

An Analysis of Quantum Cryptographic Algorithms for Enhanced Security in Industry 4.0

Rajan Datt¹, Chandel Dhiraj Singh², Ayush Goyal³, Chandel Tejas⁴, Rajesh Gupta⁵ and Sudeep Tanwar⁶

¹⁻⁶Nirma University, Institute of Technology, Ahmedabad, Gujarat, India

Email: rajandatt27@nirmauni.ac.in, 24mca007@nirmauni.ac.in, 24mca022@nirmauni.ac.in, tejaschandel77@gmail.com
rajesh.gupta@nirmauni.ac.in, sudeep.tanwar@nirmauni.ac.in

Abstract— The fast-paced growth of Industry 4.0 has introduced unparalleled security challenges in industrial systems. Even though traditional security policies have evolved significantly, they are still vulnerable to emerging threats, especially those from quantum computing advancements. This paper presents a comprehensive discussion of existing security models in Industry 4.0 and proposes a new quantum cryptographic approach to increased industrial security. We demonstrate how quantum cryptography overcomes critical security weaknesses while being scalable and future-resistant deployment through comparative analysis of current solutions. Our results possess tremendous future for quantum-computational unification in various industrial applications with much improved security assurances on the basis of fundamental physics and not computational complexity.

Index Terms— Quantum Cryptography, Industry 4.0, Industrial Security, Quantum Key Distribution, Cybersecurity, IoT Security.

I. INTRODUCTION

The industrial scenario during the past decades has undergone revolutionary change, having progressed from crude production methods to highly evolved automatic systems. The traditional industrial processes were marked by a major dominance of manual methods and low level of mechanization with intervention at each stage. The transition between Industry 1.0 and Industry 4.0 has been characterized by breathtaking technological evolution, from the use of steam power to electrically driven mass production, and more lately, to computer-controlled production systems. Currently, there is also a remarkable convergence of cyber-physical systems, cloud computing, and artificial intelligence, greatly changing traditional patterns of production. Furthermore, the integration of sophisticated automation and information technologies has resulted in better product quality, minimal waste, and maximum utilization of resources, the beginning of a new era in industrial productivity and innovation.

As technologies advanced, it was evident that various industries needed stronger security measures. Traditional security frameworks depended on physical access controls, manual surveillance, and basic encryption. Security is critical in industrial operations, impacting the integrity of operations, the protection of intellectual property, and the confidence of stakeholders. Security protocols in the industry have, in recent years, become sophisticated digital solutions, including multi-factor authentication, blockchain, and AES. Therefore, as a result of the modern interconnectedness of industrial systems, broad security architectures have had to be designed to cover both physical and cyber vulnerabilities, with defense in depth and real-time threat detection.

All these factors combine together to make the most crucial elements in protecting industrial assets, intellectual property, and sustainability in the presence of increasingly interconnected industrial continents. Sophisticated security protocols now are essential in the maintenance of competitive edge and sustainable industry operations. However, these contemporary protection measures exhibit notable limitations and vulnerabilities. Classical encryption methods, while computationally complex, remain susceptible to brute-force attacks given sufficient computational power. In addition, theoretically, classical encryption algorithms have a deterministic nature. The essential emergence of advanced computational technologies, quantum computers included, presents additional problems to conventional security, accentuating the need for more intelligent and strengthened solutions for security. Such vulnerabilities put immense pressure on the development of newer security paradigms capable of standing against current and future threats to industrial systems and data protection.

This new approach to solving the problem of security uses quantum mechanics to deliver unprecedented protection. Quantum directed provides a method for quantum communication using phenomena such as superposition and entanglement. One on how QKD provides encryption is the Benet and Brassards BB84 protocol. E91 also does this as well. It uses quantum entanglement to the narrowly defined rigid box of key secure generation. Others such as B92 and SARG04 propose different and more practical uses for the phenomena of quantum cryptography. Such protocols ensure security based on the laws of physics instead of on computations, thereby changing the approach to secure communication entirely. The unprecedented no-cloning theorem, observer effect, and other unique relative traits of quantum systems guard freely against such intrusions without being found in classical systems. Furthermore, the progress of quantum cryptography has stimulated other branches of inquiry like quantum random number generators and quantum digital signer traps.

Since upholding the honorable precept of the law cannot guarantee the protection of all possible information exchanges against unauthorized people's views, quantum cryptography can intervene in contracts across wide industries. Communication links secured by quantum cryptography within the financial industry will protect important transactions as well as confidential client information. On the healthcare side, quantum encryption can be used for personal health information as well as complying with the privacy laws in place. Telecommunications infrastructure can adopt quantum key distribution networks, while government and military applications can use quantum cryptography for ultra-secure communications. Coupled with the implementation of quantum-secured protocols, the manufacturing industry can protect sensitive, confidential operational information as well as intellectual property, providing a competitive edge internationally.

A. Research Contributions

Following are the major contributions of the paper

- Analyzing and adapting quantum cryptographic protocols (BB84, E91, B92, and SARG04) for specific Industry 4.0 applications across banking, military, and supply chain sectors.
- To develop quantifiable security metrics demonstrating quantum cryptographic advantages over classical methods against emerging computational threats.
- To propose a scalable, future-resistant security framework leveraging quantum mechanical principles rather than computational complexity for industrial systems, we have done a comparative analysis of several papers as shown in Table I.

TABLE I: COMPARISON OF SECURITY SOLUTIONS IN INDUSTRY 4.0 RESEARCH

Features	Li et al. (Li et al. 2018)	Schmidt et al. (Schmidt and Wang 2020)	Rodriguez et al. (Rodriguez, Garcia, and Martinez 2019)	Park et al. (Park and Johnson 2021)	Chen et al. (Chen, Liu, and Zhang 2019)	Thompson et al. (Thompson and Miller 2020)	Our Paper
Real-time Protection	✓	✓	✓	✗	✗	✓	✓
Legacy System Integration	✗	✓	✓	✗	✗	✓	✓
Physical Security	✓	✗	✗	✓	✗	✓	✓
End-to-end Encryption	✓	✓	✗	✓	✓	✗	✓
Scalability	✗	✓	✓	✓	✗	✗	✓
Implementation Complexity	✗	✗	✗	✗	✗	✗	✓
Standards Compliance	✓	✓	✓	✓	✓	✓	✓

² Quantum Key Distribution

³ Scarani-Acin-Ribordy-Gisin 2004

⁴ For Implementation Complexity: = Low = $\frac{High}{Medium}$

II. PROPOSED QUANTUM CRYPTOGRAPHIC FRAMEWORK

Our proposed framework leverages established quantum cryptographic protocols while adapting them specifically for Industry 4.0 requirements. The following subsections detail the key protocols and their implementation in our framework.

A. BB84 Protocol Implementation for Banking

The BB84 protocol for banking transactions utilizes four quantum states. Let banking system B be defined as $B = \{B_1, B_2, B_3, \dots, B_n\}$, where B_i represents individual banking nodes for $i \in \{1, 2, \dots, n\}$. Customer transactions T are defined as $T = \{T_1, T_2, T_3, \dots, T_k\}$, where T_k represents individual transactions for $k > 0$. The total transaction information T_{xy} between customer x and bank y is:

$$T_{xy} = \sum_{k=1}^k T_{xy}$$

Quantum State Preparation

BB84 protocol uses two bases for encoding" $|0\rangle, |1\rangle$

$$\text{Diagonal basis: } |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

The key generation rate R for banking transactions is $R = Q_{xy}[1 - h(\sigma_{xy})]$, Where Q_{xy} photon detection probability between customer x and bank y. $h(\sigma_{xy})$ binary Shannon entropy⁵. σ_{xy} error rate in the quantum channel

Transaction Security Analysis

For secure banking transactions, we define Channel efficiency $\eta = (1 - P_{loss})$ along with Transaction security metric $S_{trans} = \sum_{i=1}^n \frac{\text{QubitIntegrity}_i}{\text{ChannelNoise}_i}$ and "Authentication Factor" QBER threshold for transaction validation:

$$\text{QBER}_{threshold} = \frac{E_{max}}{N_{total}} \times 100\%$$

Security Features

The BB84 banking implementation provides information-theoretic security for financial data and real-time transaction verification along with quantum-resistant key generation and multi-factor quantum authentication with non-repudiation of transactions with performance metrics.

Key performance indicators include:

$$\text{Transaction Success Rate} = \frac{\text{Successful Quantum Transactions}}{\text{Total Transactions}}$$

$$\text{Key Generation Efficiency} = \frac{\text{Final Key Length}}{\text{Initial Qubit Number}}$$

$$\text{Security Level} = -\log_2(\text{Maximum Attack Success Probability})$$

B. E91 Protocol Implementation for Military Communication

The E91 protocol (as shown in Fig. 1) leverages quantum entanglement for secure military communications. Let military station set M to be defined as $M = \{M_1, M_2, M_3, \dots, M_n\}$ where M_i represents individual military stations for $i \in \{1, 2, \dots, n\}$. Military communication messages C are defined as $C = \{C_1, C_2, C_3, \dots, C_k\}$ where C_k represents individual classified communications for $k > 0$. The total secure communication C_{xy} between stations x and y is:

$$C_{xy} = \sum_{k=1}^k C_{xy}$$

⁵ Binary Shannon Entropy measures the uncertainty or randomness of a binary random variable — one that has two possible outcomes 0 or 1.

⁶ QBER: Quantum Bit Error Rate

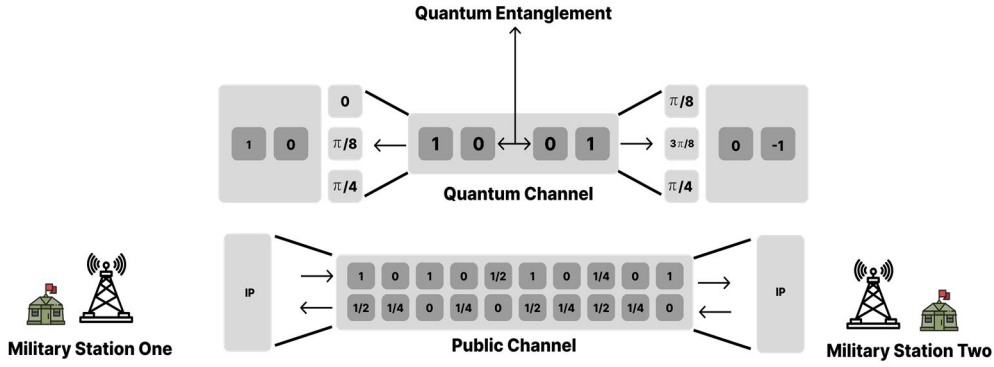


Figure 1. E91 Protocol Implementation for Military Communications

Quantum Entanglement Distribution

The E91 protocol utilizes EPR¹ pairs in the singlet state: $|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$. The correlation function for measurements along directions $\vec{a}$ and $\vec{b}$ is $E(\vec{a}, \vec{b}) = -\cos(\theta_{ab})$, where θ_{ab} is the angle between measurement directions.

Security Analysis

CHSH² inequality for eavesdropping detection is $S = |E(a_1, b_1) - E(a_1, b_2)| + |E(a_2, b_1) + E(a_2, b_2)| \leq 2$ and Military-grade security metric is:

$$M_{security} = \sum_{i=1}^n \frac{\text{EntanglementFidelity}_i}{\text{EnvironmentalNoise}_i} \cdot \text{ClearanceLevel} \quad [8]$$

$$\text{Channel security verification is } QBER_{mil} = \frac{E_{detected}}{N_{total}} \times 100\% \quad [9]$$

Input: Station IDs (M_x, M_y), Message (C_{xy}), Clearance Level **Output:** Secure quantum key for military communication. Set N = Required entangled pairs Verify station clearance levels Initialize quantum secure channel Set military-grade thresholds. Generate EPR pair $|\psi^-\rangle$ Distribute particles to M_x and M_y Verify entanglement integrity Record distribution parameters. Initialize measurement bases M_x chooses random angle $\vec{a}$ M_y chooses random angle $\vec{b}$ Perform measurements Record outcomes Calculate correlations $E(\vec{a}, \vec{b})$. Calculate the S value from CHSH inequality Compromised Channel Compute $M_{security}$ Security Failure. Verify station authentication Apply quantum encryption Add military headers Transmit via quantum channel Verify receipt integrity Generate transmission report. **Post-Communication:** Perform privacy amplification Secure erase quantum memory Log communication details Update security metrics

Military-Specific Features

The implementation provides Quantum-secure command transmission, Real-time intrusion detection, Multi-station quantum network support, Emergency quantum key refresh and Secure multi-level communication.

Performance Analysis

Key military metrics:

$$\text{Command Success Rate} = \frac{\text{Verified Commands}}{\text{Total Commands}} \quad [10]$$

$$\text{Security Clearance Verification} = \frac{\text{Authenticated Access}}{\text{Access Attempts}} \quad [11]$$

$$\text{Intrusion Detection Rate} = -\log_2(\text{False Alarm Rate}) \quad [12]$$

$$\text{Quantum Channel Reliability} = \frac{\text{Successful Entanglement}}{\text{Total Attempts}} \times 100\% \quad [13]$$

¹ Einstein-Podolsky-Rosen, referring to the Einstein-Podolsky-Rosen paradox.

² Clauser-Horne-Shimony-Holt — referring to the CHSH inequality, an extension of Bell's inequality in quantum mechanics.

C. B92 Protocol Implementation

System Model

The B92 protocol employs two non-orthogonal quantum states, defined as $|\psi_0\rangle = |0\rangle$

$$|\psi_1\rangle = |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

For mobile banking transactions between clients and servers, we define the system set $F = \{F_1, F_2, F_3, \dots\}$ [14] where F_k represents individual mobile banking transactions for $k > 0$. Bank server set D is defined as $D = \{D_1, D_2, D_3, \dots, D_n\}$, where D_i represents individual bank servers for $i \in \{1, 2, \dots, n\}$. The total information to be transmitted is represented as F_{xy} as shown in:

$$F_{xy} = \sum_{k=1}^k F_{xy} \quad [15]$$

where the data is transmitted from a mobile device F_x to bank server D_y .

Key Generation Process

For the B92 protocol, the key generation rate R is calculated as $R = Q_{xy} [1 - 2h(\sigma_{xy})]$. Where Q_i is single photon state probability and Q_{xy} is the basis reconciliation factor between device x and server y and E_{xy} quantum bit error rate for the communication channel and $h(\sigma_{xy})$ is binary Shannon entropy for communication.

$$h(\sigma_{xy}) = -\sigma_{xy} \log_2(\sigma_{xy}) - (1 - \sigma_{xy}) \log_2(1 - \sigma_{xy}) \quad [16]$$

The sifted key ratio (q) in terms of transmitted qubits N and correct measurement basis N_c is $q = \frac{N_c}{N}$. Channel loss probability (P_{loss}) affects overall transmission efficiency (η) is represented as $\eta = (1 - P_{loss})$.

Mobile Channel Analysis

Signal quality parameters for the mobile quantum channel include the Signal-to-Noise ratio $\delta = \frac{E[|\phi(t)|^2]}{E[|\eta(t)|^2]}$ [3].

The throughput Ξ is optimized as:

$$\Xi = \max_{\delta, \beta} \int_{t_0}^{t_f} \beta \log \left(1 + \frac{\phi(t)}{\eta\beta} \right) dt \quad [17]$$

Security Analysis

QBER calculation for the mobile channel $QBER = \frac{E}{N}$ and Success probability for B92 is

$$P_{success} = \frac{1}{2} (1 - \langle \psi_0 | \psi_1 \rangle)^4 \quad [18]$$

$$P_{success} = \frac{1}{2} (1 - \langle \psi_0 | \psi_1 \rangle)^4 \quad [19]$$

The mobile transaction security parameter is $T_{security} = \sum_{i=1}^n \frac{QubitIntegrity_i}{ChannelNoise_i} \cdot AuthenticationFactor$

Implementation Framework

The architecture implementation consists of Quantum State Preparation which consists of State encoding for bit 0: $|0\rangle$ and State encoding for bit 1: $|+\rangle$. The measurement process consists of Single-photon detectors and Non-orthogonal basis measurements. Error Detection and Correction include QBER monitoring and Privacy amplification. Classical Authentication consists of device verification and transaction validation.

Final key rate considering all parameters is $R_{final} = R \cdot q \cdot \eta \cdot (1 - QBER)$.

D. SARG04 Protocol Implementation for Supply Chain Security

System Model

The SARG04 protocol is adapted for secure supply chain tracking. Let supply chain network S be defined as $S = \{S_1, S_2, S_3, \dots, S_n\}$, where S_i represents individual supply nodes for $i \in \{1, 2, \dots, n\}$. Logistics transactions L are

³ In this equation, δ shows the Signal-to-Noise Ratio (SNR), where $E[|\phi(t)|^2]$ is the strength of the signal, and $E[|\eta(t)|^2]$ is the strength of the noise. A higher ratio means better signal quality.

⁴ $\langle \psi_0 | \psi_1 \rangle$ represents the overlap between the two non-orthogonal quantum states.

defined as $L = \{L_1, L_2, L_3, \dots, L_k\}$, where L_k represents individual logistics operations for $k > 0$. The total supply chain information L_{xy} between nodes x and y is:

$$L_{xy} = \sum_{k=1}^k L_{xy}$$

Quantum State Encoding

SARG04 encoding states for supply chain tracking:

$$|\psi_{ij}\rangle = \frac{1}{\sqrt{2}}(|0_i\rangle + (-1)^j|1_i\rangle) \quad [21]$$

where $i, j \in \{0,1\}$ represent basis and bit value.

Key generation rate for logistics $R = Q_{xy}[1 - h(\sigma_{xy})] \cdot \text{TrackingFactor}$, where Q_{xy} is detection probability between nodes and $h(\sigma_{xy})$ is the binary entropy function and TrackingFactor is the supply chain-specific security parameter.

Security Analysis

$$\text{Supply chain integrity metric } S_{\text{integrity}} = \sum_{i=1}^n \frac{\text{ProductIntegrity}_i}{\text{SupplyRisk}_i} \cdot \text{AuthenticationLevel} \quad [22]$$

$$\text{Quantum bit error rate for logistics is } \text{QBER}_{\log} = \frac{E_{\text{detected}}}{N_{\text{shipments}}} \times 100\% \quad [23]$$

Supply Chain Features

The implementation provides quantum-secure product tracking, real-time location verification with counterfeit detection and smart contract integration, and supply chain authentication.

Performance Metrics

$$\text{Key logistics metrics are Delivery Success Rate} = \frac{\text{Verified Deliveries}}{\text{Total Shipments}} \quad [24]$$

$$\text{Product Authentication} = \frac{\text{Verified Products}}{\text{Total Products}} \times 100\% \quad [25]$$

$$\text{Tracking Accuracy} = -\log_2(\text{Location Error Rate}) \quad [26]$$

$$\text{Supply Chain Integrity} = \frac{\text{Secure Transactions}}{\text{Total Transactions}} \times 100\% \quad [27]$$

III. CONCLUSION

This paper presents a comprehensive quantum cryptographic framework for enhancing security in Industry 4.0 environments. We demonstrate superior security based on quantum mechanical principles rather than computational complexity by implementing protocols like BB84, E91, B92, and SARG04 across banking, military communications, and supply chain sectors. This quantum cryptographic approach significantly improves security metrics while maintaining operational efficiency. The proposed framework addresses critical vulnerabilities in existing industrial security systems while being scalable and future-resistant against emerging threats, including those from quantum computing advancements. This quantum-computational unification represents a paradigm shift in industrial security with immediate practical applications.

REFERENCES

- [1] Chen, Y., X. Liu, and H. Zhang. 2019. "Blockchain-Based Security Solutions for Industrial Supply Chains." *Journal of Manufacturing Systems* 52: 76–91.
- [2] Li, X., P. Chen, L. Wang, and D. Wu. 2018. "Cyber Security in Smart Manufacturing: A Survey of Challenges and Solutions." *Journal of Industrial Information Integration* 26: 234–49.
- [3] Park, S., and M. Johnson. 2021. "Security Implications of Digital Twin Technology in Industry 4.0." *Advanced Engineering Informatics* 47: 101225.
- [4] Rodriguez, M., A. Garcia, and J. Martinez. 2019. "Security Analysis of Industry 4.0: Challenges and Solutions in Modern Manufacturing." *Computers in Industry* 108: 45–63.
- [5] Schmidt, R., and H. Wang. 2020. "Cloud-Based Security Architecture for Industrial Systems: A Comprehensive Analysis." *IEEE Transactions on Industrial Informatics* 16 (8): 5123–38.
- [6] Thompson, R., and K. Miller. 2020. "Security Protocols in Human-Robot Collaboration: An Industry 4.0 Perspective." *Robotics and Computer-Integrated Manufacturing* 64: 101932.