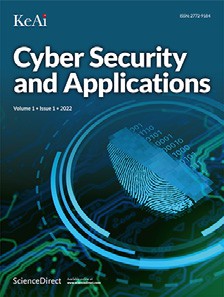
[Cyber Security and Applications 1 (2023) 100019](https://doi.org/10.1016/j.csa.2023.100019)

Contents lists available at [ScienceDirect](http://www.ScienceDirect.com/)

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](#_bookmark0), Bharat S. Rawal[b](#_bookmark1),[∗](#_bookmark2)

a *Computer Science Department, Capitol Technology University, Laurel, MD, USA*

b *Cybersecurity Department, Benedict College, Columbia, SC, USA*

a r t i c l e i n f o a b s t r a c t

*Keywords:* Cybersecurity Cryptography

Quantum Machine Learning RLP

Quantum Key Distribution Quantum cryptography

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.

# 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, Indus- trial manufacturing data(CAD, CAM, Manufacturing Products Informa- tion), 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 iden- tity, accessibility, and confidentiality guidelines within the manufactur- ing processing in industrial production sites [[1]](#_bookmark13).

In an industrial production operation, cryptography needs a public key infrastructure (PKI), which is the private root key that helps it op- erate within the units. It helps with user authentication, credential ver- ification, 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

∗ Corresponding author.

*E-mail address:* [bharat.rawal@benedict.edu](mailto:bharat.rawal@benedict.edu) (B.S. Rawal).

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 de- crypting the data from the communication media [[2](#_bookmark14)].

In a general statement, in the twenty-first century, most of the indus- trial 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](#_bookmark15)]. In manufacturing and in- dustrial facilities, data security and information exchange are key chal- lenges while dealing with day-to-day operational activities. Most indus- trial operations require the exchange of sensitive files from users to fac- tory 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 se- cure, confidential, integrity, and authenticated communications among the associated parties, whether internal or external [[4]](#_bookmark16). 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 the- ory." In quantum computing, communication theory can be the best op- tion to manage the best communication mechanism while dealing with Industry 4.0 [[5](#_bookmark17)].

<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

2772-9184/© 2023 The Authors. Published by Elsevier B.V. on behalf of KeAi Communications Co., Ltd. This is an open access article under the CC BY license (<http://creativecommons.org/licenses/by/4.0/>)

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 transac- tions, 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](#_bookmark18)]. It would be ideal to have cipher trust transparent encryption in the S/4 Hana system to protect and safe- guard enterprise data and transactions in order to meet information se- curity 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](#_bookmark19)].

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 encryp- tion keys known only to senders and receivers is quantum key distri- bution (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 commu- nication information between senders and receivers. QKD has two key players (parties): the source and the destinations [[8](#_bookmark20)].

For secure communication, the QKD enables both parties to produce and share a common key that could be used to encrypt and decrypt mes- sages while establishing the communication mechanism in the commu- nication network at the network layer. In quantum cryptography, quan- tum 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](#_bookmark21)].

From a conventional key distribution standpoint, quantum commu- nications 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 unau- thorizedly access the data in the same way as per quantum laws [[10](#_bookmark22)].

The following is how the rest of the paper is structured: The introduc- tion is covered in section I, and the related work is covered in section II. Then, section III describes quantum cryptography’s application in indus- trial manufacturing. Section IV describes facts on quantum key distribu- tion. 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 dis- tribution. Finally, section IX concludes the research paper.

# Related works

According to the quantum business report, venture capital financiers invested approximately US$ 147 million in quantum computing start- ups and governments worldwide in January 2019. Since 2017, they have also funded US$ 2.2 billion in research and development assis- tance. Quantum cryptography is a technique used to secure confiden- tial 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 abil- ity to offer security across the communication layer in the network as a

service; it integrates both hardware and software technologies in any en- vironment [[11](#_bookmark23)]. It is universally used in industrial automation, produc- tion, 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](#_bookmark24),[13](#_bookmark25)] is a well-known illustration of a DV- QKD[28] protocol, whereas Gaussian modulated coherent state CV- QKD [[13](#_bookmark25)] 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]](#_bookmark16), quantum key distribution (QKD) [[13](#_bookmark25)], and coherent one-way (COW) [[4](#_bookmark16),[14](#_bookmark26)], where the key information is only stored on the phase shift between two adja- cent poorly cohesive pulses and the photon arrival rate in both places.

Beyond these conventional protocols, there have been significant re- cent developments in QKD, most notably the proposed measurement- device-independent (MDI) QKD [[6](#_bookmark18)] (see also [[7](#_bookmark19)]) and the so-called Robin-Round (RR) DPS QKD protocol, which eliminates the need to monitor signal disturbance to establish security [[15](#_bookmark27)]. While the latter has an extremely high noise tolerance, the former offers a useful tech- nique 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](#_bookmark23)] and Photonic integration could be more beneficial and useful in industrial operations.

# Quantum cryptography’s application in industrial manufacturing

In Industry 4.0, the industrialization of smart metering and smart fac- tories is highly demanded as compared to the traditional way of manag- ing 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](#_bookmark22)]. All these industrial equipment and communication de- vices 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 ex- tra 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 quan- tum communication theory [[16](#_bookmark28)]. It can be achieved through information security, data protection, availability, and ultimately operational secu- rity 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 manufactur- ing 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 in- dustrial sites.
  + Exchange of test data and information across the industrial produc- tion sites and restricted test zone.
  + Production Pipeline data and future demand by manufacturing exe- cution 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](#_bookmark22)]. 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 plan- ning concerning the production order, make-to-order, make-to-stock, and order fulfillment scenarios [[10,17,18](#_bookmark22)]. 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 in- dustrial operation. They successfully demonstrated the customized ver- sion of the BB84 protocol. When considering a defense or critical in- dustrial product, quantum cryptography is the most important and crit- ical for industrial operational planning [[18](#_bookmark30)]. Hybrid quantum-classical machine learning is used for near real-time space-to-ground communi- cation of ISS lightning imaging sensor data [[19](#_bookmark32)]. Fadli and Rawal ex- plored the practical realities of both quantum sensing for ultrasensitive measurements and quantum communications to provide unparalleled security, data rates, and eﬃciency [[20](#_bookmark33)].

# 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 meth- ods to protect the data privacy, security, accessibilities, confidentiality, and availability of information to authorize resources in a digital man- ufacturing environment and would be best practices in industrial oper- ation within Industry 4.0 [[21](#_bookmark36),[14](#_bookmark26),[22](#_bookmark37)]. 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 with- out 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 per- form the superposition.

The QKD works by the philosophy of particles, photons, and light particles, or over the optic fibers to establish the communication mecha- nism 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](#_bookmark20),[11](#_bookmark23)]. 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 lin- early 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 encryp- tion systems. A beam splitter is an optical device that divides light into transmitted and reflected beams [[6](#_bookmark18)].

* + 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 es- tablish a fair coin-flipping relationship. All these parties are not physi- cally 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 algo- rithm can build a cryptographic protocol to establish computer security and network security [[23](#_bookmark38)].

* + 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](#_bookmark29)], 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 hon- estly follows the protocol [[24](#_bookmark39)].

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 in- formation over the classical channel to ensure Bob measured correctly. Then Alice and Bob confirm all the choices made for a few of the cir- cuits 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.

a |1⟩ state in the “Z” basis or the |+⟩ or |−⟩ state in the X-basis. Alice The BB84 protocol uses single qubits that can be in either a |0⟩ or

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 mea- surement 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 |+⟩ state and Bob

chooses to measure between 2 bases, so she has a 1 chance of picking measured on the X-basis, a “0″ would be added to the key. [[21](#_bookmark36)] Alice

2

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*) × (*𝐵𝑜𝑏 𝑠𝑎𝑚𝑒 𝑏𝑎𝑠𝑖𝑠*)

*𝑃 𝑐𝑜𝑟𝑟𝑒𝑐𝑡* = 1∕2 ×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* inf *𝑖𝑙𝑡𝑟𝑎𝑡𝑒* = (*𝐴𝑙𝑖𝑐𝑒𝑏𝑎𝑠𝑖𝑠*) × (*𝐸𝑣𝑒𝑏𝑎𝑠𝑖𝑠*)

*𝑃* inf *𝑖𝑙𝑡𝑟𝑎𝑡𝑒* = (1∕2) × (1∕2) = (1∕4)

# 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∗

[] = Generate NS Sequence; Input: p,q are two unique large prime numbers NS\_seq

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 ele-

ment 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 ex-

ample sample sequences listed in [Fig. 2](#_bookmark4) & [3](#_bookmark6).

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

# Cryptography and QKD

The QKD has the following facts and opportunities within the indus- trial manufacturing business

* + Prepare-and-measure protocols: This is mostly useful for measuring unknown quantum states. Universally used in the detection of eaves- dropping 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 eavesdrop- per accesses a previously trusted node and changes something, the other involved parties will know [[25](#_bookmark40)].
  + 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](#_bookmark25)]. 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 in- put. Quantum Coin Flipping and Quantum commitment are the best examples.
  + BNQSM: Works on commitment and unforgettable transfer proce- dure, 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](#_bookmark29)].
  + DIQC: It is device independent and very noisy.

In Quantum Communication theory and system, these are few quan- tum 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.

state with two polarization states (i.e., |H *>*, |V *>*, |45° *>*, |135° *>*) This protocol can produce four states that can be part of a quantum

[[4,14,21](#_bookmark16)]. 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](#_bookmark24),[27](#_bookmark31)]. The formula for this protocol is stated below.

*𝜑𝑗 >*= *𝛽*|0*𝑥 >* +(−1) *𝑗𝛼*|1*𝑥 >* [[22](#_bookmark37)]

Where *j* = {0,1}, {|0*x >*,|1*x >*} are the eigenstates of the *X* basis and

*𝛽* = cos *𝜃* 2 , *𝛼* = sin *𝜃* 2 [[4](#_bookmark16),[14](#_bookmark26),[22](#_bookmark37)].

* + 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 un- biased bases. Due to the possible distance between Alice and Bob, this protocol allows more noise in the transmission line without any inter- mediate nodes [39].

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

Below [Fig. 6](#_bookmark11) represents the type of attack along with the industrial device’s parameter.

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

# TS-quantum key distribution (TS-QKD)

The time sensitive QKD is the synergy between time sensitive net- working (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 com- munication cloning quantum states, and that is one of the greatest fea- tures 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 so- lutions
  + Deterministic (TSN-enforced) flow patterns with nanosecond resolu- tion
  + 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 in-

dustrial network, IIoT, equipment, and data center to reduce the cy- bersecurity attack surface by restricting cyber traﬃc injections. Essen- tially it is the most cost-effective solution for the measurement-device- independent (MDI) QKD ([Figs. 1](#_bookmark5), [3](#_bookmark6), [4](#_bookmark7), [5](#_bookmark8), [7](#_bookmark7), [8](#_bookmark9), [9](#_bookmark10), [10](#_bookmark12), [Tables 1–4](#_bookmark3)).

# Challenges of QKD

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

**Table 1**

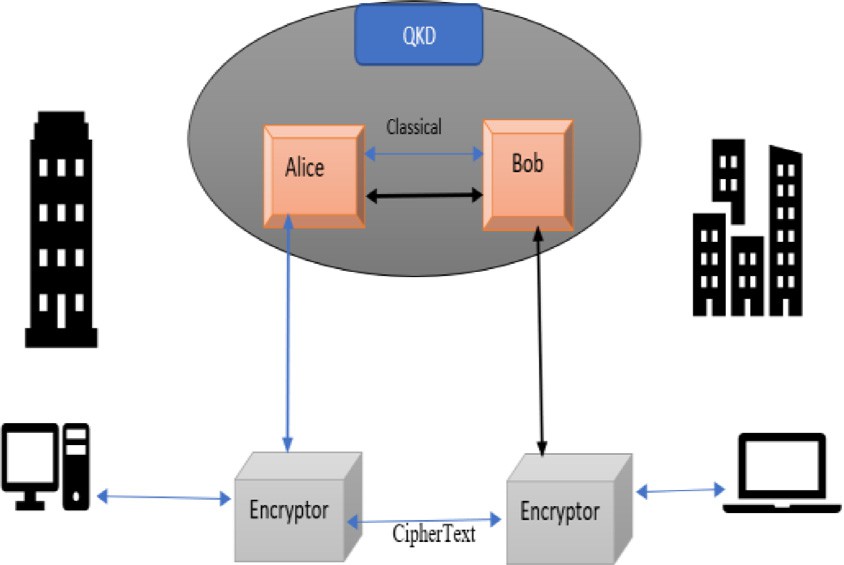
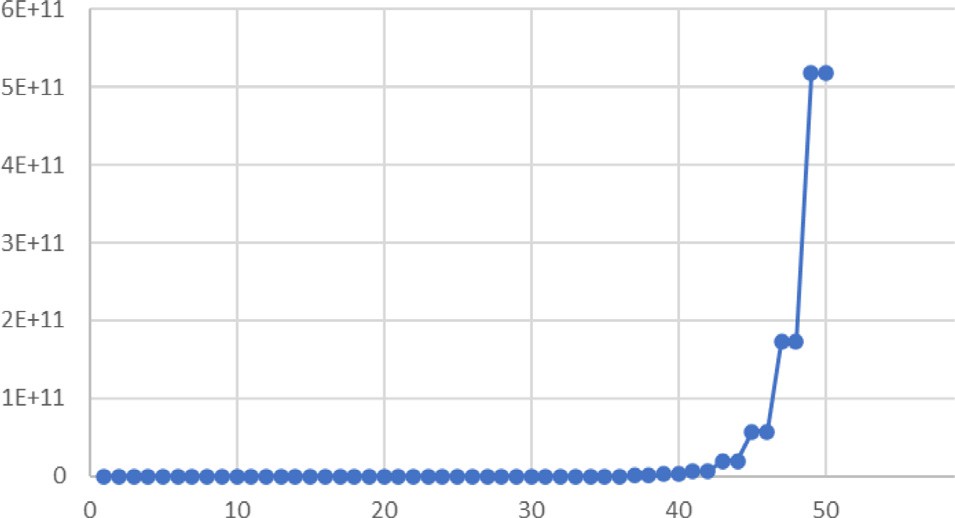
Quantum computing cryptography service provider around globe.

|  |  |  |
| --- | --- | --- |
| 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.

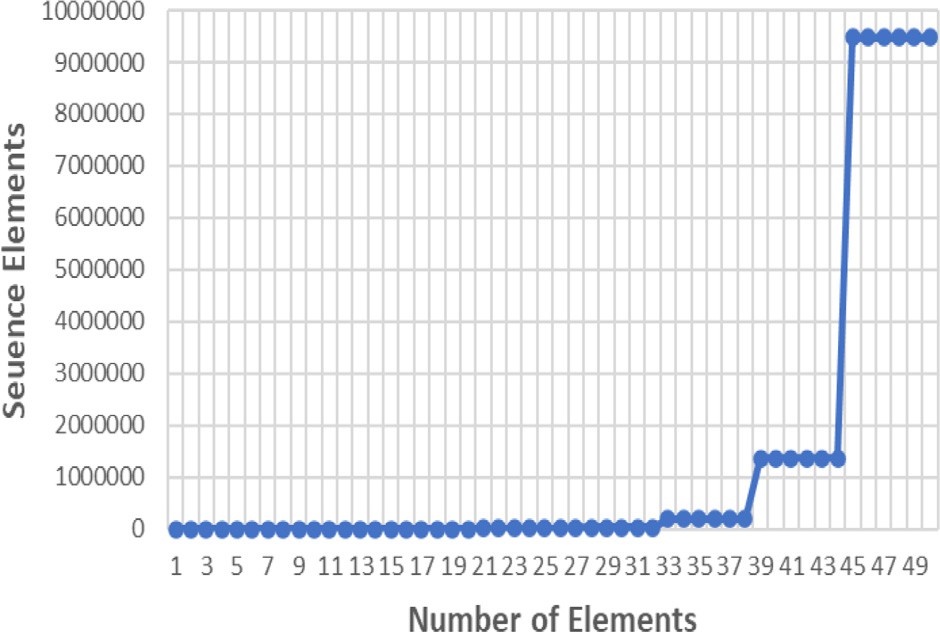
**Table 3**

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 |

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,

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

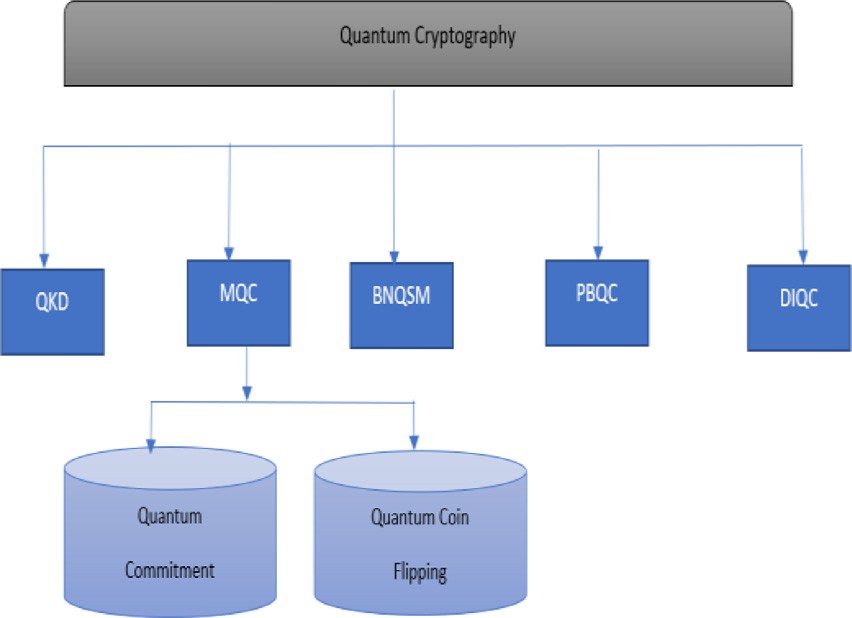
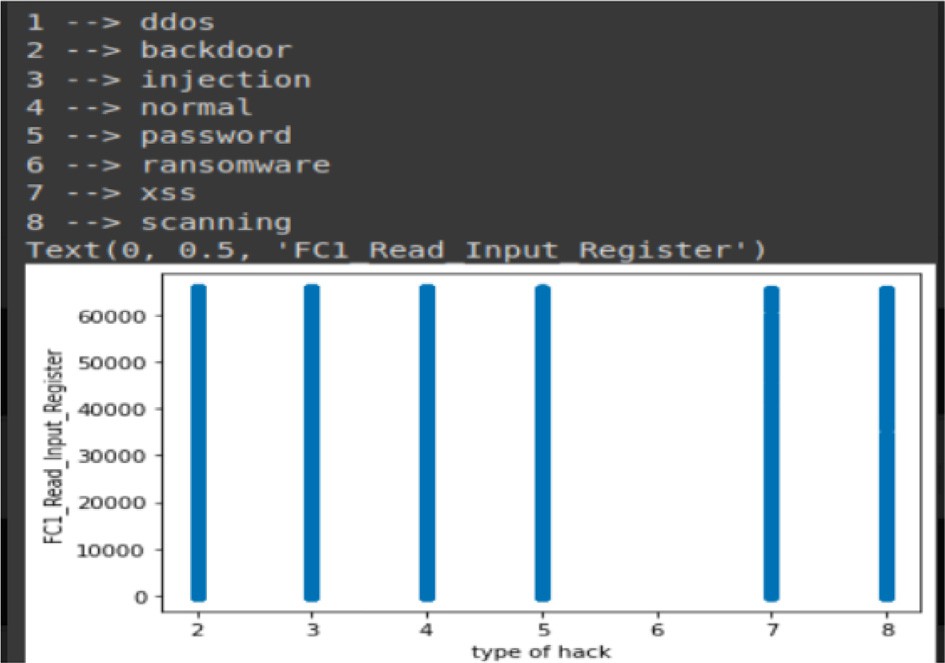


**Fig. 3.** RLP sequence with starting element numerical value 7.

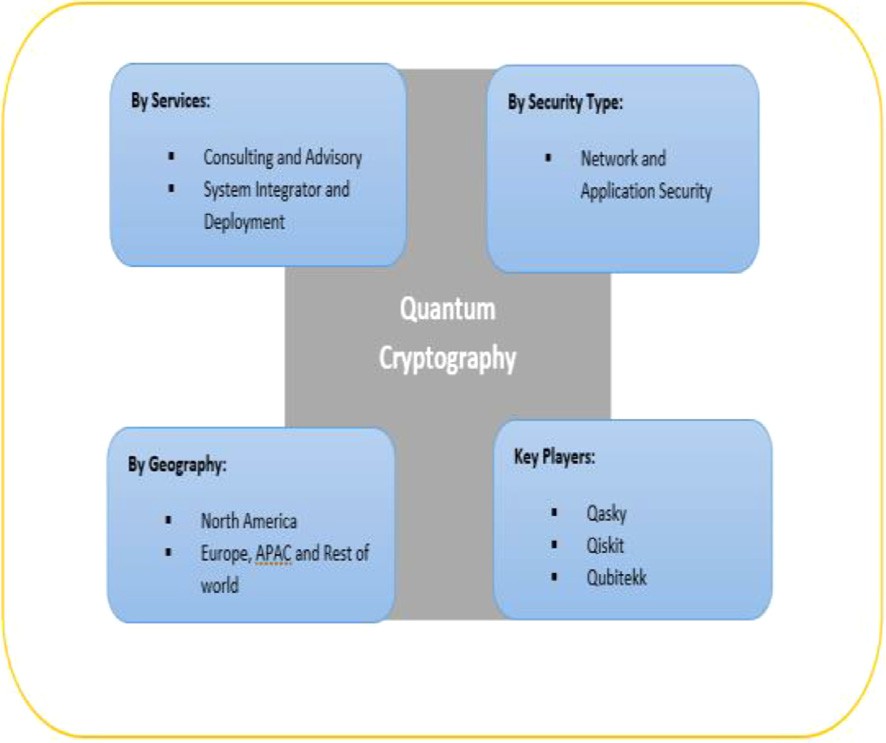
**Table 4**

Quantum algorithm and industries.

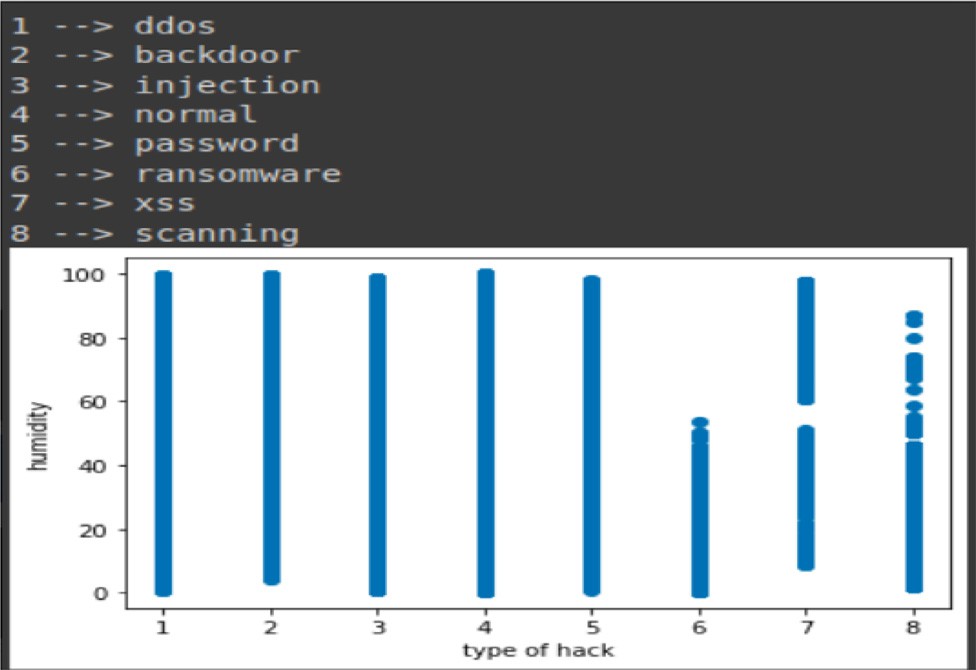
|  |  |  |
| --- | --- | --- |
| Quantum Computing Models | Useful | Industries |
| Shor’s Algorithm | Solves the discrete logarithm problem and the integer factorization problem in polynomial time | Finance and Banking Industrial Applications |
| Grover’s Algorithm | Especially searches an unstructured 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.

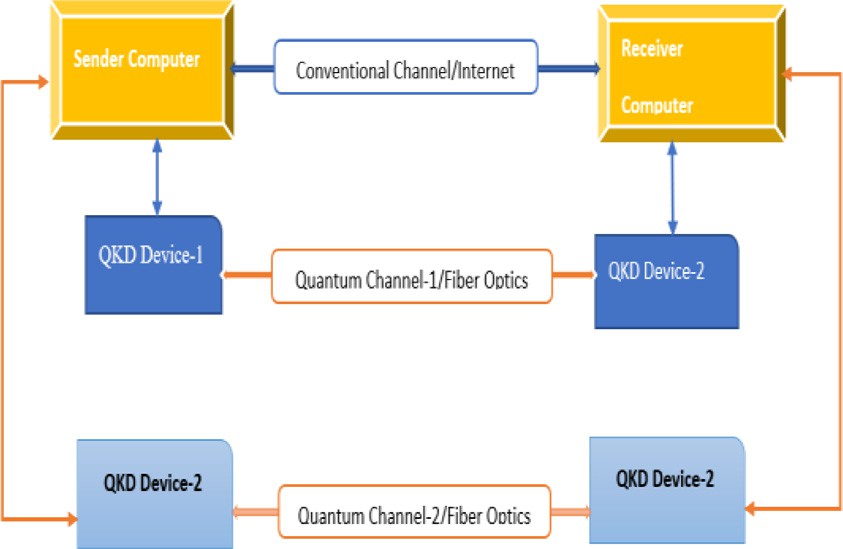


**Fig. 6.** Comparison of various attacks along with register inputs.

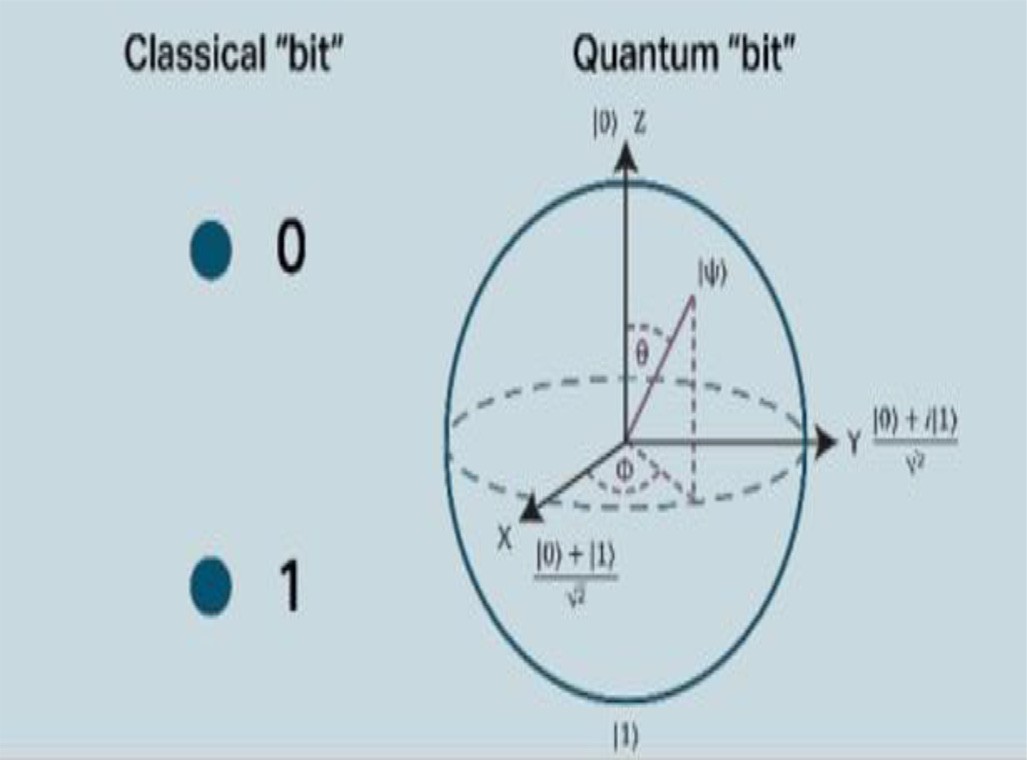
and cost factors. While considering practical network security within the QKD, it is advisable to consider the Device independent (DI), MDI- QKD, and network- QKD as the best practice to implement [[8](#_bookmark20)]. There are three main challenges concerning implementing the QKD into practice.

* 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.

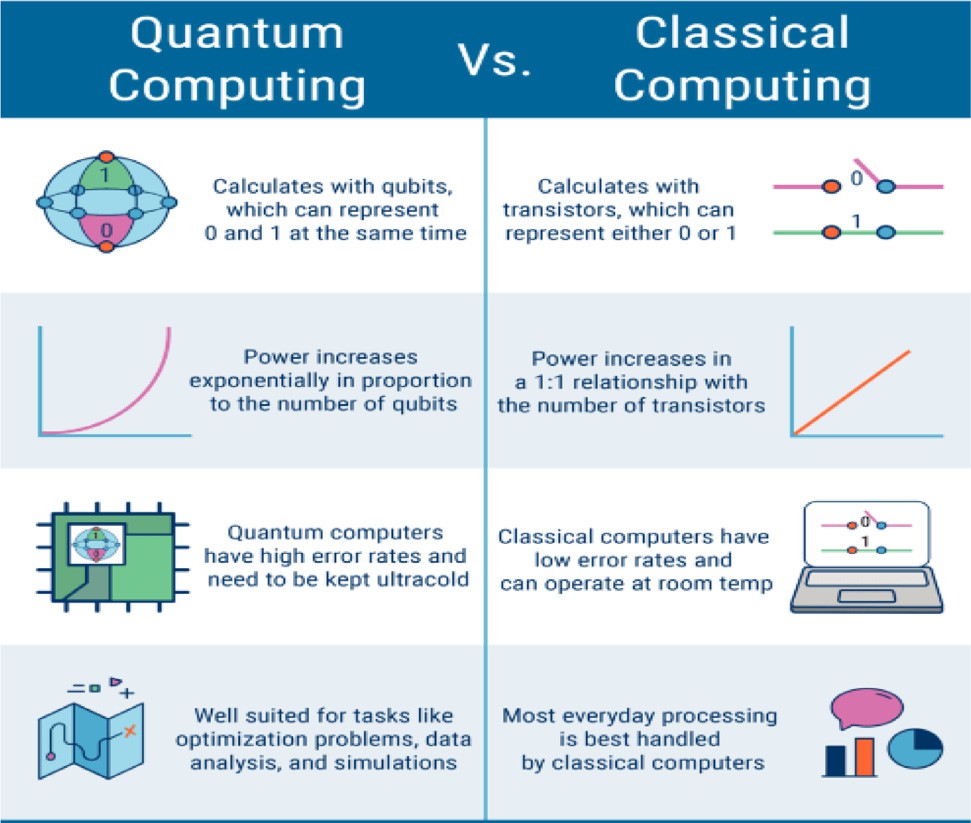


**Fig. 8.** Quantum Communications and Optical Network.



**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 com- patibility of various real-world solutions. This article examines previ- ously used methodologies, demonstrating how to set up QKD networks and outlining the current diﬃculties with QKD networking. This analy- sis examines the network aspect by taking into account network organi- zation, 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 Comput- ers:

In the computational world, there are a few key differences be- tween 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 commu- nication information sciences to solve a real-world problem.

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

# Conclusion

This paper focuses on the implications of advanced technologies, dig- ital twins, and the application of quantum cryptography in industrial operations, where quantum key distribution (QKD) protects smart facto- ries, 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, in- formation, 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](#_bookmark25)].

Quantum cryptography could save the most vital industrial product information, research and development information, product informa- tion and PIMs, and defense products related to key BOMs and compo- nents, as well as the most competitive challenges in qubits. Quantum computing and communications applications are used in industrial man- ufacturing facilities where key data, information, and sensitive indus- trial 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 ad- dressed, and the opportunity for quantum communication was handled in this article [[28](#_bookmark34)].

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 pro- tect industrial production sites [[29](#_bookmark35)]. 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 op- timize digital transformation best practices within Industry 4.0 [[8,30](#_bookmark20)]. 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 con- fidential 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 algo- rithms. The above-proposed work is especially helpful for applications where the task is time-sensitive or the data is highly confidential, re- quiring special infrastructure at industrial manufacturing sites. We in- tend to develop a simulated or layered architecture and then implement it as quantum cryptography in the field of industrial and heavy indus- trial manufacturing sites using real quantum hardware (by quantum in- frastructure 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](#_bookmark20)]. Quantum cryptography could save the most vital industrial product information, research and development infor- mation, 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 Confer- ence on Mechanical Engineering and Intelligent Manufacturing (WCMEIM), 2019.](http://refhub.elsevier.com/S2772-9184(23)00007-3/sbref0001)
2. [D.J. Bernstein, Post-Quantum Cryptography, Springer, Fiji, 2022 December 8-10](http://refhub.elsevier.com/S2772-9184(23)00007-3/sbref0012).
3. [M. Fei, Z. Haiou, W. Guilan, Application of industrial robot in rapid prototype man- ufacturing technology, in: Proceedings of the 2010 the 2nd International Conference on Industrial Mechatronics and Automation, 2010.](http://refhub.elsevier.com/S2772-9184(23)00007-3/sbref0023)
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.](http://refhub.elsevier.com/S2772-9184(23)00007-3/sbref0004)
5. N.H. Mahmood, et al.: White paper on critical and massive machine type communi- cation 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 Confer- ence of Russian Young Researchers in Electrical and Electronic Engineering (EICon- Rus), 2020.](http://refhub.elsevier.com/S2772-9184(23)00007-3/sbref0030)
7. [D. McMahon, Quantum cryptography, Quantum Computing Explained, IEEE, 2008](http://refhub.elsevier.com/S2772-9184(23)00007-3/sbref0031).
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.](http://refhub.elsevier.com/S2772-9184(23)00007-3/sbref0006)
10. [D.P. DiVincenzo, The physical implementation of quantum computation, Fortschr. Phys. 48 (9–11) (2000) 771–783.](http://refhub.elsevier.com/S2772-9184(23)00007-3/sbref0014)
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 Ad- vancement in Technology (GCAT), 2021.](http://refhub.elsevier.com/S2772-9184(23)00007-3/sbref0024)
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.](http://refhub.elsevier.com/S2772-9184(23)00007-3/sbref0025)
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.](http://refhub.elsevier.com/S2772-9184(23)00007-3/sbref0026)
14. [C.H. Bennett, Quantum cryptography using any two nonorthogonal states, Phys. Rev. Lett. 68 (21) (1992) 3121–3124 May.](http://refhub.elsevier.com/S2772-9184(23)00007-3/sbref0005)
15. [R. Lin, et al., Embedding quantum key distribution into optical telecom communi- cation systems, in: Proceedings of the 2019 21st International Conference on Trans- parent Optical Networks (ICTON), 2019.](http://refhub.elsevier.com/S2772-9184(23)00007-3/sbref0029)
16. [S. Wengerowsky, S.K. Joshi, F. Steinlechner, H. Hübel, R. Ursin, An entanglemen- t-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.](http://refhub.elsevier.com/S2772-9184(23)00007-3/sbref0021)
17. [M. Nielsen, I. Chuang, Quantum Computation and Quantum Information, Cambridge University Press, Cambridge, 2000.](http://refhub.elsevier.com/S2772-9184(23)00007-3/sbref0015)
18. [W. Stallings, Cryptography and Network Security Principles and Practice, Prentice Hall, 2011.](http://refhub.elsevier.com/S2772-9184(23)00007-3/sbref0016)
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: Proceed- ings of the 2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC), IEEE, 2023, pp. 0114–0122.](http://refhub.elsevier.com/S2772-9184(23)00007-3/sbref0032)
20. [S. Fadli, B.S. Rawal, Quantum bionic advantage on near-term cloud ecosystem, Optik 272 (2023) 170295.](http://refhub.elsevier.com/S2772-9184(23)00007-3/sbref0033)
21. [M. Aspelmeyer, T. Jennewein, M. Pfennigbauer, WR. Leeb, A. Zeilinger, Long-dis- tance quantum communication with entangled photons using satellites, IEEE J. Sel. Top. Quantum Electron. 9 (6) (2003) 1541–1551.](http://refhub.elsevier.com/S2772-9184(23)00007-3/sbref0003)
22. [Z. Zhang, Qi Zhao, M. Razavi, X. Ma, Improved key-rate bounds for practical de- coy-state quantum-key-distribution systems, Phys. Rev. A 95 (1) (Jan. 2017).](http://refhub.elsevier.com/S2772-9184(23)00007-3/sbref0009)
23. [M. Lopes, N. Sarwade, On the performance of quantum cryptographic protocols SARG04 and KMB09, in: Proceedings of the 2015 International Conference on Com- munication, Information & Computing Technology (ICCICT), 2015.](http://refhub.elsevier.com/S2772-9184(23)00007-3/sbref0013)
24. [V. Krueckl, T. Kramer, Revivals of quantum wave packets in graphene, New J. Phys. 11 (9) (2009) Sept.](http://refhub.elsevier.com/S2772-9184(23)00007-3/sbref0010)
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.](http://refhub.elsevier.com/S2772-9184(23)00007-3/sbref0020)
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 In- ternational Conference on Intelligent Networking and Collaborative Systems, 2013.](http://refhub.elsevier.com/S2772-9184(23)00007-3/sbref0022)
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.](http://refhub.elsevier.com/S2772-9184(23)00007-3/sbref0027)
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](https://doi.org/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 grad- uation 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 Interna- tional Conference on Transparent Optical Networks (ICTON), 2019.](http://refhub.elsevier.com/S2772-9184(23)00007-3/sbref0028)
31. Biswaranjan Senapati, Bharat S. Rawal, Quantum Communication with RLP Quan- tum Resistant Cryptography In Industrial Manufacturing,Cyber Security and Appli- cations, 2023, 100019, ISSN 2772-9184, doi:[10.1016/j.csa.2023.100019](https://doi.org/10.1016/j.csa.2023.100019).