



Entanglement-Coupled Dynamic Behaviour Authentication (ECDBA): A Device Behaviour Verification Framework

Vishnu Singh

Department of Physics

K.M. (Krishna Mohan) University, Mathura, Uttar Pradesh, India

ABSTRACT: Quantum communication is becoming an important technology for secure data transmission because it provides better protection against eavesdropping than classical communication systems. Many existing authentication methods verify the identity of the communicating user or the registered quantum device before communication starts. Recent research has improved authentication by introducing quantum key agreement, quantum random number generation (QRNG) and multi-layer authentication techniques. These methods improve communication security, but they mainly verify the user identity or registered device. They do not continuously check whether the physical quantum device is behaving normally during the communication session. As a result, hardware modification, fake device replacement or abnormal device behaviour may remain undetected, creating a potential security risk.

To address this limitation, this paper proposes a new framework called Entanglement-Coupled Dynamic Behaviour Authentication (ECDBA). Instead of relying only on user or device identity, the proposed framework continuously verifies the real-time behaviour of the quantum device throughout the communication process. It analyses important behavioural parameters such as timing response, detector response, phase stability, polarization behaviour and entanglement fidelity to generate a dynamic authentication fingerprint for every communication session. Any unexpected change in these parameters is treated as a possible security threat, allowing the system to stop communication before sensitive information is exchanged.

The proposed framework is supported by a mathematical model and theoretical security analysis. The expected results indicate that ECDBA can improve authentication reliability, strengthen protection against replay attacks, fake device attacks and hardware manipulation, and provide an additional layer of security for future quantum communication systems.

Keywords: Quantum communication, Behaviour authentication, Device fingerprint, Quantum security, ECDBA.

I. INTRODUCTION

Today, people use passwords, fingerprints, face recognition and one-time passwords (OTP) to access their mobile phones, computers and online accounts. These methods help verify the identity of the user before access is given. In quantum communication, authentication methods also work in a similar way. Their main purpose is to verify that the communicating user is genuine before exchanging sensitive information. At the same time, quantum communication provides a highly secure way to transfer information by using the principles of quantum mechanics. Unlike classical communication, any attempt to intercept the communication can be detected, making quantum communication one of the most promising technologies for future secure networks [1].

One of the most widely used quantum communication techniques is Quantum Key Distribution (QKD). Protocols such as BB84 and E91 allow two users to establish a secure secret key for communication [2,3]. In recent years, researchers have also focused on improving authentication before the key exchange process.

Recently, a research paper titled “**Mutual Authentication Quantum Key Agreement Protocol with Single-Particle Measurement (2025)**” proposed an improved method to verify the identity of communicating users before quantum key agreement [4]. In this protocol, both communicating users first authenticate each other before generating the shared quantum key. The protocol uses single-particle measurement and Bell-state operations to establish a secure shared key while reducing dependence on trusted third parties. However, it mainly verifies the identity of the users before communication and does not continuously monitor the behaviour of the physical quantum device during the communication session. Later, another research paper “**Hybrid Quantum Authentication Model (HQAM) (2026)**” introduced a stronger multi-layer authentication framework using quantum random numbers and digital fingerprints to improve communication security [5]. In this framework, QRNG generates unpredictable random

numbers, while digital fingerprints help verify the registered device and user. This improves authentication reliability against several security attacks. However, the framework does not continuously verify whether the physical quantum device behaves normally during communication, such as changes in timing response, detector response or other operational characteristics. These studies improve authentication, but they mainly verify the user or the registered communication process. They do not continuously check whether the physical quantum device is behaving normally during communication.

In real-life applications, this can become an important security problem. A genuine user may unknowingly use a damaged or modified quantum device. An attacker may also replace the original device with a fake one or manipulate its hardware. In such situations, the user identity may still appear valid, but the device may not behave like the original one. Existing authentication methods may not detect these changes because they mainly focus on user authentication instead of real-time device behaviour.

To solve this problem, this paper proposes a new framework called Entanglement-Coupled Dynamic Behaviour Authentication (ECDBA). The proposed framework checks not only the user but also the real-time behaviour of the quantum device. It continuously monitors the device timing pattern (timing response), signal response (detector response), light wave behaviour (phase) and light polarization, and combines these characteristics with entanglement fidelity, which represents the quality of the quantum connection, to generate a dynamic authentication fingerprint for every communication session.

The proposed framework is supported by a mathematical model and a theoretical security analysis. The expected results suggest that ECDBA can improve device authentication, reduce replay attacks and fake device attacks, and provide an additional layer of security for future quantum communication systems.

II. LITERATURE REVIEW

Traditional communication systems mainly use classical authentication methods such as passwords, One-Time Passwords (OTP) and Multi-Factor Authentication (MFA) to verify the identity of the user. These methods are simple, widely used and help protect user accounts in daily life [6]. However, they mainly verify the user before communication starts and do not provide quantum-level security. As quantum computing is developing rapidly, researchers are exploring quantum-based authentication methods to make future communication more secure. Unlike classical communication, quantum communication uses the laws of quantum mechanics to protect information. If someone tries to intercept the transmitted quantum data, the quantum state changes automatically, making the attack detectable. This property makes quantum communication more secure than many traditional communication methods[1].

One of the first and most widely used quantum communication protocols is BB84. In this protocol, the sender (Alice) sends photons to the receiver (Bob). Each photon carries one quantum bit (qubit) using different polarization states. Bob measures the received photons using randomly selected measurement bases. After the transmission, Alice and Bob compare only their measurement bases through a public communication channel. The measurement results obtained with matching bases are kept to generate the secret key, while the remaining results are discarded. If an attacker tries to observe the photons during transmission, the quantum states change automatically and the communication becomes insecure. This allows both users to detect the presence of an attacker before using the generated key [2, pp. 175–179].

Another important protocol is E91, which is based on quantum entanglement. In this method, a source creates a pair of entangled photons. One photon is sent to Alice and the other to Bob. Even if the two photons are separated by a long distance, their measurement results remain strongly correlated because of quantum entanglement. If an attacker interferes with the communication, this correlation changes and the attack can be detected. Because of this property, E91 has become an important foundation for secure quantum communication and future quantum networks [3].

As quantum communication developed, researchers realised that secure key distribution alone is not sufficient. The communicating users should also be authenticated before starting the key agreement process. To solve this problem, Yang et al. (2025) proposed a Mutual Authentication Quantum Key Agreement Protocol with Single-Particle Measurement. In this protocol, both communicating parties verify each other's identity before generating the shared quantum key. The protocol uses single-particle measurement and Bell-state operations to improve authentication efficiency while reducing dependence on trusted third parties. The authors also analysed the protocol against several common attacks and showed that it provides secure mutual authentication before key agreement [4, pp. 1–6]. However, the authentication process mainly verifies the identities of the communicating users. It does not continuously verify whether the physical quantum device itself behaves normally throughout the communication session [4, pp. 6–7].

Another recent study by Belkhir et al. (2026) proposed the Hybrid Quantum Authentication Model (HQAM). The main goal of this framework is to make user authentication stronger by combining Quantum Random Number Generator (QRNG), digital identity verification and multiple authentication layers. During the authentication process, the QRNG generates true random values that are used to create secure fingerprints, session keys and other authentication parameters. These random values make it more difficult for attackers to predict or copy authentication information. The framework also uses post-quantum cryptography and formal verification to improve the reliability of the authentication process and compares its performance with several existing authentication methods [5, pp. 1–19].

After the user is successfully authenticated and the session key is generated, secure communication begins. However, the framework mainly focuses on the authentication stage. It does not include a mechanism to continuously verify whether the physical quantum device is still behaving like the original registered device during the communication session. If the behaviour of the device

changes because of hardware faults, device replacement or physical tampering after authentication, these changes are not continuously checked by the framework [5, pp. 19–20].

This limitation creates an opportunity for further research. Instead of verifying only the user's identity, the proposed ECDBA framework also verifies the real-time behaviour of the quantum device. It continuously analyses timing pattern, signal pattern, phase pattern, polarization pattern, noise pattern and entanglement fidelity. These behaviour features are compared with the registered behaviour profile before making the final security decision. As a result, ECDBA provides an additional security layer that complements existing authentication methods rather than replacing them.

III. METHODOLOGY

The proposed Entanglement-Coupled Dynamic Behaviour Authentication (ECDBA) framework is designed to improve the security of quantum communication. In many existing authentication methods, the system checks only the identity of the users before communication starts. After the authentication is completed, the communication continues normally. However, physical quantum device is not checked again during the communication session. If the device becomes faulty, is replaced, or its behaviour changes because of an attack, the communication may become unsafe even though the user is genuine.

To solve this problem, the proposed ECDBA framework adds one more verification layer. Along with user authentication, it also checks whether the quantum device continues to behave like the original registered device. This is done by continuously observing the behaviour of the device during communication and comparing it with its stored reference behaviour.

3.1 Working Process

The complete working process of the proposed framework is explained below.

Step 1: Device Registration

Before the communication starts, the original quantum device is registered. During this stage, the Quantum Behaviour Monitoring Unit records the normal operating behaviour of the device. It observes how the device normally responds while generating and receiving quantum signals. The collected information is stored in the Reference Behaviour Database. This stored information becomes the reference behavioural profile of that device and is used in future communication sessions.

Step 2: User Authentication

After device registration, Alice and Bob perform the normal quantum authentication process. Their identities are verified using the existing authentication protocol before the secret key is generated. If both users are successfully authenticated, the communication session is allowed to start.

Step 3: Quantum Communication

After successful authentication, Alice and Bob exchange quantum information using entangled photons through the quantum channel. At the same time, the Quantum Behaviour Monitoring Unit starts observing the physical behaviour of the quantum device. This monitoring process works continuously in the background and does not interrupt the communication.

Step 4: Behaviour Monitoring

During communication, the Quantum Behaviour Monitoring Unit records the real-time operating behaviour of the device. It measures different characteristics such as the detector timing pattern, signal pattern, phase pattern, polarization pattern, detector response, background noise pattern and entanglement fidelity. These values together represent the behavioural signature of the quantum device. Under normal conditions, these patterns remain almost the same. If the hardware changes or the device becomes faulty, these patterns also change.

Step 5: Behaviour Comparison

The Behaviour Analysis Engine receives the monitored data from the Quantum Behaviour Monitoring Unit and compares it with the reference behavioural profile stored in the Reference Behaviour Database. Instead of checking only one parameter, the engine compares the complete behavioural pattern of the device. Small differences caused by temperature, normal hardware variation or environmental noise are accepted by using a predefined threshold. However, if the difference becomes larger than the allowed limit, the system considers the device behaviour abnormal.

Step 6: Security Decision

Finally, the system combines the results of user authentication and behavioural verification. If the user identity is correct and the device behaviour matches the stored reference profile, secure communication continues normally. If the behaviour does not match, the system immediately stops the communication session and generates a security alert. In this way, the system protects the communication even when the user identity is genuine but the physical device is no longer trusted.

3.2 System Architecture

The proposed system contains four main components. The first component is the User Authentication Module, which verifies the identity of Alice and Bob before communication begins. The second component is the Quantum Behaviour Monitoring

Unit (QBMU). This unit continuously observes the physical behaviour of the quantum device while communication is running. The third component is the Reference Behaviour Database (RBD), where the normal behaviour of the original device is stored during the registration stage. The fourth component is the Behaviour Analysis Engine (BAE). It compares the current behaviour of the device with the stored reference behaviour and makes the final security decision.

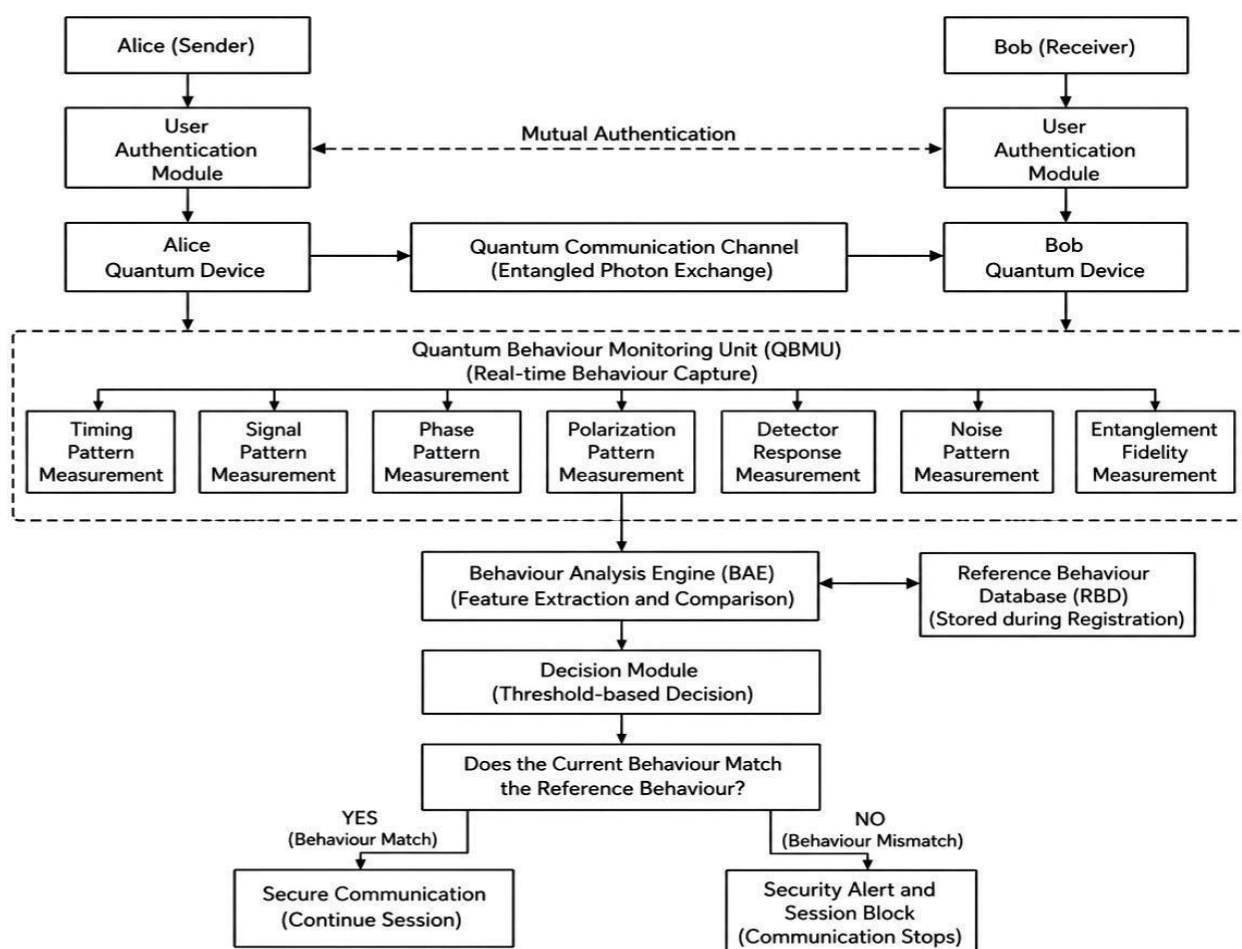


Fig. 1 Architecture of the proposed ECDBA framework.

figure 1 shows the complete architecture of the proposed ECDBA framework. It explains the complete authentication workflow, from user verification to continuous device behaviour monitoring. Communication continues only when the observed behavioural profile matches the expected profile; otherwise, the session is blocked.

3.3 Working Example

Consider a simple example of a defence communication system. During installation, the original quantum device is registered and its normal behaviour is stored in the Reference Behaviour Database. Later, an authorised officer starts a communication session. The user authentication is completed successfully, so the system allows communication to begin. While the communication is running, the Quantum Behaviour Monitoring Unit continuously observes the detector timing pattern, signal pattern and phase pattern. After a few seconds, the Behaviour Analysis Engine finds that these values are significantly different from the stored reference profile. This may happen because the device has developed a hardware fault, has been replaced, or has been modified by an attacker. Although the authorised user is genuine, the system recognizes that the physical device is behaving differently. Therefore, it immediately blocks the communication and generates a security alert before confidential information is exchanged.

The proposed ECDBA framework therefore performs two security checks at the same time. The first check verifies the identity of the communicating user, while the second check verifies the real-time behaviour of the quantum device. By combining these two verification methods, the proposed framework provides stronger protection than systems that depend only on user authentication.

3.4 Summary

The proposed ECDBA framework combines user authentication with continuous behavioural verification of the quantum device. By analysing the device behaviour in real time, the system can detect abnormal operation even after successful user authentication. This approach improves the overall reliability and security of quantum communication systems.

IV. MATHEMATICAL FRAMEWORK OF ECDBA

The proposed ECDBA framework verifies whether the quantum device is behaving like its original registered device. Instead of Mathematical Framework of ECDBA

The proposed ECDBA framework verifies whether the quantum device is behaving like its original registered device. Instead of checking only one parameter, the framework compares several behavioural features together. The mathematical model used for this comparison is explained below.

4.1 Behaviour Representation

During communication, the Quantum Behaviour Monitoring Unit (QBMU) records the important behavioural features of the quantum device. These features form the behavioural profile.

$$B = (T, S, P, L, N, F)$$

Where,

T = Timing Pattern

S = Signal Pattern

P = Phase Pattern

L = Polarization Pattern

N = Noise Pattern

F = Entanglement Fidelity

The reference behaviour stored during device registration is represented as

$$Br = (Tr, Sr, Pr, Lr, Nr, Fr)$$

The current behaviour measured during communication is

$$Bc = (Tc, Sc, Pc, Lc, Nc, Fc)$$

4.2 Behaviour Comparison

The Behaviour Analysis Engine (BAE) compares each behavioural feature with the stored reference profile.

$$Di = ABS(Bri - Bci)$$

Where,

Di = Difference of the i-th feature

Bri = Reference feature

Bci = Current feature

The overall behaviour score is calculated as

$$D = (dT + dS + dP + dL + dN + dF) / 6$$

A smaller value of D indicates normal device behaviour, while a larger value indicates behavioural deviation.

4.3 Authentication Decision

The overall behaviour score is compared with a predefined threshold value.

If $D \leq Th \rightarrow$ Behaviour Match

If $D > Th \rightarrow$ Behaviour Mismatch

The final authentication decision is obtained by combining user authentication and behaviour verification.

$$A = U \text{ AND } M$$

Where, A = Final Authentication Result

U = User Authentication Result

M = Behaviour Match Result

If A = TRUE, secure communication continues. Otherwise, the communication session is terminated and a security alert is generated.

V. RESULTS AND DISCUSSION

proposed ECDBA framework was developed to improve the security of quantum communication. Existing authentication methods mainly verify the identity of the users before communication starts. However, they do not continuously check whether the quantum device is behaving normally during communication. The proposed ECDBA framework solves this problem by adding real-time device behaviour verification. This additional verification helps the system make a more reliable security decision.

V.1 Expected Performance

Based on the proposed methodology and mathematical framework, the ECDBA framework is expected to provide better security than authentication methods that verify only the user identity. During communication, the Quantum Behaviour Monitoring Unit (QBMU) continuously monitors the behaviour of the quantum device. At the same time, the Behaviour Analysis Engine (BAE) compares the current behaviour with the stored reference behaviour profile.

If both the user authentication and behaviour verification are successful, secure communication continues normally. If the behaviour changes beyond the allowed threshold, the system immediately generates a security alert and stops the communication.

This process helps detect hardware faults, device replacement and unexpected changes in device behaviour before confidential information is transmitted.

Although this work presents a theoretical framework, the proposed system is expected to provide an additional layer of security without changing the basic quantum communication process.

V.2 Comparison with Existing Methods

V.3 Table 1 compares the proposed ECDBA framework with recent authentication methods.

Feature	Classical authentication (Password, OTP, MFA)	Yang et al. (2025)	HQAM (2026)	Proposed ECDBA
User authentication	Yes	Yes	Yes	Yes
Quantum key agreement	No	Yes	Yes	Yes
QRNG support	No	No	Yes	Yes
Multi-layer authentication	Limited	No	Yes	Yes
Continue device behaviour verification	No	No	No	Yes
Real time behaviour monitoring	No	No	No	Yes
Behaviour profile matching	No	No	No	Yes
Behaviour based security decision	No	No	No	Yes
Authentication during communication	No	No	No	Yes
Device tampering detection	Limited	No	No	Yes

Table 1 shows that the proposed ECDBA framework keeps the strengths of existing authentication methods while adding continuous device behaviour verification. This additional feature helps improve the reliability of quantum communication by checking both the user and the physical device.

5.3 Discussion

The literature review shows that recent research has improved quantum authentication in different ways. The 2025 protocol focuses on secure mutual authentication before key agreement. The HQAM model adds multiple authentication layers to make the authentication process stronger. These methods improve user verification, but they mainly focus on confirming the identity of the communicating users.

The proposed ECDBA framework extends this idea by also checking the behaviour of the quantum device during communication. Instead of asking only “Is the user genuine?”, the system also asks “Is the device behaving like the original registered device?” This additional check helps detect problems that may not be found by user authentication alone.

Another advantage of the proposed framework is that it does not replace the existing authentication process. It works as an additional security layer. This means that the framework can be added to existing quantum communication systems with only a small change to the overall security process.

Overall, the proposed ECDBA framework combines user authentication with device behaviour verification. This dual verification approach can improve the reliability and security of future quantum communication systems.

5.4 Limitations

The proposed ECDBA framework is a theoretical model supported by system architecture and mathematical analysis. It has not yet been tested on a real quantum communication system. Therefore, the practical performance of the framework still needs to be verified through hardware implementation and experimental testing.

The framework also depends on accurate behaviour monitoring. If the behaviour data are not measured correctly, the final decision may be affected. Future experimental studies will help evaluate the performance of the framework under different operating conditions.

5.5 Future Scope

The proposed ECDBA framework can be applied to future quantum communication systems where both user identity and device trust are important. It may be useful in defence communication, banking, healthcare, satellite communication and future quantum internet applications.

Future work can focus on building a hardware prototype of the proposed framework and testing it in a real quantum communication environment. Advanced behaviour analysis methods may also be added to improve the accuracy and speed of behavioural verification.

VI. CONCLUSION

In this paper, we proposed the Enhanced Continuous Device Behaviour Authentication (ECDBA) framework to improve the security of quantum communication. Existing authentication methods can verify whether the user is genuine or not. However, they do not check whether the quantum device is still behaving like the original registered device during communication.

To solve this problem, we added one more security layer called device behaviour verification. In our framework, the Quantum Behaviour Monitoring Unit (QBMU) continuously checks important behaviour features of the quantum device, such as timing pattern, signal pattern, phase pattern, polarization pattern, noise pattern and entanglement fidelity. The Behaviour Analysis Engine (BAE) compares these features with the registered behaviour profile before making the final decision.

If both the user authentication and the device behaviour verification are successful, the communication continues safely. If the behaviour of the device changes beyond the allowed limit, the system stops the communication and generates a security alert. In this way, the proposed framework helps detect hardware faults, device replacement and other abnormal behaviour that may not be detected by existing authentication methods.

This work presents a theoretical framework supported by system architecture and a mathematical model. In future work, the proposed framework can be tested on a real quantum communication system and improved through hardware implementation and experimental validation. The ECDBA framework may also be useful for future applications such as defence communication, banking, satellite communication and the quantum Internet.

Overall, the proposed ECDBA framework adds an extra layer of security to quantum communication by verifying not only the user but also the behaviour of the quantum device. This approach can make future quantum communication systems more reliable and secure.

REFERENCES

- [1] Nielsen, M. A., & Chuang, I. L. (2010). *Quantum Computation and Quantum Information* (10th Anniversary ed.). Cambridge University press
- [2] Bennett, C. H., & Brassard, G. (1984). Quantum Cryptography: Public Key Distribution and Coin Tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (pp. 175–179). Bangalore, India.
- [3] Ekert, A. K. (1991). Quantum Cryptography Based on Bell's Theorem. *Physical Review Letters*, 67(6), 661–663.
- [4] Yang, H., Yi, Z., Lu, S., & Wang, M. (2025). Mutual authentication quantum key agreement protocol with single-particle measurement. *Frontiers in Physics*, 13, 1563674. DOI: 10.3389/fphy.2025.1563674
- [5] Belkhir, M., Benkaouha, H., & Benkhelifa, E. (2026). A Hybrid Quantum Authentication Model (HQAM) with QRNG Enhanced Protection. *International Journal of Information Security*, 25, Article 41. DOI: 10.1007/s10207-026-01210-8
- [6] Stallings, W. (2020). *Cryptography and Network Security: Principles and Practice* (8th ed.). Pearson.