.H. Mahmood, et al.: White paper on critical and massive machine type communication towards 6G (2020).
[6] K.O. Polyakov, N.G. Butakova, Comparative analysis of post-quantum key transfer protocols using mathematical modeling, in: Proceedings of the 2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), 2020.
[7] D. McMahon, Quantum cryptography, Quantum Computing Explained, IEEE, 2008.
[8] The IEE seminar on quantum cryptography: secure communications for business? - Title," 2005 The IEE Seminar on Quantum Cryptography: Secure Communications for Business (Ref. No. 2005/11310), 2005.
[9] V. Scarani, R. Renner, Quantum cryptography with finite resources: unconditional security bound for discrete-variable protocols with one-way postprocessing, Phys. Rev. Lett. 100 (20) (2008) 200501 May.
[10] D.P. DiVincenzo, The physical implementation of quantum computation, Fortschr. Phys. 48 (9–11) (2000) 771–783.
[11] A. Aji, K. Jain, P. Krishnan, A survey of quantum key distribution (QKD) network simulation platforms, in: Proceedings of the 2021 2nd Global Conference for Advancement in Technology (GCAT), 2021.
[12] C. Anghel, A. Istrate, M. Vlase, A comparison of several implementations of B92 quantum key distribution protocol, in: Proceedings of the 2022 26th International Conference on System Theory, Control and Computing (ICSTCC), 2022.
[13] H.H. Brunner, S. Bettelli, C.-H.F. Fung, M. Peev, Precise noise calibration for CV-QKD, in: Proceedings of the 2020 22nd International Conference on Transparent Optical Networks (ICTON), 2020.
[14] C.H. Bennett, Quantum cryptography using any two nonorthogonal states, Phys. Rev. Lett. 68 (21) (1992) 3121–3124 May.
[15] R. Lin, et al., Embedding quantum key distribution into optical telecom communication systems, in: Proceedings of the 2019 21st International Conference on Transparent Optical Networks (ICTON), 2019.

[16] S. Wengerowsky, S.K. Joshi, F. Steinlechner, H. Hübel, R. Ursin, An entanglement-based wavelength multiplexed quantum communication network, in: Proceedings of the 2019 Conference on Lasers and Electro-Optics Europe & European Quantum Electronics Conference, CLEO/Europe-EQEC, 2019.
[17] M. Nielsen, I. Chuang, Quantum Computation and Quantum Information, Cambridge University Press, Cambridge, 2000.
[18] W. Stallings, Cryptography and Network Security Principles and Practice, Prentice Hall, 2011.
[19] S. Fadli, BS. Rawal, Hybrid quantum-classical machine learning for near real-time space to ground communication of ISS lightning imaging sensor data, in: Proceedings of the 2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC), IEEE, 2023, pp. 0114–0122.
[20] S. Fadli, B.S. Rawal, Quantum bionic advantage on near-term cloud ecosystem, Optik 272 (2023) 170295.
[21] M. Aspelmeyer, T. Jennewein, M. Pfennigbauer, WR. Leeb, A. Zeilinger, Long-distance quantum communication with entangled photons using satellites, IEEE J. Sel. Top. Quantum Electron. 9 (6) (2003) 1541–1551.
[22] Z. Zhang, Qi Zhao, M. Razavi, X. Ma, Improved key-rate bounds for practical decoy-state quantum-key-distribution systems, Phys. Rev. A 95 (1) (Jan. 2017).
[23] M. Lopes, N. Sarwade, On the performance of quantum cryptographic protocols SARG04 and KMB09, in: Proceedings of the 2015 International Conference on Communication, Information & Computing Technology (ICCICT), 2015.
[24] V. Krueckl, T. Kramer, Revivals of quantum wave packets in graphene, New J. Phys. 11 (9) (2009) Sept.
[25] M.G. de Andrade, W. Dai, S. Guha, D. Towsley, Optimal policies for distributed quantum computing with quantum walk control plane protocol, in: Proceedings of the 2021 IEEE International Conference on Quantum Computing and Engineering (QCE), 2021.
[26] K. Liang, L. Fang, W. Susilo, D.S. Wong, A ciphertext-policy attribute-based proxy Re-encryption with chosen-ciphertext security, in: Proceedings of the 2013 5th International Conference on Intelligent Networking and Collaborative Systems, 2013.
[27] R. Bin-bin Su, Y.-. Zhou, X.-. Zhou, B92 protocol analysis related to the same basis eavesdropping, in: Proceedings of the 2016 IEEE International Conference on Cloud Computing and Big Data Analysis (ICCCBDA), 2016.
[28] R. Shokri, M. Stronati, C. Song, V. Shmatikov, Membership inference attacks against machine learning models, in: Proceedings of the 2017 IEEE Symposium on Security and Privacy (SP, 2017, pp. 3–18, doi:10.1109/SP.2017.41.
[29] Guo, Daqiang, Ray Y. Zhong, Yiming Rong, and George GQ Huang. “Synchronization of shop-floor logistics and manufacturing under IIoT and digital twin-enabled graduation intelligent manufacturing system.” *IEEE Transactions on Cybernetics* (2021).
[30] I.B. Djordjevic, Hybrid DV-CV QKD outperforming existing QKD protocols in terms of secret-key rate and achievable distance, in: Proceedings of the 2019 21st International Conference on Transparent Optical Networks (ICTON), 2019.
[31] Biswaranjan Senapati, Bharat S. Rawal, Quantum Communication with RLP Quantum Resistant Cryptography In Industrial Manufacturing,Cyber Security and Applications, 2023, 100019, ISSN 2772-9184, doi:10.1016/j.csa.2023.100019.