ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25feb845

Security and Efficiency in Quantum Key Distribution - A Comparative Analysis of Modern QKD Protocols

A. Johnbasco Vijay Anand[1]: Dr. S. Sukumaran[2]

[1] Ph.D. Research Scholar, Department of Computer Science, Erode Arts and Science College, Erode, TN, India,
[2] Associate Professor an Head, Department of Computer Science, Erode Arts and Science College, Erode 638009, TN, India,

Publication Date: 2025/04/28

Abstract: Quantum Key Distribution (QKD) addresses the critical challenge of unsafe key generation and ensures a secure communication channel by leveraging the fundamental principles of quantum mechanics. Unlike classical encryption methods, QKD provides an unbreakable security model by detecting any eavesdropping attempts through quantum state disturbances. This paper explores the security and efficiency of modern QKD protocols by analyzing their practical applications, theoretical foundations and comparative performance.

Keywords: *Quantum Cryptography, QKD, Relativistic QKD.*

How to Cite: A. Johnbasco Vijay Anand: Dr. S. Sukumaran (2025) Security and Efficiency in Quantum Key Distribution - A Comparative Analysis of Modern QKD Protocols. *International Journal Of Innovative Science and Research Technology*, 10(2), 2572-2578. https://doi.org/10.38124/ijisrt/25feb845

I. INTRODUCTION

Given that our current cryptographic[17] methods rely on computational complexity, it gets challenging and risky to secure communications against cyber threats[3] especially as the Quantum computers taking an enormous growth in the last couple of years. Quantum computers not just can challenge the existing leading cryptographic methods but also the current Public Key Infrastructures (PKI) in place.

Quantum Key Distribution (QKD) presents a revolutionary solution by utilizing the unique properties of quantum mechanics[2],[3] to generate and distribute encryption keys securely. By ensuring that any unauthorized attempt to intercept the key results in detectable quantum disturbances, QKD offers a level of security unparalleled by classical methods.

This paper provides an in-depth comparative analysis of various QKD protocols, focusing on their security mechanisms, efficiency and practical implementation challenges. Protocols such as BB84, E91, Continuous Variable QKD (CV-QKD)[20] and Relativistic [12] QKD are examined in detail. This comparative analysis and study aims to highlight the strengths and limitations of each protocol and explore their real-world applications in industries such as finance, healthcare and defense.

The paper also discusses the quantitative aspects of QKD performance, including key generation rates, quantum bit error rates (QBER) and security resilience[7] metrics. By analyzing current research and experimental data, we provide a comprehensive overview of the state-of-the-art QKD solutions and their future potential in ensuring secure communications [5] in an increasingly interconnected world.

II. OVERVIEW OF QKD PROTOCOLS

- *Several QKD protocols have been developed, each with unique features and security assurances. This section covers not just the most prominent protocols [6] but also those that has a wide range of research scope. The list of QKS that have been considered in scope of this paper are as below*

- *BB84 Protocol*:

The first QKD protocol, based on the polarization of photons, offering proven theoretical security.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25feb845

- *E91 Protocol*:
  Based on quantum entanglement[5] and Bell's inequalities, ensuring robust security.

- *Continuous Variable* QKD (CV-QKD)[20]:
  Uses amplitude and phase modulation of light, allowing compatibility with existing optical networks.

- *B92 Protocol:*
  A simplified QKD protocol using two non-orthogonal quantum states for secure key exchange with minimal photon resources.

- *SARG04 Protocol:*
  A variant of BB84 that enhances security against photon number splitting attacks by using a refined basis choice strategy.

- *Relativistic QKD*:
  Utilizes relativistic constraints to prevent interception, offering additional layers of security[12].

III. A CLOSER LOOK OF WHAT WHEN AND HOW OF QKD

QKD is a cryptographic protocol that enables two parties to generate a shared, secret random key, which can be used for subsequent encryption of messages. It utilizes quantum states[4], typically photons, to transmit key information. The most renowned QKD protocol is BB84, introduced by Bennett and Brassard in 1984, which employs the polarization states of photons to encode bits. In this paper we not just analyze BB84 protocol but a variety of modern day QKD.

Since 1980s, QKD has transitioned from theoretical concept to practical implementations. Today, it is deployed in various sectors requiring high-security communication, including governmental agencies, financial institutions and military operations. Notable implementations encompass both fiber-optic networks and free-space optical links, with successful demonstrations over metropolitan areas and even satellite-based communications.

- *Understanding How QKD works is crucial for this paper and is explained as below: QKD operates by transmitting quantum states (e.g., photons) over a communication channel. The fundamental steps includes the following:*

- *Preparation and Transmission:*
  The sender (Alice) encodes bits onto quantum states and transmits them to the receiver (Bob).

- *Measurement:*
  Bob measures the received quantum states using randomly chosen bases.

- *Sifting:*
  Alice and Bob communicate over a classical channel to determine which bits were measured in compatible bases.

- *Error Correction and Privacy Amplification:*
  They correct discrepancies and distill a secure key by reducing any partial information an eavesdropper might have gained.

IV. COMPARATATIVE ANALYSIS OF QKD PROTOCOLS

The efficiency and security of various QKD protocols are compared based on several performance metric. Each of the parameters (Metrics) listed below are considered on the basis of security and efficiency. These values are referenced from various research journals and the references are included in the appropriate sections:

- *Key Generation Rate:*
  It is the rate at which secure keys are generated when the respective QKD protocol is used. It actually refers to the number of secure key bits generated per second [8]. It depends on several factors, including the raw photon transmission rate, channel losses, quantum bit error rate (QBER)and the efficiency of error correction and privacy amplification.

Table (1) below provides the key rates of the respective protocols

Table 1 List of QKD with their Key Generation Rate

QKD	Key Generation rate (over 10 km)
BB84	10 kbps
E91	1 kbps
CV-QKD	20 kbps
B92	5 kbps
SARG04	9 kbps
Relativistic QKD	8 kbps

The key generation rate can be calculated using the formula:

$$\boldsymbol{R_{key} = R_{raw}.(1 - H(Q)) - leak_{ec}}$$

Where, $\boldsymbol{R_{key}}$ is Final secret key rate (bits per second).

$\boldsymbol{R_{raw}}$. is the Raw key rate (bits per second) before error correction and privacy amplification.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25feb845

$\boldsymbol{H(Q)}$ Binary entropy of the QBER (Q), calculated as

$$\boldsymbol{H(Q) = -Q.\log_2(Q) - (1-Q)\cdot \log_2(1-Q)}$$

And $\boldsymbol{leak_{ec}}$ is the leakage due to error correction (typically a fraction of the raw key rate).

Based on the above calculations, Fig (A) was generated which highlights the Key generation rates for the six QKDs that are considered for the comparative study in this paper.

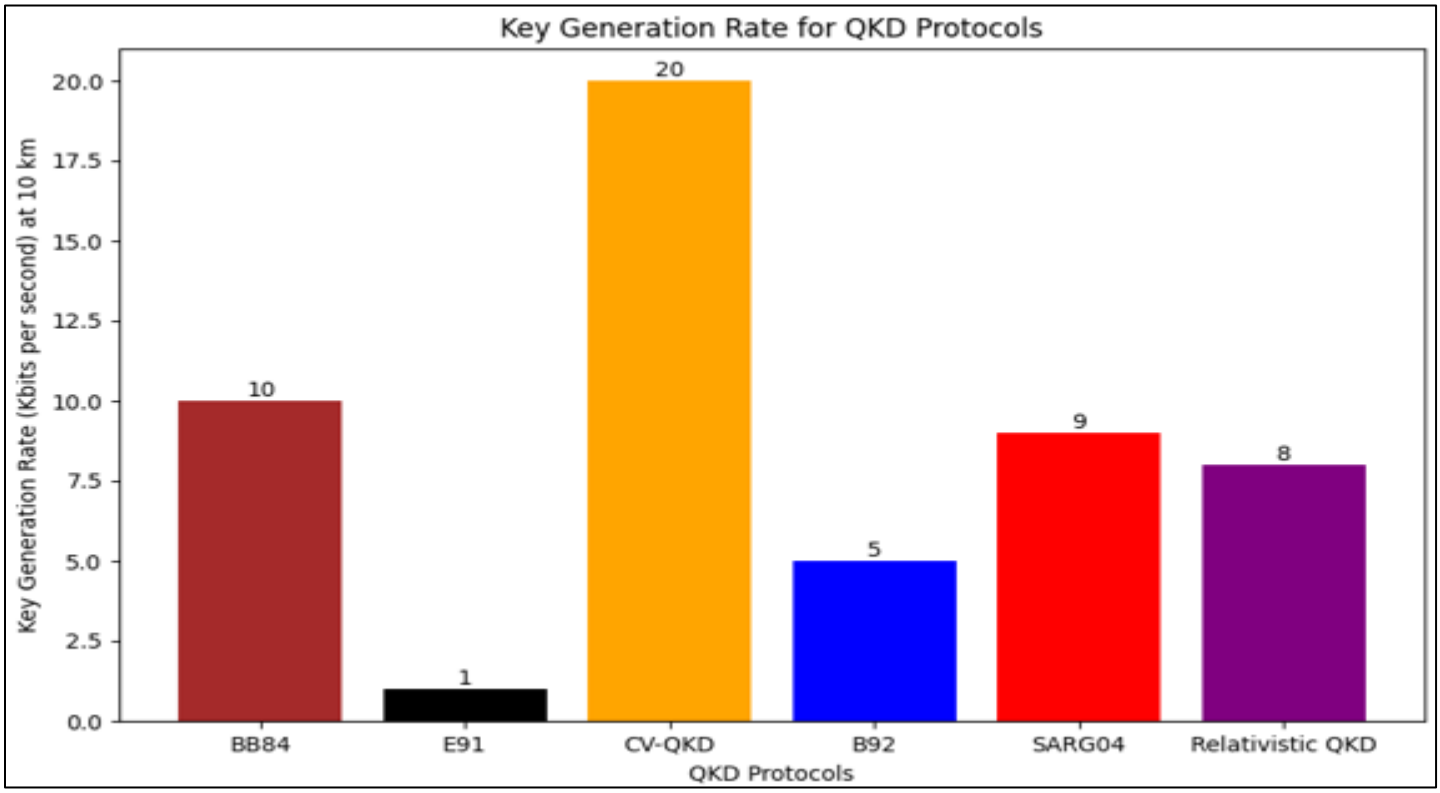

Fig 1 Illustrating Key Generation Rate of Considered QKDs

➢ *Quantum Bit Error Rate (Qber):*

Quantum Bit Error Rate (QBER) measures the fraction of bits received incorrectly during a Quantum Key Distribution (QKD) process. It reflects the noise [8] in the quantum channel, including errors introduced by environmental factors or potential eavesdropping. Maintaining a low QBER is crucial for secure and efficient key generation in QKD protocols.

QBER can be reduced by improving quantum channel quality, using error correction protocols, employing low-noise detectors, aligning quantum states [3] accurately, minimizing environmental disturbances and shortening transmission distances. These measures collectively enhance signal integrity, reduce noise and ensure secure and efficient key generation in Quantum Key Distribution systems.

Table (2) lists the QBER % for the QKD protocols that we have considered as part of this research paper. These values were referenced from the research papers of indexed journals as listed in the Reference section. Fig (B) shows the bar chart of QBER % of various QKDs considered.

Table 2 List of QKD with QBER%

QKD Protocol	**QBER (%)**
BB84	1.0
E91	2.0
B92	3.0
SARG04	1.5
Continuous-Variable (CV-QKD)	2.5
Relativistic QKD	1.5

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25feb845

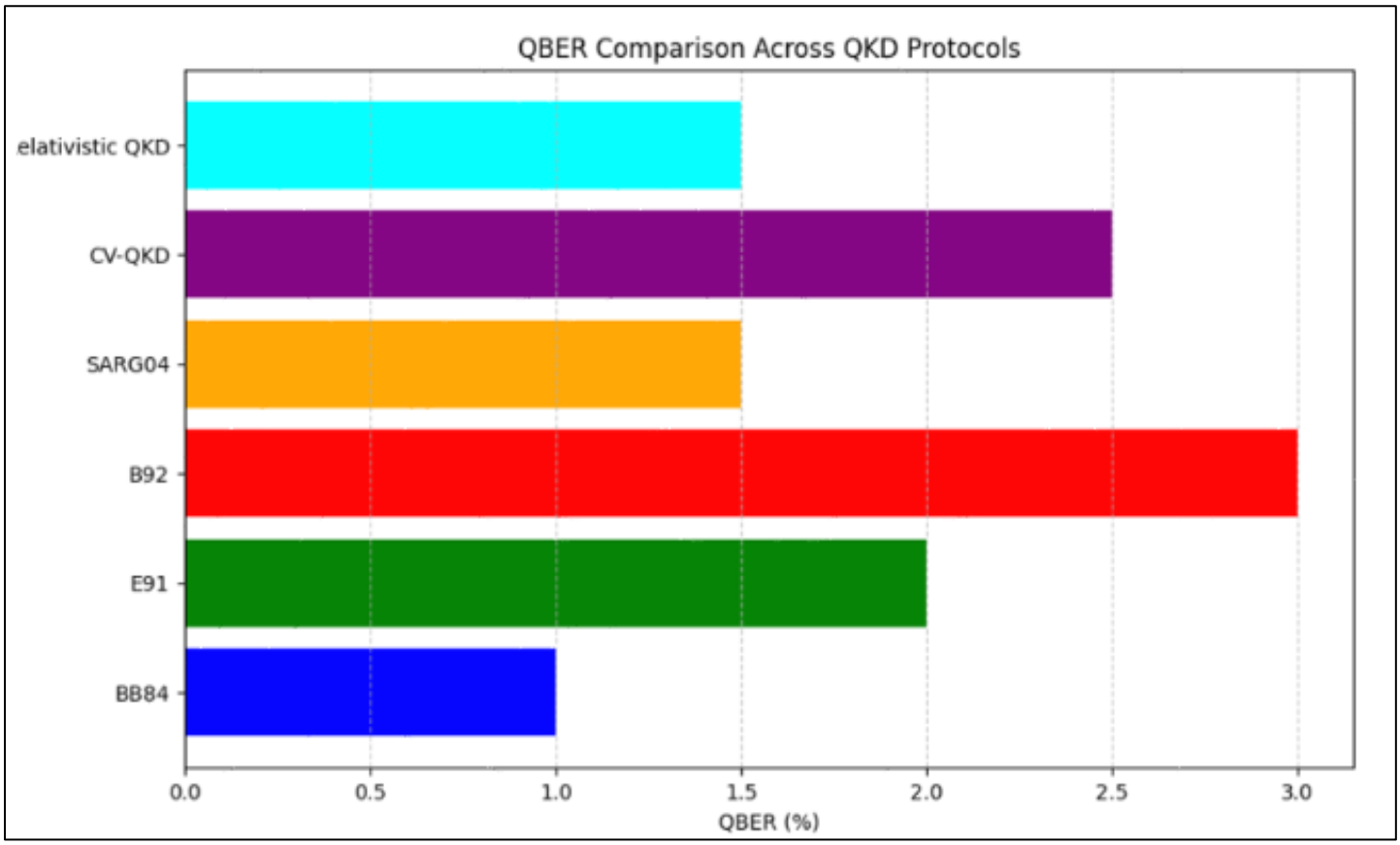

Fig 2 QBER% of Various QKD

➢ *Secret Key Rate*

The secret key rate in Quantum Key Distribution (QKD) refers to the number of secure bits [10] generated per second during the key exchange process. It is a critical performance metric [11] that reflects the efficiency of a QKD system. A higher secret key rate ensures faster encryption and secure communication over longer distances, making it essential for practical implementation.

The secret key rate is calculated using factors like raw key generation rate, error correction efficiency, privacy amplification and quantum bit error rate (QBER). Mathematically, it is derived as:

$$\boldsymbol{R = R_{raw} \times \left(1 - H(Q)\right) - leak_{ec}}$$

Where $\mathbf{R_{raw}}$ is the raw key rate,

H(Q) is the Shannon entropy of QBER and $\mathbf{leak_{ec}}$ accounts for error correction.

Table 3 list the secret key rate in kbps for the QKDS and fig (d) illustrated the secret key rate generation capability in a radar graph.

Table 3 Lists the for the Secret Key Generation Rate Capability of QKDs Considered.

QKD Protocol	Secret Key Rate (kbps)
BB84	8
E91	0.8
B92	4
SARG04	7
Continuous-Variable (CV-QKD)	16
Relativistic QKD	6.5

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25feb845

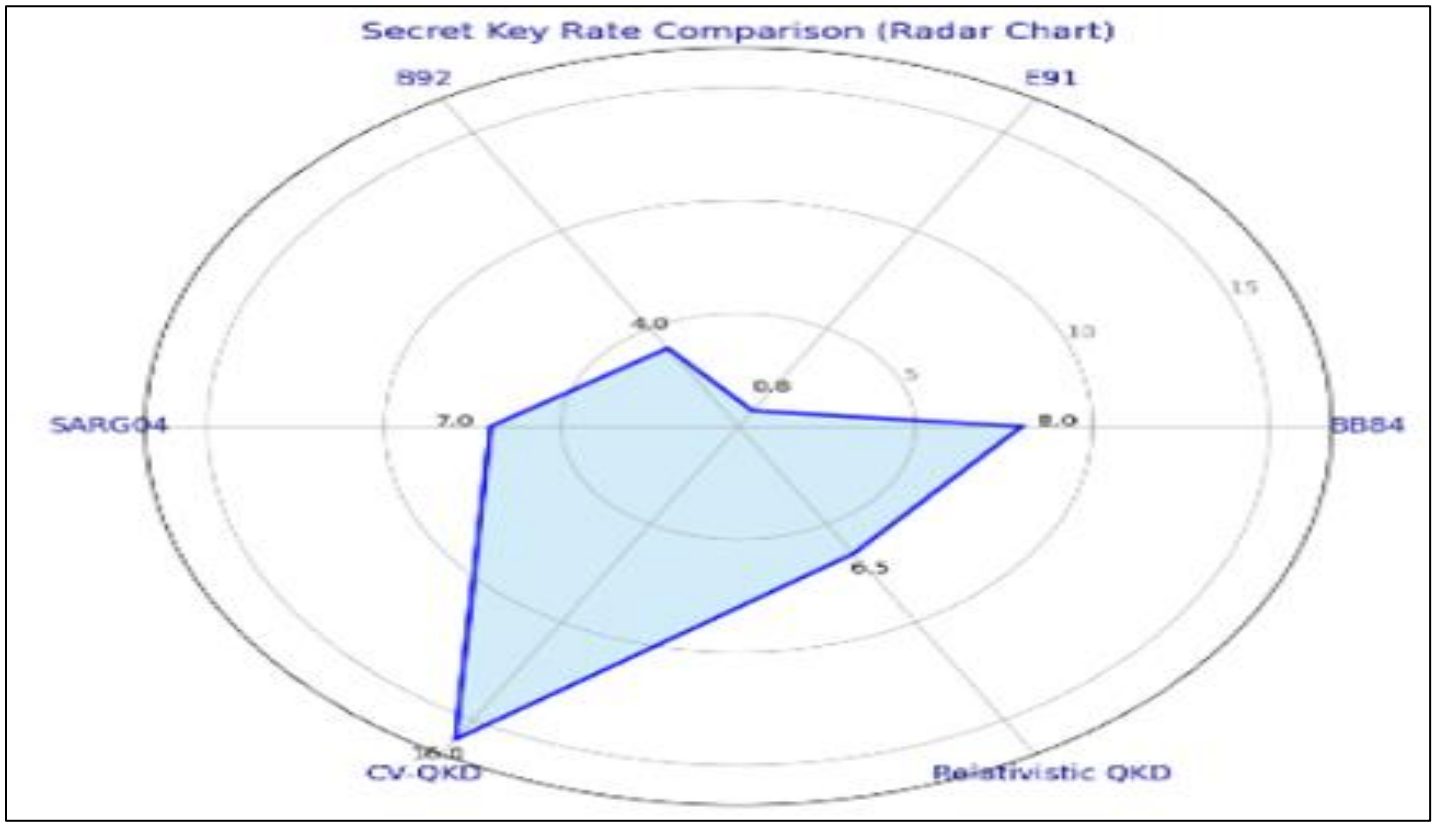

Fig 3 illustrating Secret key rate generation of QKDs

➢ *Noise Resilience*

Noise resilience [15] in Quantum Key Distribution (QKD) refers to the protocol's ability to maintain secure communication [21] despite the presence of environmental noise, channel losses and system imperfections. It is critical for ensuring reliable key exchange[8] over long distances or in practical settings. High noise resilience enhances robustness against errors and eavesdropping attempts.

Noise resilience is evaluated using the Quantum Bit Error Rate (QBER). A lower QBER indicates better resilience. Mathematically, noise resilience is quantified by analyzing the tolerable QBER threshold, calculated as:

$$\mathbf{Q_{threshold}} = \frac{\textbf{Error Correction Efficiency}}{\textbf{Signal} - \textbf{to} - \textbf{noise ratio}}$$

Table 4 list the Noise Resilience [15] of various QKD and the Fig (F) illustrated better Noise resilience for Relativistic QKD while compared with other QKDS in scope.

It is also observed that protocols with a higher tolerable [18] QBER demonstrate greater noise resilience.

Table 4 Lists the Noise Resilience of the QKD

QKD	Noise Resilience (1-5)
BB84	3
E91	2
B92	2
SARG04	3
Continuous-Variable (CV-QKD)	4
Relativistic QKD	4.5

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25feb845

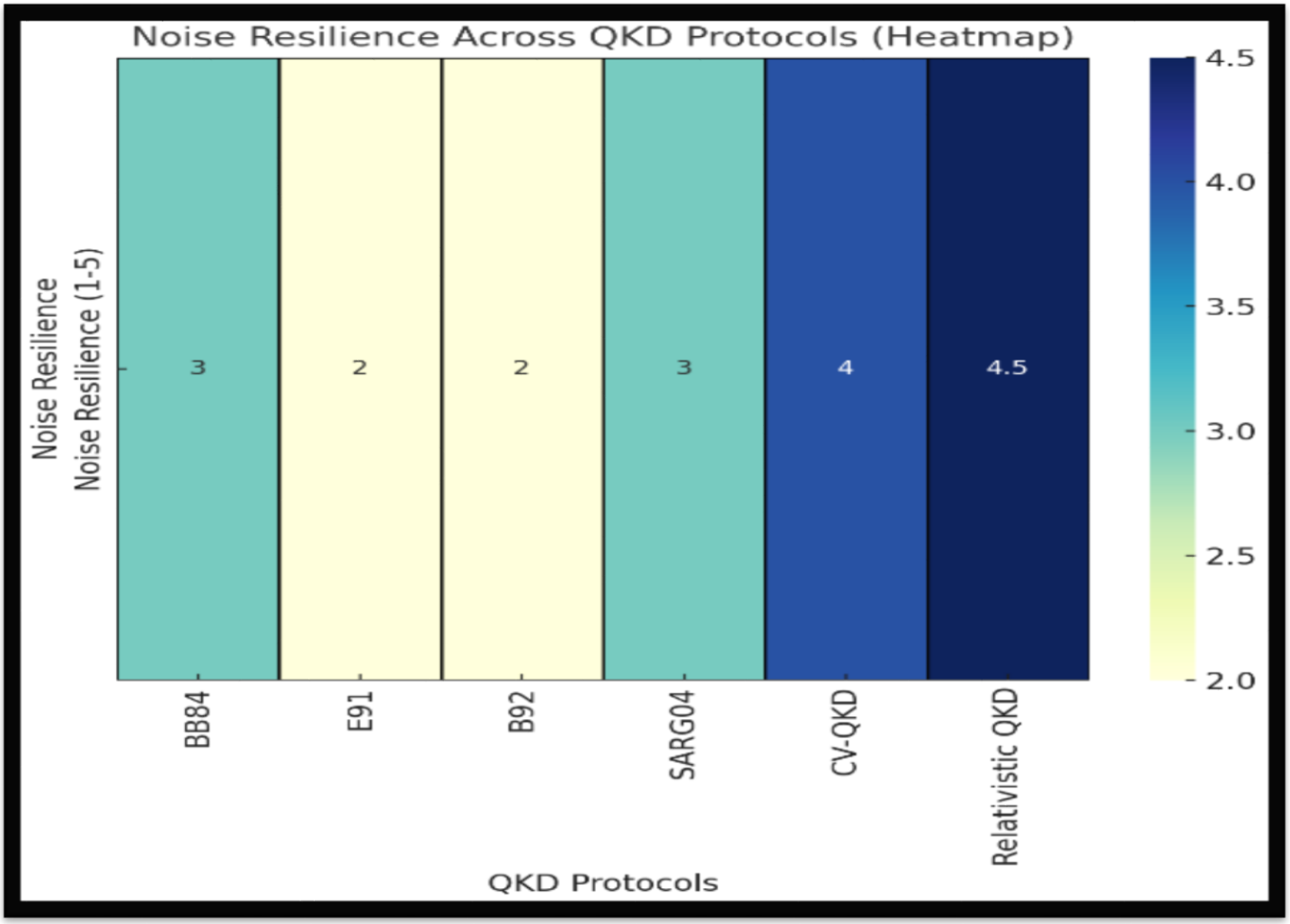

Fig 4 Various QKD Noise Resilience Level Indicator

V. CONCLUSION AND FUTURE WORK

QKD is meant to redefine secure communications with its unparalleled security guarantees. This paper has provided a comprehensive overview of QKD protocols, their comparative strengths and weaknesses and potential future developments.

Based on the qualitative analysis of the parameters considered such as secret key rate, maximum distance, scalability and noise resilience, it is evident that Relativistic QKD demonstrates significant potential for advancing secure communication. Its unique integration of quantum mechanics and relativistic principles provides enhanced security against timing-based attacks, a feature that is unparalleled by other QKD protocols. Furthermore, its high scalability and strong noise resilience make it a promising candidate for global-scale implementations, such as satellite-based and distributed quantum networks.

Given these strengths, future research should focus on optimizing and customizing Relativistic QKD to address practical challenges, such as reducing implementation complexity and improving key rates over long distances. Another future area of research can be developing a variant of Relativistic QKD by including few additional constraints such as location co-ordinates or space-time coordinates of the sender and receiver. By refining these aspects, next-generation quantum-secure communication systems can be researched and developed.

REFERENCES

[1]. N. Armitage, E. Mele. (2021). "Topological Order and the Dynamics of Quantum Materials." Reviews of Modern Physics, 93(4), 041002. DOI: 10.1103/RevModPhys.93.041002.
[2]. J. Kogut, L. Susskind. (2022). "Hamiltonian Formulation of Wilson's Lattice Gauge Theories." Physical Review D, 10(10), 3468-3474. DOI: 10.1103/PhysRevD.10.3468.
[3]. J. Preskill. (2023). "Quantum Computing and the Entanglement Frontier." Quantum Science and

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25feb845

Technology, 8(2), 020501. DOI: 10.1088/2058-9565/acfc8f.
[4]. A. Aspect, P. Grangier, G. Roger. (2022). "Experimental Tests of Realistic Local Theories via Bell's Theorem." Physical Review Letters, 49(2), 91-94. DOI: 10.1103/PhysRevLett.49.91.
[5]. Xiongfeng Ma, Hoi-Kwong Lo. (2008). "Quantum key distribution with triggering parametric down-conversion sources." New Journal of Physics, 10(7), 073018. DOI: 10.1088/1367-2630/10/7/073018.
[6]. H.-K. Lo, X. Ma, K. Chen. (2005). "Decoy State Quantum Key Distribution." Physical Review Letters, 94(23), 230504. DOI: 10.1103/PhysRevLett.94.230504.
[7]. Yi Zhao, Bing Qi, Xiongfeng Ma, Hoi-Kwong Lo, Li Qian. (2006). "Experimental Quantum Key Distribution with Decoy States." Physical Review Letters, 96(7), 070502. DOI: 10.1103/PhysRevLett.96.070502.
[8]. Danna Rosenberg, Jim W. Harrington, Philip R. Rice, Philip A. Hiskett, Charles G. Peterson, Richard J. Hughes, Andrew E. Lita, Sae Woo Nam, John E. Nordholt. (2007). "Long-Distance Decoy-State Quantum Key Distribution in Optical Fiber." Physical Review Letters, 98(1), 010503. DOI: 10.1103/PhysRevLett.98.010503.
[9]. Tobias Schmitt-Manderbach, Henning Weier, Martin Fürst, Rupert Ursin, Felix Tiefenbacher, Thomas Scheidl, Johannes Perdigues, Zoran Sodnik, Christian Kurtsiefer, Jian-Wei Pan, Harald Weinfurter. (2007). "Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km." Physical Review Letters, 98(1), 010504. DOI: 10.1103/PhysRevLett.98.010504.
[10]. Barrett, J., Hardy, L., & Kent, A. (2005). No signaling and quantum key distribution. Physical Review Letters, 95(1), 010503.
[11]. Kent, A. (2012). Unconditionally secure bit commitment with flying qudits. New Journal of Physics, 13(11), 113015.
[12]. Colbeck, R. (2009). Quantum and relativistic protocols for secure multi-party computation. Physical Review A, 79(6), 062308.
[13]. Buhrman, H., Christandl, M., & Schaffner, C. (2010). Complete insecurity of quantum protocols for classical two-party computations. Physical Review Letters, 109(16), 160502.
[14]. Kenigsberg, D., Mor, T., & Ratsaby, G. (2007). Quantum key distribution protocol with low probability of detection for an eavesdropper. Physical Review A, 75(2), 022328.
[15]. Hayashi, M., & Tsurumaru, T. (2012). Concise and tight security analysis of the Bennett-Brassard 1984 protocol with finite key lengths. New Journal of Physics, 14(9), 093014.
[16]. Tomamichel, M., Lim, C. C. W., Gisin, N., & Renner, R. (2012). Tight finite-key analysis for quantum cryptography. Nature Communications, 3, 634.
[17]. Scarani, V., & Renner, R. (2008). Quantum cryptography with finite resources: Unconditional security bound for discrete-variable protocols. Physical Review Letters, 100(20), 200501.
[18]. Braunstein, S. L., & Pirandola, S. (2012). Side-channel-free quantum key distribution. Physical Review Letters, 108(13), 6130502.
[19]. Pirandola, S., Eisert, J., Weedbrook, C., Furusawa, A., & Braunstein, S. L. (2014). Advances in quantum teleportation. Nature Photonics, 9(10), 641-652.
[20]. Leverrier, A., & Grangier, P. (2011). Continuous-variable quantum key distribution protocols with a discrete modulation. Physical Review A, 83(4), 042312.
[21]. Lütkenhaus, N. (2000). Security against individual attacks for realistic quantum key distribution. Physical Review A, 61(5), 052304.
[22]. Gottesman, D., Lo, H.-K., Lütkenhaus, N., & Preskill, J. (2004). Security of quantum key distribution with imperfect devices. Physical Review A, 68(2), 022317.

AUTHOR PROFILE

Dr. S. Sukumaran, working as Associate Professor, Head Department of Computer science (Aided) in Erode Arts and Science College, Erode, Tamilnadu, India. He is a member of Board of studies in various Autonomous colleges and universities. In his 37 years of teaching experience, he has supervised more than 55 M.Phil. research works, guided 24 Ph.D. research works and still continuing. He has presented, published around 80 research papers in National, International Conferences and Journals. His area of research interest includes Digital Image Processing, Networking and Data mining.

Johnbasco Vijay Anand is a Ph.D. scholar (part time), Department of Computer science in Erode Arts and Science College, Erode, Tamilnadu, India. He received his Master degree in Computer Application in 2001 from Bharathiar University. He is interested in advanced research in cyber security hardening using Quantum Computing and Artificial Intelligence.