A Comprehensive Approach for Harnessing Entanglement for Next-Generation Authentication: From Passwords to Qubits

Srivaramangai Ramanujam, Furkan Sayyed

***Abstract:** Traditional authentication mechanisms, such as password-based systems and multi-factor authentication (MFA), face escalating vulnerabilities in an era marked by sophisticated cyberattacks, quantum computing advancements, and evolving regulatory demands. Passwords, inherently prone to phishing, brute-force attacks, and credential reuse, remain a weak link in cybersecurity despite decades of incremental improvements. Meanwhile, emerging technologies like quantum computing threaten to dismantle classical cryptographic protocols, necessitating a paradigm shift in authentication frameworks. This paper proposes From Passwords to Qubits: Harnessing Entanglement for Next-Generation Authentication," a novel approach that leverages the principles of quantum mechanics—specifically quantum entanglement—to design secure, scalable, and future-proof authentication systems. The implications of this research extend beyond cybersecurity: it lays the groundwork for a future where quantum entanglement underpins secure digital identities, blockchain systems, and IoT ecosystems. As quantum computing matures, the fusion of entanglement-driven authentication with classical protocols will be pivotal in safeguarding sensitive data against existential threats, heralding a new era of trust in the digital age.*

***Keywords:** Entanglement, FIDO2, No-cloning Theorem, post-quantum Cryptography, QKD, Quantum Authentication, Quantum Cybersecurity.*

Abbreviations:

BB84: A Quantum Key Distribution Protocol
BPNN: Backpropagation Neural Network
BSM: Bell State Measurement
CRYSTALS-Kyber: Cryptographic Suite for Algebraic Lattices (a Post-Quantum Cryptography Algorithm)
DH: Diffie-Hellman (Key Exchange Algorithm)
ECC: Elliptic Curve Cryptography
FIDO2: Fast Identity Online 2 (Authentication Standard)
GHZ: Greenberger–Horne–Zeilinger
LA: Longitudinal Phonon-Assisted Excitation
MDI-QKD: Measurement Device-Independent Quantum Key Distribution
MFA: Multi-Factor Authentication
MQTT: Message Queue Telemetry Transport
NIR: Near-Infrared Spectroscopy
NIST: National Institute of Standards and Technology
PQC: Post-Quantum Cryptography
QAS: Quantum Authentication Scheme
QDS: Quantum Dot-based Single-Photon Sources
QECC: Quantum Error Correcting Codes
QGA: Quantum Genetic Algorithm
QIA: Quantum Identity Authentication
QKD: Quantum Key Distribution
RQGA: Real-Coded Quantum-Inspired Genetic Algorithm
SPDC: Spontaneous Parametric Down-Conversion
SPHINCS+: A Stateless Hash-Based Digital Signature Scheme
SPIR: Secure Private Information Retrieval
TLS: Transport Layer Security, TPE: Two-Photon Excitation
WPA3: Wi-Fi Protected Access 3

Manuscript received on 22 February 2025 | First Revised Manuscript received on 28 February 2025 | Second Revised Manuscript received on 17 March 2025 | Manuscript Accepted on 15 April 2025 | Manuscript published on 30 April 2025.

***Correspondence Author(s)**

Srivaramangai Ramanujam*, Head, Department of Information Technology, University of Mumbai, Mumbai (Maharashtra), India. Email ID: rsrimangai@gmail.com, ORCID ID: 0000-0003-2723-6067

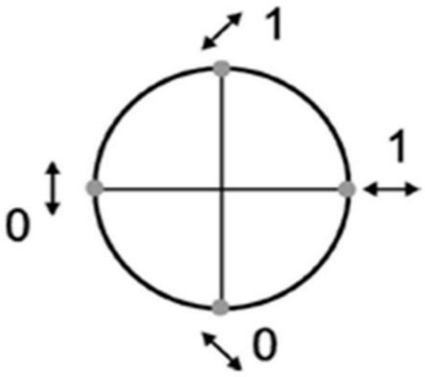
Furkan Sayyed, Student, Department of Information Technology, University of Mumbai, Mumbai (Maharashtra), India. Email ID: sayyedfurkan115@gmail.com

I. INTRODUCTION

In an increasingly digitized world, authentication lies at the heart of cybersecurity, safeguarding access to everything from personal emails to critical infrastructure. Yet, the foundational mechanisms of authentication—passwords and classical cryptographic protocols—are buckling under the weight of modern threats. Despite decades of incremental improvements, password-based systems remain vulnerable to phishing, brute-force attacks, and credential stuffing, with 81% of data breaches traced to weak or reused passwords. Even multi-factor authentication (MFA), hailed as a panacea, struggles with usability trade-offs and emerging attack vectors like SIM-swapping and biometric spoofing. Concurrently, the advent of quantum computing has cast a shadow over classical cryptography: Shor's algorithm threatens to dismantle RSA and ECC by factoring large integers exponentially faster than classical methods while Grover's algorithm jeopardizes symmetric encryption by halving the effective security of keys. As nations and corporations race toward quantum supremacy, the urgency to reimagine authentication for a post-quantum era has never been greater. This paper addresses these dual challenges by proposing a paradigm shift from passwords to qubits, leveraging the unique properties of quantum mechanics—particularly quantum entanglement—to design next-generation authentication systems. Traditional authentication relies on shared secrets (passwords) or mathematical hardness assumptions (public-key cryptography), both of which are fundamentally incompatible with the threat landscape of tomorrow. In contrast, quantum entanglement offers a radical alternative: the non-local correlations between entangled particles enable tamper-evident communication, while the no-cloning theorem ensures that quantum states cannot be copied or intercepted without detection. These principles, when harnessed for authentication, promise to eliminate the vulnerabilities of classical systems while future-proofing security against quantum adversaries. The core contribution of this work is a novel entanglement-driven authentication framework that integrates quantum key distribution (QKD), post-quantum cryptographic primitives, and biometric-like quantum "fingerprints." By exploiting the collapse of entangled states during measurement, our protocol generates unforgeable, single-use authentication tokens that are immune to replay and man-in-the-middle (MITM) attacks. Furthermore, we bridge the gap between theoretical quantum mechanics and practical cybersecurity by addressing scalability, interoperability with legacy systems, and standardization challenges. For instance, our hybrid model combines lattice-based cryptography (e.g., CRYSTALS-Kyber) with entanglement-based keys, ensuring backward compatibility while preparing for a quantum future. This research is timely and critical. Recent advances in quantum hardware, such as IBM’s 433-qubit Osprey processor and China’s Micius satellite, demonstrate that quantum networks are transitioning from labs to real-world deployments. Meanwhile, initiatives like NIST’s Post-Quantum Cryptography Standardization Project and FIDO2’s password-less authentication standards underscore the global push to phase out classical methods. However, existing literature lacks a unified approach to quantum authentication that balances theoretical rigour with practical feasibility—a gap this paper aims to fill. The remaining sections of this paper are organized as follows: Section 2 describes the reviews of classical authentication vulnerabilities and quantum threats. Section 3 introduces quantum entanglement and its relevance to authentication. Section 4 details our proposed protocol, including simulations on IBM Quantum Experience. Section 5 evaluates performance, security, and scalability, while Section 6 discusses challenges and future work. Section 7 concludes with implications for policymakers, enterprises, and the broader cybersecurity community. By merging the frontiers of quantum physics and cybersecurity, this work not only advances the science of authentication but also provides a blueprint for securing digital identities in a world where quantum computers render classical defences obsolete.

II. LITERATURE SURVEY

In this paper, Gisin et. al [1]. Present a comprehensive review of QC, discussing both theoretical foundations and experimental advancements. The authors begin by contrasting classical cryptographic techniques, such as public-key cryptosystems and the one-time pad, with quantum key distribution (QKD), which derives security from fundamental quantum principles rather than computational complexity. The paper explores major QKD protocols, including the BB84 protocol, which relies on the Heisenberg uncertainty principle and the no-cloning theorem, and the EPR-based protocol, which leverages entanglement and Bell's inequality violations for security. Various alternative protocols, such as the two-state and six-state schemes, are also discussed. The authors then examine key technological challenges in implementing QC, including the development of efficient photon sources like weak laser pulses and parametric down-conversion, the optimization of quantum channels using optical fibres and free-space links, and advancements in single-photon detection. The review also highlights practical experimental implementations of QKD, covering polarization, phase, and frequency encoding, as well as multi-user quantum communication systems. A significant portion of the paper is dedicated to analyzing security threats, such as intercept-resend attacks, photon number splitting, and Trojan horse attacks, and it discusses various methods to counteract them, including privacy amplification and error correction. The authors emphasize that while QKD offers provable security, real-world implementations require further advancements in photon sources, quantum repeaters, and integration with existing communication infrastructure. The paper concludes by reaffirming the immense potential of quantum cryptography, noting that despite existing technical limitations, continuous progress in the field will likely lead to widespread adoption of QC for secure communication in the future.

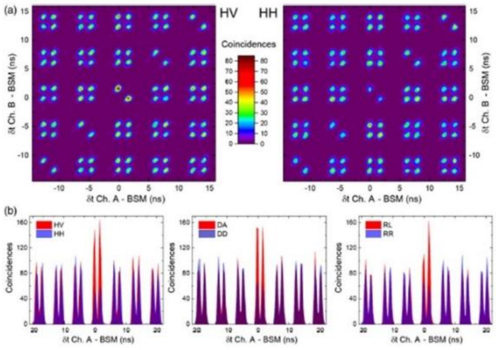


[Fig.1: Implementation of BB84 Protocol [1]]

Bozzio, M. et.al. (2022) explore the enhancement of quantum cryptography (QC) through quantum dot-based single-photon sources (QDS), which provide high brightness and low multiphoton contribution, making them more secure and efficient than traditional Poisson-distributed sources (PDS) like attenuated lasers and down-conversion methods. The authors examine optimal optical pumping schemes, including resonant excitation (RE), longitudinal phonon-assisted (LA) excitation, and two-photon excitation (TPE), to determine their impact on brightness, purity, and security. The study highlights the advantages of QDS in quantum key distribution (QKD), particularly in BB84 [2], decoy-state QKD, and twin-field QKD, by reducing eavesdropping risks and improving communication range. Furthermore, the paper extends its analysis to other quantum cryptographic primitives, such as unforgeable quantum tokens, strong quantum coin flipping, and quantum bit commitment, demonstrating how QDS can outperform PDS in these applications by enhancing security and efficiency. The findings suggest that QDS-based quantum communication can significantly improve future secure communication networks, underscoring the necessity for further research and development in this field. This paper by Bloom et.al

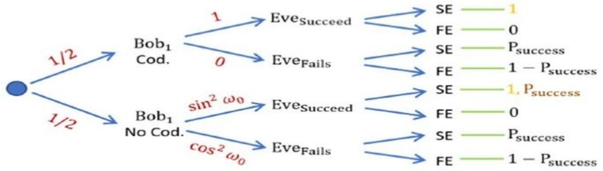
Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

offers an easy [3], efficient way of teaching quantum cryptography concepts at an undergraduate level. It explores quantum key distribution (QKD) through the BB84 protocol, concentrating on how it achieves secure communication by leveraging quantum physics. The authors offer an experiment utilizing a pulsed laser, substituting the single-photon source, so that students may simulate exchanging keys while still maintaining the fundamental concepts of QKD. The paper touches on fundamental cryptographic concepts, such as the no-cloning theorem, one-time pad encryption, and quantum randomness effect. A computer simulation is also developed so that students may analyze and understand key distribution, error checking, and the presence of an eavesdropper in a quantum channel. The study highlights the challenges posed by applying quantum cryptography [3] in practical scenarios, including accuracy while transmitting, cost, and limitations of equipment. The proposed educational experiment, however, offers an accessible, affordable means by which students can experiment with quantum encryption without specialized training. Both experimental and simulated setups' findings confirm that QKD allows secure exchange of keys while it also detects unauthorized party attempts. The authors discover that this method serves as an excellent teaching tool, connecting quantum mechanics theories and practical cryptography, an excellent introduction to quantum concepts of physics and engineering studies. Basset, F. B. et.al. (2019) [4] achieve entanglement swapping by harnessing pairs of polarization-entangled photons created on demand by a GaAs quantum dot, unaided by spectral or temporal filtering. Entanglement swapping, an inevitable quantum network tool, makes possible entanglement between two remote photons without direct coupling, bypassing limitations in optical communications due to the no-cloning theorem. In contrast to past strategies, relying previously on probabilistic sources, such as spontaneous parametric own-conversion (SPDC), this work employs deterministic quantum dot sources to offer an efficient, scalable approach. The experiment follows the BB84 protocol by generating entangled photon pairs through two-photon resonant excitation, utilizing beam splitter-based measurements of the Bell states. A theoretical description is also developed, accurately simulating the experimental data, while extracting essential parameters necessary for maximizing quantum dot performance over quantum communications over distance.



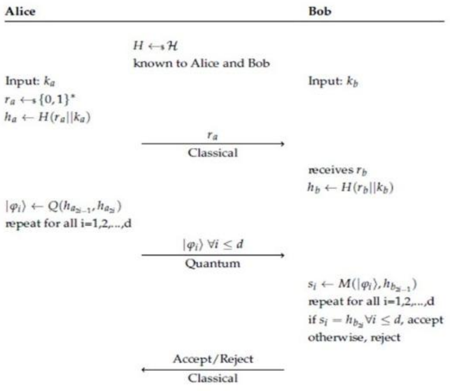
[Fig.2: Fourfold Coincidences Histograms [4] as a Function of the Delays Between the BSM and the XX Detection]

Cardoso-Isidoro, C. et.al. (2023) [5] suggest an authentication method using double quantum teleportation, wherein an arbitrary quantum state gets teleported to two receivers in superposition. The method aims to enhance cryptographic authentication by ensuring neither sender (Alice) nor receivers (Bob0, Bob1) initially know the quantum state, thus making unauthorized entry and impersonation very difficult. The authentication method involves Bob1 applying an openly known operation over the teleported state while retaining an undisclosed key, later verified by Bob0. The paper also explores threats by an eavesdropping adversary (Eve) stealing authentication credentials [5], either by pure guessing or by employing a heralded qubit method to boost the success probability. The authors demonstrate that by well-structuring authentication chains and selecting the best quantum states, successful impersonation by an adversary can significantly decrease. Beyond authentication, the paper also explores whether it is possible to implement double teleportation over Quantum Key Distribution (QKD), specifically protocols such as BB84. The proposed method makes the secure exchange of a key possible by harnessing quantum entanglement and non-locality phenomena while eliminating quantum communication loopholes. The work reveals that the choice of suitable quantum states, together with the application of multi-qubit authentication sequences, significantly enhances security against eavesdropping. The study concludes that authentication through double teleportation has an efficient, scalable, and secure quantum network platform, paving the way for future quantum application studies. Barnum, H. et.al. (2002) address quantum authentication, applying authentication techniques from the classical case to the quantum case. They give rigorous authentication definitions for quantum scenarios [6], whereby the sender (Alice) and recipient (Bob), both having an agreed-on classical private key, want to send quantum messages securely over an untrusted quantum channel. The authors build an efficient, non-interactive quantum authentication scheme (QAS) that allows Alice both to encrypt and verify an m-qubit message by representing it as an m+s encoded qubit, where the parameter s determines the probability of tampering detection. In contrast to authentication, possible independently over classical channels, they demonstrate authentication must involve encryption, by virtue of quantum cryptography, due to the no-cloning principle and principle of measurement disturbance. This implies an asymptotic quantum authentication lower bound of 2m classical key bits, making their protocol asymptotically optimal.

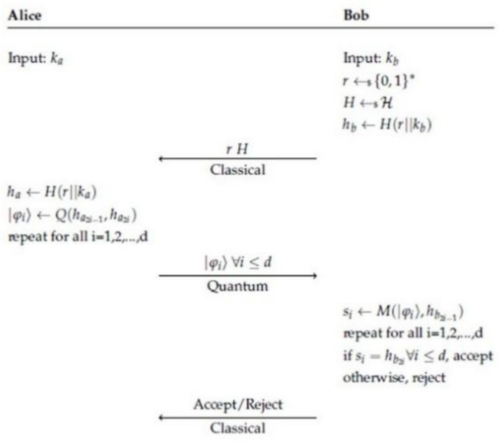

1/2
1/2
Bob_1 Cod.
Bob_1 No Cod.
1
0
$\sin^2 \omega_0$
$\cos^2 \omega_0$
$\text{Eve}_{\text{Succeed}}$
$\text{Eve}_{\text{Fails}}$
$\text{Eve}_{\text{Succeed}}$
$\text{Eve}_{\text{Fails}}$
SE — 1
FE — 0
SE — P_{success}
FE — $1 - P_{\text{success}}$
SE — 1, P_{success}
FE — 0
SE — P_{success}
FE — $1 - P_{\text{success}}$

[Fig.3: General Scheme for Eavesdropping [5]]

The paper also develops further protocols for purification testing through quantum error-correcting codes (QECCs) to assure the integrity of messages [6]. These protocols allow both Alice and Bob to confirm any tampering with their quantum states before finishing the transmission. The authors also address threats by an adversary due to eavesdropping, demonstrating that any attempt by an adversary to get information out of a quantum state must inevitably cause traceable changes. A fundamental result is the unprovability of digitally authenticating quantum states, as any authentication method enabling a recipient to verify a quantum message also allows them to tamper undetectably, unlike classical digital signatures. This result emphasizes the need for other approaches to quantum communications' security. The paper also finally proposes an exacting quantum authentication method, providing provable means by which quantum messages may securely be sent while preventing tampering messages as well as unauthorized entry. Their work opens the way toward secure quantum communications networks, laying the groundwork for future practical quantum authentication protocols. González-Guillén et.al in their paper present a critical analysis of Zawadzki's quantum identity authentication (QIA) scheme, targeted at authenticating the identity of an individual through mutual quantum resources [7]. The authors argue that the protocol is inherently insecure, drawing support from Lo, Colbeck, and Buhrman et.al.'s theoretical impossibility results, whereby secure quantum authentication protocols are declared not possible unless there are additional restrictions laid down against the adversary. The authors reveal that Zawadzki's authentication scheme, applying quantum measurements and a hash function, has defects that allow an adversary to significantly reduce the key space through conclusive exclusion attacks. Through quantum measurements, an adversary has the power to exclude wrong possibilities, significantly reducing the system's security by mere authentication attempts. Beyond proving Zawadzki's protocol vulnerable, the paper also explores the general implications for other quantum authentication protocols. The authors relate their results to previous QIA protocols, indicating those still vulnerable to the same type of attacks, and those secure by virtue of other cryptographic assumptions, such as authentication by means of entanglement. Their result highlights the need for fundamental quantum authentication design changes, beyond today's toolkit of classical cryptography, and adopting new paradigms if one wishes to achieve quantum-proof security. The figures below represent the designed protocol and modified protocol.


Alice
Bob
$H \leftarrow_{\$} \mathcal{H}$
known to Alice and Bob
Input: k_a
$r_a \leftarrow_{\$} \{0,1\}^*$
$h_a \leftarrow H(r_a||k_a)$
Input: k_b
r_a
Classical
receives r_b
$h_b \leftarrow H(r_b||k_b)$
$|\varphi_i\rangle \leftarrow Q(h_{a_{2i-1}}, h_{a_{2i}})$
repeat for all i=1,2,...,d
$|\varphi_i\rangle\ \forall i \leq d$
Quantum
$s_i \leftarrow M(|\varphi_i\rangle, h_{b_{2i-1}})$
repeat for all i=1,2,...,d
if $s_i = h_{b_{2i}} \forall i \leq d$, accept
otherwise, reject
Accept/Reject
Classical

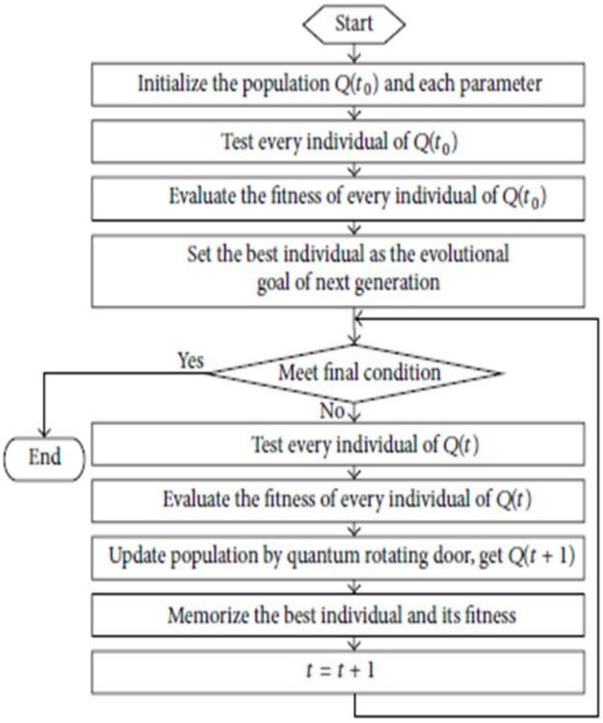
[Fig.4: Original Protocol [7]]


Alice
Bob
Input: k_a
Input: k_b
$r \leftarrow_{\$} \{0,1\}^*$
$H \leftarrow_{\$} \mathcal{H}$
$h_b \leftarrow H(r||k_b)$
$r\ H$
Classical
$h_a \leftarrow H(r||k_a)$
$|\varphi_i\rangle \leftarrow Q(h_{a_{2i-1}}, h_{a_{2i}})$
repeat for all i=1,2,...,d
$|\varphi_i\rangle\ \forall i \leq d$
Quantum
$s_i \leftarrow M(|\varphi_i\rangle, h_{b_{2i-1}})$
repeat for all i=1,2,...,d
if $s_i = h_{b_{2i}} \forall i \leq d$, accept
otherwise, reject
Accept/Reject
Classical

[Fig.5: Modified Protocol [7]]

Boykin et.al in their paper explores the encryption of quantum bits (qubits) by way of classical secret keys, developing an approach toward quantum information protection against an eavesdropper. The authors provide an argument that it requires at least 2n randomly selected classical bits to securely encode n qubits, so an adversary without the secret classical key gains no information about the encrypted quantum state. They introduce a quantum encryption approach utilizing unitary transformations, which generalizes the one-time pad principle to quantum data. By applying unitary transformations selected using classical keys, the encrypted quantum state is converted into a completely mixed state, making it indistinguishable from random noise without access to the key. This approach ensures perfect security for both storing and transmitting quantum information, making it an essential tool for secure quantum communications. The study also makes an explicit connection between quantum encryption and quantum teleportation, providing original proof of the optimality of teleportation protocols. The authors demonstrate that teleportation inherently functions as quantum encryption, where classical bits act as encryption keys that determine the final quantum state during transmission [8]. They also discuss practical applications, including secure quantum data storage, secret sharing, and hybrid quantum-classical cryptographic schemes. These findings emphasize the importance of developing encryption protocols that integrate both quantum and classical cryptography, paving the way for future secure quantum communication networks. Liu, J. et.al. (2015) [9] propose a real-coded quantum-inspired genetic algorithm (RQGA) to optimize backpropagation neural network (BPNN) weights and threshold values, addressing the drawbacks of gradient descent-based learning strategies. Traditional BPNN faces challenges such as slow convergence, local minima entrapment, and instability due to poor weight initialization. The paper highlights that while quantum genetic algorithms (QGA) offer strong global optimization capabilities, their reliance on binary encoding limits computational efficiency.

To overcome this, the authors introduce real-coded QGA, eliminating the need for encoding and decoding, thereby improving search speed and accuracy. The proposed approach integrates adaptive learning rates and quantum evolutionary operators to refine BPNN training, ensuring faster convergence while maintaining accuracy. Simulation results confirm that RQGA-BP outperforms traditional BPNN and GA-BP (genetic algorithm-based BPNN) models by significantly enhancing network stability, convergence speed, and generalization ability [9]. The paper also explores RQGA's evolutionary mechanisms, detailing how quantum bit representation helps maintain population diversity and prevents premature convergence. The authors employ quantum rotation gates and migration strategies to optimize efficiency, demonstrating superior performance in real-world applications such as machinery fault diagnosis and gasoline octane number prediction using near-infrared spectroscopy (NIR). Comparative analysis against BP and GA-BP networks shows that RQGA-BP achieves lower prediction errors and higher accuracy across multiple test cases. Statistical validation through t-tests confirms that the improvements in convergence and prediction reliability are significant, making RQGA a promising alternative for optimizing complex neural network models. The study concludes that RQGA-BP offers an efficient and scalable solution for real-world optimization challenges, paving the way for future advancements in quantum-inspired artificial intelligence. [Wang, H. et.al. (2013) provide an improved Quantum Genetic Algorithm (QGA) that seeks maximum efficiency and accuracy in function optimization. Classical QGA employs quantum computing concepts such as superposition, coherence, and entanglement to optimize performance over traditional Genetic Algorithms (GA). However, conventional QGA has limitations, including premature convergence, slow search speed, and difficulty in selecting optimal rotation angles. To address these issues, the authors propose several enhancements, including an adaptive rotation angle strategy, the introduction of quantum mutation processes, and a quantum disaster recovery mechanism. The improved QGA strengthens global search capabilities, accelerates convergence, and prevents the algorithm from getting stuck in local optima. Simulation results confirm that the proposed approach outperforms conventional QGA in function optimization, achieving higher accuracy and faster convergence. Beyond function optimization, the paper explores the theoretical foundation of QGA, detailing how quantum principles are applied to evolutionary computing. The authors discuss quantum bit representation, quantum rotation gates, and parallelism, highlighting their contributions to the algorithm's superior performance. The study includes extensive simulations comparing conventional and improved QGA, demonstrating that the enhancements significantly reduce computational time while improving solution accuracy. The findings suggest that refining QGA with adaptive quantum operators and advanced evolutionary strategies can lead to more effective optimization in a variety of complex problem domains. The paper concludes that quantum-inspired evolutionary algorithms have the potential to revolutionize optimization techniques in fields such as machine learning, engineering, and artificial intelligence [10].


Start
Initialize the population $Q(t_0)$ and each parameter
Test every individual of $Q(t_0)$
Evaluate the fitness of every individual of $Q(t_0)$
Set the best individual as the evolutional goal of next generation
Yes
Meet final condition
No
End
Test every individual of $Q(t)$
Evaluate the fitness of every individual of $Q(t)$
Update population by quantum rotating door, get $Q(t+1)$
Memorize the best individual and its fitness
$t = t + 1$

[Fig.6: Flowchart of Improved Quantum Genetic Algorithm [10]]

Kanamori, Y. et.al. (2009) propose a quantum authentication method that utilizes quantum superposition states instead of quantum entanglement, aiming to develop a practical and scalable authentication mechanism for secure communication. Traditional authentication processes rely on classical cryptographic techniques, vulnerable to quantum computer-based attacks. While quantum cryptography has been explored as a solution, many existing quantum authentication protocols require the prior sharing of entangled quantum particles, making them impractical for large-scale authentication systems [11]. The proposed method addresses this challenge by using quantum superposition states, where the sender (Alice) and receiver (Bob) share a randomly chosen number that serves as both an authentication key and a classical encryption key. The protocol ensures that Alice's identity is verified before communication begins, preventing impersonation attacks. Since superposition states do not require large-scale entanglement, this approach offers a significant advantage in multi-user authentication scenarios. The paper also evaluates the security properties of the proposed protocol, demonstrating its resilience against intercept-resend and beam-splitting attacks, thanks to the no-cloning theorem. The encryption mechanism involves rotating photon polarization at randomly selected angles as secret keys, making unauthorized interception virtually impossible without introducing detectable errors. Additionally, the study highlights how the protocol can be seamlessly integrated with Quantum Key Distribution (QKD) to establish a secure authentication session. Experimental implementations suggest that the protocol can be realized using existing technologies such as linear polarizers and Faraday rotators, making it a viable solution for near-term deployment. The research concludes that quantum superposition-based authentication provides a secure, scalable, and efficient alternative to conventional authentication methods, particularly in the face of emerging quantum threats.

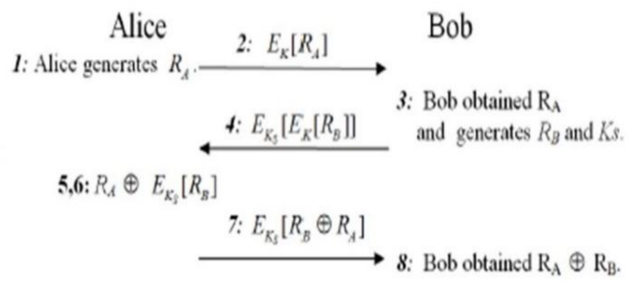
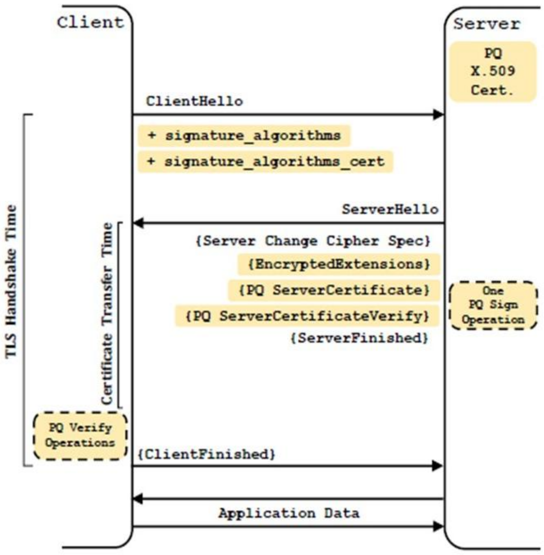

Alice
Bob
1: Alice generates R_A.
2: $E_K[R_A]$
3: Bob obtained R_A and generates R_B and Ks.
4: $E_{K_S}[E_K[R_B]]$
5,6: $R_A \oplus E_{K_S}[R_B]$
7: $E_{K_S}[R_B \oplus R_A]$
8: Bob obtained $R_A \oplus R_B$.

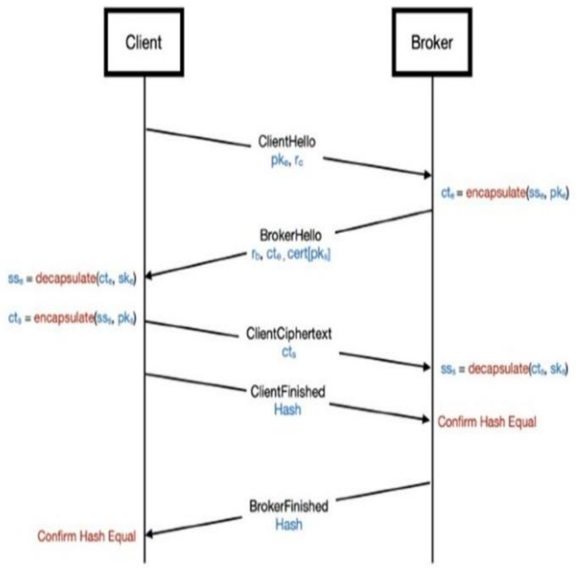
Fig.7: Two-Party Authentication Protocol [11]

Kanamori, Y. et.al. (2009) propose an authentication method that employs quantum superposition states instead of quantum entanglement, aiming to develop an efficient and scalable authentication system for secure communications. Traditional authentication methods rely on classical cryptographic schemes, which are vulnerable to attacks from quantum computers. While quantum cryptography has been explored as a solution, many existing quantum authentication protocols require the prior sharing of entangled quantum particles, making them impractical for large-scale authentication. The proposed method addresses this challenge by utilizing quantum superposition states, where both authentication and classical encryption rely on a randomly chosen number shared between the sender (Alice) and the receiver (Bob). This ensures that Alice’s identity is verified before communication begins, eliminating the risk of impersonation attacks. Since superposition states do not require large-scale entanglement distribution, this approach offers a significant advantage in multi-user authentication scenarios. The paper further explores the security features of the proposed protocol, demonstrating its resistance to intercept-resend and beam-splitting attacks due to the no-cloning theorem. The encryption process involves rotating the polarization of photons at randomly selected angles as secret keys, making unauthorized interception virtually impossible without introducing detectable errors. Additionally, the study highlights how the protocol can be seamlessly integrated with Quantum Key Distribution (QKD) to establish a secure communication channel. Experimental tests show that the protocol can be implemented using existing technologies such as linear polarizers and Faraday rotators, making it a viable option for near-term deployment. The research concludes that quantum superposition-based authentication provides a secure, scalable, and efficient alternative to conventional authentication methods, particularly in the face of emerging quantum threats [12].



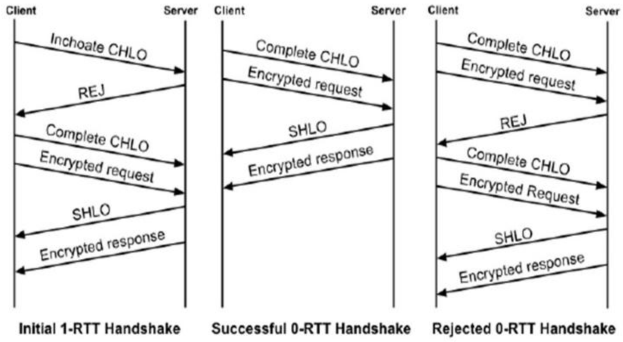
[Fig.8: Post Quantum TLS Handshake [12]]

Samandari, J. et.al. (2023) analyze the integration of post-quantum authentication into the Message Queue Telemetry Transport (MQTT) protocol, a widely used lightweight communication framework for the Internet of Things (IoT). Traditional MQTT lacks built-in authentication, making it vulnerable to security threats, especially as quantum computing advances and threatens classical cryptographic schemes like RSA and ECDSA. To address this risk, the study incorporates CRYSTALS-Dilithium, a post-quantum digital signature scheme, into MQTT authentication and evaluates its impact on CPU, memory, and disk usage. Additionally, the authors explore an alternative Key Encapsulation Mechanism (KEM)-based authentication using CRYSTALS-KYBER, which is proposed as a computationally efficient alternative. The findings indicate that while post-quantum digital signatures introduce noticeable overhead, KEM authentication reduces CPU usage by 71% and improves speed by 25ms compared to classical authentication methods, making it a better fit for resource-constrained IoT environments. Furthermore, the paper discusses the trade-offs between digital signature-based authentication and KEM-based authentication, highlighting their effects on latency, storage, and computational resources. While KEM-based authentication significantly improves connection speed, it slightly increases memory usage, though still within acceptable limits for most IoT devices. The authors suggest that a hybrid approach combining both authentication methods could provide an optimal balance between security and efficiency. The study concludes that post-quantum cryptography is essential for securing IoT communications in the future, and optimizing MQTT authentication with quantum-resistant algorithms will play a crucial role in protecting IoT networks from quantum threats [13].


Client
Broker
ClientHello
pk_e, r_c
ct_e = encapsulate(ss_e, pk_e)
BrokerHello
r_b, ct_e, cert[pk_s]
ss_e = decapsulate(ct_e, sk_e)
ct_s = encapsulate(ss_s, pk_s)
ClientCiphertext
ct_s
ss_s = decapsulate(ct_s, sk_s)
ClientFinished
Hash
Confirm Hash Equal
BrokerFinished
Hash
Confirm Hash Equal

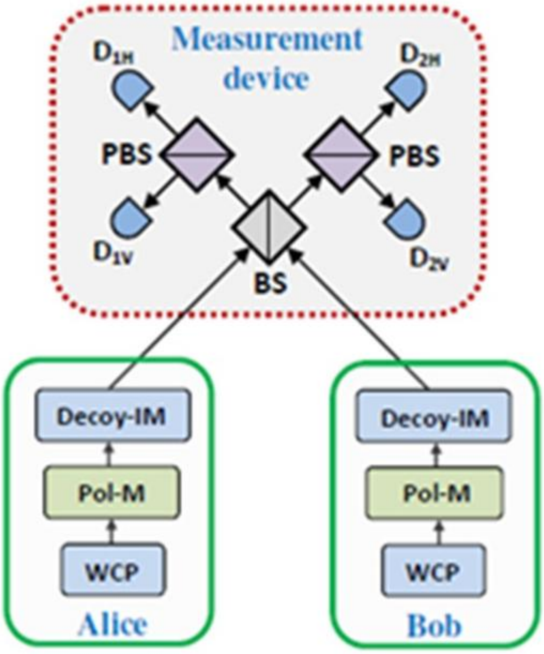
[Fig.9: TLS Handshake for MQTT Authentication Using KEMs [13]]

Langley, A. et.al. (2017) [14] introduce QUIC (Quick UDP Internet Connections), an encrypted, multiplexed, low-latency transport protocol designed to enhance HTTPS performance while enabling rapid deployment and evolution of transport mechanisms. QUIC replaces traditional HTTPS stack components, including TCP, HTTP/2, and TLS, by leveraging a user-space implementation over UDP, effectively bypassing TCP's head-of-line blocking issues. The protocol features zero-round-trip time (0-RTT) handshakes, reducing connection delays, and integrates congestion control and loss recovery mechanisms optimized for modern internet applications. The study highlights QUIC's large-scale deployment across Google's front-end servers, where it has significantly improved response times, r reducing latency by 8% on desktop and 3.6% on mobile, while also lowering YouTube rebuffering rates by up to 18%.



[Fig.10: Timeline of QUIC's Initial 1-RTT Handshake [14]]

The paper also discusses the challenges of deploying a new transport protocol, particularly the role of middleboxes in restricting network evolution. The authors emphasize QUIC's encryption-first design, which prevents protocol ossification and strengthens security against passive surveillance and active attacks. Additionally, QUIC incorporates stream multiplexing, eliminating delays caused by TCP's sequential packet delivery and enabling faster, more efficient data transfers. Performance evaluations demonstrate that QUIC performs effectively in high-latency environments and reduces retransmission delays, making it particularly well-suited for mobile networks. The study concludes that QUIC is a robust, adaptable protocol that overcomes long-standing limitations of traditional transport protocols, paving the way for future advancements in secure and efficient web communications [14]. Li, T. et.al. (2024) propose a Quantum Privacy Query (QPQ) protocol that utilizes GHZ-like entangled states to enhance the privacy and security of database queries, particularly in medical-assisted diagnosis systems. Traditional Secure Private Information Retrieval (SPIR) protocols are vulnerable to quantum computing attacks, making quantum cryptographic solutions essential. The authors employ GHZ-like states, a type of entangled quantum state, to ensure that the querying party cannot determine the database address while preventing the database from accessing excessive user information. In this protocol, a trusted third party (Charlie) generates and distributes entangled GHZ-like states among the data provider (hospital), database manager (Bob), and querier (Alice). The entanglement properties of GHZ-like states enable a secure query process, preventing joint measurement attacks, participant fraud, and external eavesdropping. Additionally, authentication mechanisms and decoy-state detection further enhance the protocol's resilience against malicious attacks. The study also compares the functional and security advantages of GHZ-like state-based QPQ with quantum single-particle query strategies, demonstrating its superiority in resisting quantum cloning attempts and intercept-resend attacks. By integrating secondary authentication processes, the protocol ensures that only the intended recipient can access the queried data while maintaining user anonymity and database confidentiality. Performance evaluations indicate that GHZ-like state-based QPQ is both secure and scalable, making it a strong candidate for secure quantum database queries in sensitive fields such as healthcare. The study suggests future research should focus on optimizing multi-user queries and improving quantum resource efficiency to further enhance practical applications For clarity, we describe a schematic to explain the proposed quantum privacy query based on a GHZ-like states scheme, as shown in Figure Lo, H.-K. et.al. (2012) offer an introduction to Measurement Device-Independent Quantum Key Distribution (MDI-QKD) as an antidote to the detector side-channel attacks, which have proved an inevitable loophole in practical Quantum Key Distribution (QKD) deployments [15]. Traditional QKD protocols rely on secure detectors, but practical limitations allow an eavesdropping possibility. MDI-QKD removes this problem by eliminating the need to trust the measuring device, normally the weakest link, by introducing an untrusted relay (Charlie) that makes a Bell state measurement (BSM) of quantum signals sent by both Alice and Bob, both utilizing weak coherent pulses in a usual BB84 protocol with decoy states. Public announcement of the measurements allows secure keying by both Alice and Bob without any compromise. MDI-QKD significantly boosts the distance, almost doubling the secure QKD over Fiber optic cable distance over traditional deployments [16]. The paper also compares DI-QKD with MDI-QKD, indicating that while DI-QKD has perfect security in principle, it requires near-perfect efficiency in detection, as well as amplifiers, making it impracticable. However, MDI-QKD has experimentally practical implications, only relying on general optical elements, as well as weak coherent sources. The authors, both through simulations, as well as through theoretical analysis, indicate that MDI-QKD has a very high generation rate, equalling that of traditional QKD setups, while securely eliminating any future, as well as past, detector-based attacks. The paper also makes an indication of the practical application of MDI-QKD, indicating that it has enormous implications for quantum communications over very large distances, making it an inevitable stepping stone toward secure quantum networks [16].



[Fig.11: Basic Setup of an MDI-QKD Protocol [16]]

Diamanti, E. et.al. (2016) provide an extensive overview of practical issues confronting Quantum Key Distribution (QKD), an encryption system that offers unconditionally secure encryption by utilizing quantum physics. While QKD has theoretical guarantees, practical application has suffered due to several issues, including poor key rate, distance limitations, costly implementation, and practical loopholes. The paper reviews several QKD protocols, including BB84, decoy-state QKD, and Measurement-Device-Independent QKD (MDI-QKD), evaluating them across various application contexts. The authors highlight those limitations due to hardware, specifically single-photon detectors and quantum random number generators, playing an essential role in degrading the efficiency of QKD systems. The paper also broaches the topic of the need to marry QKD with classical cryptography so that it contributes toward developing quantum-proof infrastructure, indicating recent progress toward developing QKD on chips, quantum repeaters, and QKD via satellites, enabling secure extension over vast distances [17]. The study also encompasses practical security threats due to side-channel attacks, whereby defects in QKD equipment allow attackers to extract secret keys. Solutions including decoy-state protocols, MDI-QKD, and loss-tolerant QKD have emerged, but the writers argue there still has to be work toward quantum-safe standards and practical deployments. The paper also highlights the use of network-based QKD solutions, including trusted-relay networks, as well as satellite-based QKD, to break distance limitations. The writers summarize that, while there has indeed been progress toward QKD performance, security, and scaling, further progress toward quantum hardware, standardization, and cost-effective deployments is necessary to enable it across the board in secure infrastructures and communications [17]. Zeydan, E. et.al. (2024) provides an overview of recent advancements in network security via post-quantum cryptography (PQC), specifically the need to transition to quantum-resistant cryptography [18]. The paper emphasizes that quantum computing threats render traditional encryption protocols such as RSA, Diffie-Hellman (DH), and Elliptic Curve Cryptography (ECC) significantly vulnerable, necessitating post-quantum alternatives. The authors summarize PQC advancements in three categories: communications, computations, and network security, discussing how PQC can support both established and future network infrastructures [19]. The paper overviews various PQC proposals, including lattice (Kyber, NTRU, SABER), code (McEliece)-, multivariate (Rainbow)-, and hash (SPHINCS+) approaches, describing performance vs. security trade-offs [20]. The paper also refers to PQC implications for security protocols such as TLS, IPSec, and WPA3, indicating possible performance overheads due to longer key sizes and processing requirements [21]. The paper also broaches issues relating to implementation, including compatibility of hardware and software, side-channel attacks, and efficient algorithm optimization required for smooth PQC implementation across 5G, IoT, and cloud computing. The paper also makes references to recent attempts by NIST toward standardization, including the selection and implementation of quantum-resistant encryption methods. The survey also includes hybrid cryptography approaches, the confluence of classical cryptography and post-quantum cryptography, so that there exists a gradual, secure transition toward PQC. The study expresses the opinion that PQC, while still in an embryonic stage, calls for further research, standardization, and industry coordination toward secure network communications in the quantum computing era.

III. INFERENCES

A. Quantum Key Distribution (QKD) and Quantum Communication

- **Foundational Work**: Gisin et.al. (2002) established the theoretical and practical basis for QKD, emphasizing protocols like BB84 and their reliance on quantum mechanics for unconditional security.
- **Technological Advances:** Bozzio et.al. (2022) demonstrated how quantum dot single-photon sources enhance QKD by

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

improving photon indistinguishability and reducing errors.

Basset et.al. (2019) achieved entanglement swapping with on-demand quantum dot photons, a critical step toward scalable quantum networks.

- **Practical Challenges:** Diamanti et.al. (2016) highlighted limitations in QKD, such as distance constraints, channel loss, and the need for trusted relays. Lo et.al. (2012) addressed these with measurement-device-independent QKD (MDI-QKD), closing security loopholes from imperfect detectors.

B. Quantum Authentication Protocols

- **Theoretical Frameworks:** Barnum et.al. (2002) proposed a foundational framework for authenticating quantum messages using quantum encryption and classical keys.

Cardoso-Isidoro & Delgado (2023) introduced a double-teleportation quantum authentication scheme, leveraging entanglement for secure identity verification.

- **Attacks and Vulnerabilities:** González-Guillén et.al. (2021) exposed flaws in Zawadzki's authentication protocol, stressing the need for rigorous security proofs against quantum adversaries.
- **Hybrid Approaches:** Kanamori et.al. (2009) explored authentication using quantum superposition states, bridging quantum and classical techniques.

C. Post-Quantum Cryptography in Network Protocols

- **Integration with Classical Infrastructure:** Sikeridis et.al. (2020) evaluated post-quantum authentication in TLS 1.3, showing lattice-based schemes (e.g., CRYSTALS-Kyber) adds minimal overhead. Samandari & Gritti (2023) adapted MQTT for IoT using post-quantum signatures, emphasizing energy efficiency trade-offs. Zeydan et.al. (2024) surveyed lattice- and hash-based algorithms for networks, advocating standardization efforts (e.g., NIST PQC).
- **Protocol Design**: Langley et.al. (2017) discussed QUIC's adaptability for post-quantum security, though challenges remain in latency and key management.

D. Quantum-Inspired Algorithms and Optimization

- **Neural Networks and Genetic Algorithms:** Liu et.al. (2015) and Wang et.al. (2013) used quantum-inspired genetic algorithms to optimize neural networks and function parameters, suggesting potential applications in cryptographic key optimization.
- **Limitations**: These works focus on classical systems but hint at future synergies with quantum computing for faster decryption or attack simulations.

E. Emerging Trends and Challenges

- **Scalability**: While quantum dots (Bozzio 2022) and MDI-QKD (Lo 2012) improve scalability, real-world deployment requires addressing cost, photon loss, and integration with existing infrastructure.
- **Standardization**: Post-quantum protocols (Sikeridis 2020; Zeydan 2024) need industry-wide adoption to replace vulnerable RSA/ECC systems.
- **Hybrid Systems:** Combining QKD with post-quantum cryptography (e.g., lattice-based signatures) could mitigate risks during the quantum transition.
- **Security Proofs:** Several works (González-Guillén 2021; Barnum 2002) emphasize the need for formal security analyses in quantum authentication to prevent novel attack vectors.

F. Critical Gaps and Future Directions

While quantum protocols (e.g., QKD, MDI-QKD) and post-quantum cryptographic algorithms (e.g., lattice-based schemes) are advancing independently, there is limited research on integrating them into existing classical infrastructure seamlessly. For example: Langley et.al. (2017) designed QUIC for modern internet traffic but did not address quantum-safe upgrades. Samandari & Gritti (2023) adapted MQTT for IoT with post-quantum signatures but noted compatibility issues with legacy devices. Diamanti et.al. (2016) emphasized QKD's reliance on trusted nodes, which conflicts with decentralized network architectures. Bloom et.al. (2022)simplified QKD experiments for undergraduates, but most curricula lack hands-on training in post-quantum cryptography or quantum authentication (Cardoso-Isidoro & Delgado, 2023). Industry professionals often lack familiarity with quantum-safe migration strategies (Zeydan et.al., 2024). Many quantum authentication schemes (e.g., Kanamori et.al., 2009; Cardoso-Isidoro & Delgado, 2023) lack rigorous security proofs against adaptive quantum adversaries. Attacks like those on Zawadzki's protocol (González-Guillén et.al., 2021) reveal vulnerabilities in ad-hoc designs.

IV. CONCLUSION

The rapid progress in quantum cryptography and post-quantum cryptography showcases excellent developments in combination with future challenges in securing communications infrastructure from attacks by quantum computers. This set of 18 papers captures breakthrough developments in quantum key distribution (QKD), new approaches to quantum authentication, and integration of post-quantum cryptography in classical networking protocols. Developments in quantum dot single-photon emitters (Bozzio et.al., 2022), measurement-device-independent QKD (Lo et.al., 2012), and lattice-based post-quantum TLS 1.3 authentication (Sikeridis et.al., 2020) demonstrate the potential of the field to bridge theoretical and practical vulnerabilities. However, critical challenges remain. The interoperability of classical and quantum systems remains a bottleneck, with few architectures for hybrid protocols that combine QKD with post-quantum primitives. The scalability of quantum technology such as entanglement-swapping technology (Basset et.al., 2019) is constrained by cost and environmental limitations, whereas resource-poor IoT networks demand low-overhead, energy-conserving approaches (Samandari & Gritti, 2023). Additionally, the lack of standardized proof of security for hybrid systems and the lack of professionals' quantum literacy (Bloom et.al., 2022) pose risks for mass adoption. To bridge these discrepancies, future work must focus on:

Collaborative Standardization of quantum-safe protocols like integration of NIST PQC with QKD.

Education Initiatives to give researchers and engineers experience in practical quantum cryptography.

Hardware Innovation to miniaturize quantum technology to make deployment cheaper.

Hybrid Security Methods that merge quantum and post-quantum methods for transitional robustness.

As quantum computing redefines the landscape of cybersecurity, the task is to transition from proof-of-principle demonstrators to functional, interoperable technology in practice. Through interdisciplinary research—among academia, industry, and policymakers—the community has the capability to counter quantum-related risks while opening doors to secure communications infrastructure powered by quantum technology. Reaching a quantum-safe future is not only a technical challenge but also a collective effort requiring urgency, ingenuity, and global coordination.

DECLARATION STATEMENT

After aggregating input from all authors, I must verify the accuracy of the following information as the article's author.

- **Conflicts of Interest/ Competing Interests:** Based on my understanding, this article has no conflicts of interest.
- **Funding Support:** This article has not been sponsored or funded by any organization or agency. The independence of this research is a crucial factor in affirming its impartiality, as it has been conducted without any external sway.
- **Ethical Approval and Consent to Participate:** The data provided in this article is exempt from the requirement for ethical approval or participant consent.
- **Data Access Statement and Material Availability:** The adequate resources of this article are publicly accessible.
- **Authors Contributions:** The authorship of this article is contributed equally to all participating individuals.

REFERENCES

1. Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H. (2002). Quantum cryptography. Reviews of Modern Physics, 74(1), 145–195 DOI: https://doi.org/10.1103/RevModPhys.74.145
2. Bozzio, M., Vyvlecka, M., Cosacchi, M., Nawrath, C., Seidelmann, T., Loredo, J. C., Portalupi, S. L., Axt, V. M., Michler, P., & Walther, P. (2022). Enhancing quantum cryptography with quantum dot single-photon sources. npj Quantum Information, 8(104). DOI: https://doi.org/10.1038/s41534-022-00626-z
3. Bloom, Y., Fields, I., Maslennikov, A., & Rozenman, G. G. (2022). Quantum Cryptography—A Simplified Undergraduate Experiment and Simulation. Physics, 4(1), 104–123. DOI: https://doi.org/10.3390/physics4010009
4. Basset, F. B., Rota, M. B., Schimpf, C., Tedeschi, D., Zeuner, K. D., Covre da Silva, S. F., Reindl, M., Zwiller, V., Jöns, K. D., Rastelli, A., & Trotta, R. (2019). Entanglement Swapping with Photons Generated on Demand by a Quantum Dot. Physical Review Letters, 123(16), 160501. DOI: https://doi.org/10.1103/PhysRevLett.123.160501
5. Cardoso-Isidoro, C., & Delgado, F. (2023). Quantum authentication using double teleportation. Journal of Physics: Conference Series, 2448(1), 012018 https://iopscience.iop.org/article/10.1088/1742-6596/2448/1/012018/pdf
6. Barnum, H., Crépeau, C., Gottesman, D., Smith, A., & Tapp, A. (2002). Authentication of quantum messages. arXiv preprint arXiv:quant-ph/0205128 https://arxiv.org/pdf/quant-ph/0205128
7. González-Guillén, C. E., González Vasco, M. I., Johnson, F., & Pérez del Pozo, Á. L. (2021). An Attack on Zawadzki's Quantum Authentication Scheme. Entropy, 23(4), 389. DOI: https://doi.org/10.3390/e23040389
8. Boykin, P. O., & Roychowdhury, V. (2000). Optimal Encryption of Quantum Bits. arXiv preprint arXiv:quant-ph/0003059. https://arxiv.org/abs/quant-ph/0003059
9. Liu, J., Wang, H., Sun, Y., Fu, C., & Guo, J. (2015). Real-coded quantum-inspired genetic algorithm-based BP neural network algorithm. Mathematical Problems in Engineering, 2015, 571295. DOI: https://doi.org/10.1155/2015/571295
10. Wang, H., Liu, J., Zhi, J., & Fu, C. (2013). The improvement of quantum genetic algorithm and its application on function optimization. Mathematical Problems in Engineering, 2013, 730749. DOI: https://doi.org/10.1155/2013/730749
11. Kanamori, Y., Yoo, S. M., Gregory, D. A., & Sheldon, F. T. (2009). Authentication protocol using quantum superposition states. International Journal of Network Security, 9(2), 101–108. http://ijns.jalaxy.com.tw/contents/ijns-v9-n2/ijns-2009-v9-n2-p101-108.pdf
12. Sikeridis, D., Kampanakis, P., & Devetsikiotis, M. (2020). Post-quantum authentication in TLS 1.3: A performance study. Network and Distributed Systems Security (NDSS) Symposium 2020. https://eprint.iacr.org/2020/071.pdf
13. Samandari, J., & Gritti, C. (2023). Post-quantum authentication in the MQTT protocol. Journal of Cybersecurity and Privacy, 3(3), 416–434 DOI: https://doi.org/10.3390/jcp3030021
14. Langley, A., Riddoch, A., Wilk, A., Vicente, A., Krasic, C., Zhang, D., Yang, F., Kouranov, F., Swett, I., Iyengar, J., et.al. (2017). The QUIC transport protocol: Design and internet-scale deployment. Proceedings of SIGCOMM '17, Los Angeles, CA, USA, August 21-25, 2017 DOI: https://doi.org/10.1145/3098822.3098842
15. Li, T., Liu, B., & Zhang, J. (2024). Quantum privacy query protocol based on GHZ-like states. Applied Sciences, 14(608). DOI: https://doi.org/10.3390/app14020608
16. Lo, H.-K., Curty, M., & Qi, B. (2012). Measurement device-independent quantum key distribution. Physical Review Letters, 108(13), 130503. DOI: https://doi.org/10.1103/PhysRevLett.108.130503
17. Diamanti, E., Lo, H.-K., Qi, B., & Yuan, Z. (2016). Practical challenges in quantum key distribution. npj Quantum Information, 2, 16025. DOI: https://doi.org/10.1038/npjqi.2016.25
18. Zeydan, E., Turk, Y., Aksoy, B., & Ozturk, S. B. (2024). Recent advances in post-quantum cryptography for networks: A survey. Applied Sciences, 14(20608). DOI: http://dx.doi.org/10.1109/MobiSecServ50855.2022.9727214
19. M, G., B, G., & Wahi, A. (2020). Quantum Key Distribution Based-on Refraction and Polarization Entanglement. In International Journal of Recent Technology and Engineering (IJRTE) (Vol. 8, Issue 6, pp. 2911–2918). DOI: https://doi.org/10.35940/ijrte.f8222.038620
20. Tom, Dr. J. J., P. Anebo, Dr. N., Onyekwelu, Dr. B. A., Wilfred, A., & E. Eyo, R. (2023). Quantum Computers and Algorithms: A Threat to Classical Cryptographic Systems. In International Journal of Engineering and Advanced Technology (Vol. 12, Issue 5, pp. 25–38). DOI: https://doi.org/10.35940/ijeat.e4153.0612523
21. Shivani Gaba, Shifali Singla, Deepak Kumar, A Genetic Improved Quantum Cryptography Model to Optimize Network Communication. (2019). In International Journal of Innovative Technology and Exploring Engineering (Vol. 8, Issue 9S, pp. 256–259). DOI: https://doi.org/10.35940/ijitee.i1040.0789s19

AUTHOR'S PROFILE

Srivaramangai Ramanujam, Head, Department of IT, University of Mumbai, India. Having 24 years of experience in teaching and 6 years in industry. The specialization areas are artificial intelligence, security, and image processing. Has industry experience in web development and report code generators. Has published more than 35 International journal papers, 25 conference papers, resource persons for various workshops and chaired sessions. She is actively involved in project management of various projects undertaken by the university for the automation of administrative functions. The papers relevant to Cyber Security include "Assessment of Deep Packet Inspection System of Network Traffic and Anomaly Detection", Enhancing Security using ECC in Cloud Storage", "Recapitulation of the Use of Machine Learning for Prevention of DDoS Attack on SDN Controller" and

"Unmasking Deceptive Websites: Harnessing Machine Learning For Phishing Detection".

Furkan Sayyed, is a master's student of Cyber Security in the Department of Information Technology, University of Mumbai, Mumbai, India**.** Passionate about technology and cybersecurity, he is a versatile professional with a keen interest in Python and JavaScript Full Stack web development. With a creative mindset and a knack for problem-solving, he thrives on building innovative web applications and exploring the fascinating world of cybersecurity and Quantum Technology. He had worked on a Resume Ranking system developed in Django which uses a Machine Learning model to rank the resume with a score of similarity with the job description. He is currently involved in the portal development for the University of Mumbai for managing research project funding and other funding received from various funding agencies.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of the Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)/ journal and/or the editor(s). The Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP) and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.