Al-Noor Journal of Engineering Management and Computer Science

ISSN: 3079-0689 (Online)

https://njemcs.edu.iq/index.php/njemcs/

A Hybrid ECC–Falcon Secure Handshake Protocol for Post-Quantum Authentication and Forward Secrecy

Dhamyaa Z. Fatah Al-Kerboly [1], and Omar A. Dawood[2]

[1,]Computer Science Department, College of Computer Science and Information Technology, University of Anbar, Anbar, Iraq.
[2] Electronic Computer Center, Computer Science Department, College of Computer Science and Information Technology, University of Anbar, Anbar, Iraq,

ARTICLE INFO

Article history:
Received 13-06-2026
Revised 13-06-2026
Accepted 28-06-2026
Available online 28-06-2026

Keywords:
Post-Quantum Cryptography
Elliptic-Curve Cryptography
Fast-Fourier Lattice-based Compact Signatures over NTRU(Falcon)
Digital Signature
Hybrid Cryptosystem

ABSTRACT

Quantum computing technology is developing at a pace that threatens classic public-key ciphers, including those based on integer factorization and elliptic-curve discrete logarithms. In response, it has been proposed to work towards a hybrid model that can be used in the short term and that is based on the combination of classical Elliptic-Curve Cryptography (ECC) and Post-Quantum Cryptographic (PQC) primitives, increasing security where classically secure key exchanges are used and found to be secure against quantum attacks. The proposed protocol combines ephemeral ECDH key exchange with Falcon-512 digital signatures to provide authenticated session establishment with forward secrecy. This work extends upon these results and assesses as well as justifies the construction of hybrid ECC-Lattice protocols, specifically ECC + Falcon, for quantum-safe authentication and authenticated key establishment. The results highlight that hybrid architecture provides a balanced trade-off between performance, interoperability, and robustness against quantum transition period, positioning them as an essential pathway in the global migration toward quantum-safe cryptography. The protocol was implemented and evaluated under controlled network conditions using 2000 protocol executions. Experimental results demonstrated an average handshake latency of 41.61 ms, a throughput of 24.03 handshakes per second, and a total communication overhead of 1434 bytes per handshake. The results indicate that the proposed Hybrid ECC–Falcon protocol achieves efficient authenticated key establishment while maintaining moderate communication costs. By combining ECDH-based forward secrecy with Falcon-512 post-quantum authentication, the protocol provides a practical solution for secure communications during the post-quantum transition period, particularly in post-quantum transition environments.

1. Introduction

Scalable Quantum Computing has in fact revolutionized the entire cryptographic ecosystem in practice. Shor's algorithm and low-error, high-speed implementations of Shor's algorithm cover RSA and ECC public key schemes mainstream applied today, destroying servicing strategy based upon time-tested safety in addition to enabling store-now, decrypt-later-style secrets to be susceptible via ancient-style security infrastructures[1]. This has made the development of quantum-resistant cryptographic mechanisms an urgent global priority for governments, industries, and research institutions[2].

In response to this threat PQC is presented with new types of mathematical hardness assumptions with a focus on certain lattice problems such as Learning with Errors (LWE)

Corresponding author E-mail address: dha24c1005@uoanbar.edu.iq
https://doi.org/10.71229/3mj7ne58

(Singh no date) and Shortest Vector Problem (SVP). These foundations are at the base of schemes like CRYSTALS-Kyber, CRYSTALS-Dilithium, Falcon, SPHINCS+, BIKE and HQC –most of the schemes which have either been adapted as standards NIST Helper bring it or are on the horizon as standards NIST bring it. Nevertheless, although theoretically secure, PQC schemes are often accompanied by practical complications in deployment, namely in the form of large key and signature sizes, increased memory consumption, higher computational overhead and lower correctness for constrained IoT and mobile environments[3].

Hybrid cryptography represents a practical compromise between classical and post-quantum security. Hybrid protocols based on the combination of ECC and PQC mechanisms can maintain backward compatibility while keeping security against the potential compromise of one component, either classical or post-quantum in nature.[4]Previous works demonstrate that quantum-safe hybrid key-exchange (X25519 + Kyber), hybrid digital signatures (ECDSA + Dilithium) and hybrid TLS/SSH cipher suites can provide cross-platform performance-optimized confidentiality and authenticity without significant performance overhead in a variety of platforms, including blockchain platforms, cloud networks, 6G communications, IPsec/VPN infrastructures, and PQC-capable IoT deployments[5]. Current hybrid post-quantum authentication protocols often suffer from large signature sizes, high communication overhead, or limited suitability for constrained IoT environments. Falcon-512 provides compact signatures and fast verification, making it a strong candidate for lightweight hybrid authenticated key exchange. Appropriate survey of literature as is considered in section 2 by the paper. Section 3: Theoretical background, Section 4: Proposed Hybrid ECC Falcon key exchange protocol, Section 5: Results and analysis, Section 6: Comparison with related work and Section 7: Conclusion.

2. Literature Survey

Transitioning to post-quantum cryptography poses massive hurdles for digital platforms: from networks to IoT, to financial services. Evaluate NIST-standardized algorithms and assess how they fare compared to classical schemes and even suggest hybrid systems that combine ECC with PQC such that the quantum-resilient aspect of the combined system would not be compromised while still being able to stay within the current industry infrastructure. They study security analysis and analyze performance, memory usage, protocol behavior in a diverse set of protocols such as TLS, SSH, and blockchain systems.

Fernández-Caramés (2020) [6] This paper presents a comprehensive survey with major contributions including an overview of the relevant IoT development progress the analysis of post-quantum public-key cryptosystems guidance on the selection of the appropriate scheme and challenges and future trends in IoT security. It highlights critical challenges, such as the fast-approaching reality of quantum computing, large key sizes that challenge even resource-poor devices slow demands for key generation large resource consumption in cryptosystem operation and the ongoing process of cryptosystem standardization. It also touches on IoT-specific optimizations the unsuitability of some cryptosystems for certain IoT hardware and the need to improve physical security against many types of attacks. This paper does a great job of summarizing the developments in post-quantum cryptography as well as the challenges that will need to be overcome to implement IoT with true quantum resistance.

Giron (2023) [7]The paper suggests hybrid PQC that combines classical and PQC algorithms to improve security. It shows that for hybrid Key Exchange Mechanisms (KEM), the latency remains below 2% compared to their pure-PQC versions. Anew PQ-Transition Challenge improves the speed 4.22x issuance of ACME certificates on average and reduces data transfer by 35%. The hybrid KEMTLS implementations incur small performance

overheads but a significant security increase. This Paper introduces wrapped certificates–an extension to the Public-Key Infrastructure (PKI) PKI Extended Lifetime Period (PKIELP) – delivering extra protection specifically towards constrained devices. Some limitations are Protocol coverage is still limited, usability of the TLS 1.3 Handshake Analyzer, and no support for KEMTLS with ACME certificates. Next research should examine how to modify PKIELP for V2V communication and assess hybrid KEMTLS in IoT and 5G, emphasizing the necessity for more robust security PQC algorithms. Overall, the study highlights the advantages of hybrid PQC and points out important areas that require more investigation.

Rubio Garcia (2024) [8] The author emphasizes the connection of QKD and PQC to the TLS protocol and discusses a few hybrid schemes such as Concatenation and XOR. Applying PQC (CRYSTALS-Dilithium) for authentication and QKD and PQC (CRYSTALS-Kyber) for key exchange results in 9% lower performance than the PQC-only approach. Nevertheless, the hybrid approach suffers from a performance penalty of 117% through QKD key retrieval challenges that take about 100 ms as illustrated when the research highlights that " QKD key retrieval and TLS 1.3 profiling both need to be further optimized to achieve higher performance while greatly enhanced security but also need to be improved to resist limited QKD key availability and possible Denial of Service attacks." The authors advocate for enhanced combination of QKD together with PQC and ask for a lot of exploration in resolving functionality and interoperability difficulties.

Cherkaoui Dekkaki and et .al (2024)[9] The study insight into PQC identifies the NIST standardization process which assesses algorithms such as CRYSTALS-Kyber and SPHINCS+, and stresses hybrid cryptography as part of a transition approach. However, it has significant drawbacks including serious weaknesses on some algorithms (e.g., SIKE Leap and Rainbow), performance issues with key sizes and computation complexity, and the requirement to continuously move along with an evolving quantum threat landscape. The transition period is also where integration problems crop up, especially in secure communication between classical systems and quantum-resistance systems. The PQC landscape is a mix of progress and daunting obstacles for protecting digital systems against the quantum threat.

Egbuagha & Ikwunna (2025) [10] This paper reviews the integration of PQC to communication protocols, highlighting critical findings and challenges. Highlights include how strong security can often be achieved by classical and PQC hybrid implementations at only low resource costs CRYSTALS-Dilithium and CRYSTALS-Kyber as the leading PQC algorithms and feasibility of PQC integration even on such constrained devices as IoT. The adoption of hybrid KEX mechanisms in standards (e.g. KEMs in OpenSSH 10) Drawbacks: Performance overheads, backward compatibility and interoperability hurdles PKI integration complexity no real-world testing of PQC Undeveloped tooling for PQC signatures in order to effectively transition over towards quantum-resistant communication peers will need to cooperate with more than just other communication technology, and between various parties.

Wang & Ismail (2025) [11] The document presents the addition of HCF – Hybrid Cryptographic Framework classical and PQC algorithms with formal security proofs. It uses discrete optimization based on NSGA-II to choose PQC algorithms within a latency, storage, and energy envelope. In-depth metrics comparing various PQC schemes (Kyber, Dilithium, Falcon, SPHINCS+, McEliece). Case studies of JPMorgan Chase, Ethereum, and other entities are used as examples of how this framework is applied in finance, blockchain, and IoT contexts. It measures trade-offs, for example pointing out that Kyber-768 adds 15-20% to TLS handshake latency. It also discusses side-channel resistance but points out some limitations: it is based on literature performance without original experiments, may be too complex for constrained environments, and does not give

much practical guidance on deployment. IOSCC: Energy consumption benchmarks for IoT are limited sources, suggesting a need for broader validation.

Although previous studies have extensively investigated post-quantum cryptography, hybrid TLS deployments, and lattice-based digital signatures, limited attention has been given to lightweight authenticated key-exchange protocols that combine the efficiency of ECC with the compact post-quantum authentication capabilities of Falcon-512. Existing PQC-only approaches often introduce considerable communication and computational overhead, while many hybrid solutions focus primarily on migration frameworks rather than practical authenticated handshake protocols. Furthermore, few studies provide a detailed performance evaluation of ECC–Falcon integration in in post-quantum transition environments . Therefore, this work proposes a Hybrid ECC–Falcon authenticated handshake protocol that combines ECDH-based forward secrecy with Falcon-512 post-quantum authentication to achieve efficient and practical secure session establishment during the post-quantum transition period.

3. Theoretical Background

This section describes the mathematical and cryptographic basis for the hybrid key-exchange protocol we propose. This protocol offers a unique double-hardness authenticated key-Exchange Mechanism (KEM) combining with the classical hardness present in ECC signatures, along with the PQC security promises offered by Falcon lattice-based signatures.

3.1 Preliminaries

This initial stage lists the basic concepts, expressions and mathematical tools necessary for the reader to digest the following sections in a research project. Notation assumptions and relevant background information they assumption, consistency and clarity.

3.2 Notation

We donate to $\mathcal{A}$, $\mathcal{B}$ Communication parties (e.g., Alice and Bob), λ Security parameter, $\mathbb{G}$ Elliptic curve group of prime order, $\mathcal{P}$ Large prime defining the finite field $\mathbb{F}_p$, E(F_p) Elliptic curve defined over finite field $\mathbb{F}_p$, G Generator point of the elliptic curve group, n Order of the base point G, d_A,d_B Ephemeral ECC private keys of $\mathcal{A}$ and $\mathcal{B}$, Q_A , Q_B ECC public key of $\mathcal{A}, B$, (PK_A^{PQC},SK_A^{PQC})Falcon public/private key pair of $\mathcal{A}$,$\left(PK_B^{PQC}, SK_B^{PQC}\right)$ Falcon public/private key pair of $\mathcal{B}$, σ_A Falcon signature generated by $\mathcal{A}$, σ_B Falcon signature generated by $\mathcal{B}$, ‖ Concatenation operator, Falcon. Sign(sk, M) Falcon signing algorithm, Falcon. Verify(pk, M, σ)Falcon verification algorithm, N Fresh random nonce, $K_{session}$ Final derived session key, H (·) Cryptographic hash function (e.g., SHA-256)

3.3 Elliptic Curve Cryptography (ECC)

Elliptic Curve Cryptography (ECC) is based on the higher mathematical properties of elliptic curves over finite fields to offer high protection using smaller key sizes. This subsection provides a summary of the key to ECC operations and the algebraic structures and equations that are relevant for encryption, key exchange, and digital signatures.

I. Group Structure over GF(p)

Definition: At the heart of elliptic-curve cryptography lies the algebraic structure of elliptic curves defined over prime fields GF(p). Let $\mathbb{G}$ be a generator some point on the elliptic curve $E(\mathbb{F}_p)$,as defined in $|\mathbb{G}| = n, G \in E(\mathbb{F}_p)$, where n denotes the order of cyclic group generated by $\mathbb{G}$ [12].

II. A Weierstrass elliptic curve E over GF(p)

A Weierstrass elliptic curve E over GF(p) is defined by equation 1.

$$y^2 = x^3 + ax + b(mod\ p) \quad \ldots\ldots (1)$$

where the parameters a and b are integers included in the prime field GF(p) which satisfies in equ2.

$$4a^3 + 27b^2 \neq 0\ (mod\ p) \quad \ldots\ldots \quad (2)$$

to guarantee non-singularity consists of a set of points P = (x, y), with x, y ∈ GF(p) together with an extra point $\boldsymbol{O}$ called “point at infinity”.[13]

III. Short Weierstrass Form (NIST P-256)

The NIST P elliptic curves are Weierstrass curves over GF(p) and their parameters can be found in

The hybrid protocol we propose uses the NIST P-256 elliptic curve (secp256r1) and is defined in[14] short Weierstrass form in equation 3

$E: y^2 = x^3 - 3x + b(mod\ p)$…. (3) [15] .

IV. Private–Public Key Construction

A private–public key pair is defined as equation 4:[16]

$x \xleftarrow{\$} \{1, \dots, n-1\}, X = xG$ … (4)

The standard Elliptic-Curve Diffie–Hellman (ECDH) key agreement computes a shared point in 5,6 equations:

- Alice: $K_{\text{ECC}} = H(aB)$…… (5)
- Bob: $K_{\text{ECC}} = H(bA)$…….…. (6)
- $H(\cdot)$is a cryptographic hash function.

Where $a, A = aG$ are Alice's ephemeral keys,

$b, B = bG$ Bob's keys, and both values satisfy in 7:

$aB = bA = abG$. ……..… (7)

So both parties now have the same shared secret. ECC has the advantages of light weight and small key, so it is suitable for constraint environment. Since P-256 offers a good trade-off with respect to speed, security and usability P-256 is a good option for our hybrid scheme where the authentication component is a lattice-based signature [17].

3.4 Post-Quantum Cryptography and Lattice-Based Signatures

Lattice-based cryptography provides strong security against quantum adversaries. Falcon is an efficient signature scheme based on the Short Integer Solution (SIS) problem. A Falcon key pair as shown in equation (8) consists of:

$(pk_F, sk_F) \leftarrow$ Falcon.KeyGen()… …. (8)

The signature over a message M as shown in equation (9):

$\sigma \leftarrow$Falcon.Sign(sk_F, M) … … ….… (9)

Verification checks as shown in equation (10):

Falcon. Verify$(pk_F, M, \sigma) =$ True (10) [18]

Falcon offers post-quantum security, very small signatures (≈666 bytes for Falcon-512) and fast verification.

Falcon is used in the protocol not for key exchange but for authentication of the exchanged ECC ephemeral keys as shown in fig.1.

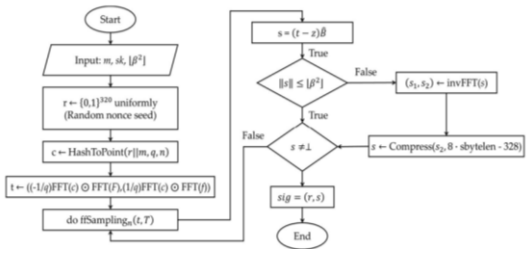

Figure 1. Falcon Digital signing process flowchart [19].

3.5 The GPV Framework for Lattice Signatures

The popular family of lattice-based digital signatures relies on the GPV (Gentry, Peikert, Vaikuntanathan) framework, which allows for strong post-quantum security. Not only does it use a hash-and-sign scheme (using a public key and a private trapdoor for signing), but it also achieves fast lattice signature sampling (by efficiently hashing messages to lattice points and sampling from a discrete Gaussian) [20]. It is quantum-resistant and its security relies on the Short Integer Solution (SIS) problem. Although Falcon is efficient, its signatures are still larger than the ECDSA ones in our scheme. Ever smaller digital signature sizes, up to 30–40% smaller in most recent advances with new sampling and coding methods & a similar level of security as we had before with all the old schemes[21].

4. METHODOLOGY

4.1 Proposed Hybrid ECC–Falcon Key Exchange Protocol

A hybrid ECC–Falcon key-exchange technique for creating safe and quantum-resistant sessions is presented in this section. And that would be classical elliptic-curve Diffie–Hellman (ECDH) for fast key agreement and forward

secrecy, combined with Falcon post-quantum signatures for strong authentication. The architecture, message flow, cryptographic operations, formal description of the algorithm, correctness and security analysis are described in the following subsections.

Protocol Overview

In this work, the proposal model used a combination of classical elliptic-curve cryptography (ECC) with the post-quantum Falcon signature scheme resulting in a hybrid key-exchange model, where the two components provide long-term security for different parameter ranges. Each party generates a public key using ephemeral ECC key pairs, fresh $(a, A = aG)$and $(b, B = bG)$per session, following the protocol with forward secrecy, and the shared secret is derived by ECDH as $K_{ECC} = H(aB) = H(bA)$.

In Falcon, each party signs its ephemeral public key (along with some identity information and a nonce) with its own Falcon private key ensuring authentication. The signatures (σ_A, σ_B) ensure that malicious agents cannot impersonate Alice or Bob and thus cannot give the other party malicious ECC keys, where they can execute a man-in-the-middle attack. This means the keying material is directly from the output of the ECDH and hashed together with a KDF of the session transcript containing all exchanged parameters (the public keys, the identities, and the signatures). This binding ensures resistance to tampering and provides a fully authenticated key-exchange (AKE) mechanism. Overall, this design achieves a secure and efficient hybrid authenticated key-exchange suitable for the post-quantum transition period. 4.3 Algorithm

4.2 Detailed Protocol Description

In this work, we present a hybrid ECC–Falcon key–exchange protocol, which allows Alice and Bob to securely establish a session key even in the presence of powerful classical and post–quantum adversaries. Both parties have a long-term Falcon key pair, and they each generate a new ephemeral elliptic-curve key pair per session to preserve forward secrecy. It begins with Alice sends her ephemeral ECC public key and a signed authentication message (identity and session nonce). Bob checks that signature and replies in the same way with his own signature and message. Post mutual authentication, they each compute the shared secret by elliptic-curve Diffie–Hellman and use its x coordinate to hash into a symmetric secret. From all parameters exchanged, a session transcript is created, and the session key itself is derived from a key derivation function, applied to the ECDH secret and the session transcript hash → This makes it impossible to use the session key if the entire protocol execution is not confirmed.

4.3 Algorithm 1: Hybrid ECC–Falcon Handshake

Algorithm 1: Hybrid ECC–Falcon Secure Handshake Protocol

Input
- Long-term Falcon public keys:(PK_A^{PQC} , PK_B^{PQC})
- Long-term Falcon secret keys: (SK_A^{PQC} SK_B^{PQC})

Output
- Shared session key ($K_{session}$)

Initialization
1. A generates Falcon-512 key pair :(PK_A^{PQC} , SK_A^{PQC})
2. B generates Falcon-512 key pair (PK_B^{PQC}, SK_B^{PQC})
3. Generate a fresh session nonce ($N \leftarrow \{0,1\}^{128}$)

Handshake Phase

Step 1: Ephemeral Key Generation
1. A generates ECC key pair $d_A \in R[1, n-1]$ (d_A , $Q_A = d_A$
2. B generates ECC key pair $d_B \in R[1, n-1]$(d_B , $Q_B = d_B$.

Step 2: Alice → Bob (Authenticated Message)
1. A compute:
   $M_A = ID_A \,||\, ID_B \,||\, N \,||\, Q_A$
   A generates Falcon signature: $\sigma_A = Sing_{SK_A^{PQC}}(M_A)$
2. A sends (Q_A, σ_A)to B

Step 3: Bob Verification
1. B reconstructs:
   $M_A = ID_A \,||\, ID_B \,||\, N \,||\, Q_A$
   B verifies:
   $Verify_{PK_A^{PQC}}(M_A, \sigma_A)$
   If verification fails, abort protocol

Step 4: Bob → Alice (Authenticated Response)
1. B computes:
   $M_B = ID_B \,||\, ID_A \,||\, N \,||\, Q_B$
2. B generates Falcon signature: $\sigma_B \leftarrow Sing_{SK_B^{PQC}}(M_B)$
   B sends (Q_B, σ_B) to A

Step 5: Alice Verification
1. A reconstructs:
   $M_B = ID_B \,||\, ID_A \,||\, N \,||\, Q_B$
2. A verifies:
   $Verify_{PK_B^{PQC}}(M_B, \sigma_B)$
3. If verification fails, abort protocol

Key Agreement Phase

Step 6: ECDH Shared Secret Computation
1. A compute: $S \leftarrow d_A . Q_B$
2. B computes: $S \leftarrow d_B . Q_A$

$S_x \leftarrow X(S)$

$K\_ECC \leftarrow H(S_x)$

Key Derivation Phase

Step 7: Transcript Construction

$T = ID_A \,||\, ID_B \,||\, N \,||\, Q_A \,||\, Q_B \,||\, \sigma_A \,||\, \sigma_B$

Step 8: Session Key Derivation

$K_{session} \leftarrow KDF(K\_ECC \,||\, H(T))$

Output

Both parties output the shared session key ($K_{session}$)

Participants: Alice (A), Bob (B)
Long-term keys: Falcon-512 key pairs
Ephemeral keys: ECC (NIST P-256)
Algorithm diagram of the hybrid ECC–Falcon authenticated key-exchange protocol in figure 2. It uses ephemeral elliptic-curve Diffie–Hellman for forward secrecy and Falcon post-quantum signatures for authentication. To protect against both classical and quantum adversaries, the final session key is obtained by combining the ECDH shared secret with a hash of a session transcript that includes all the values sent in the session.

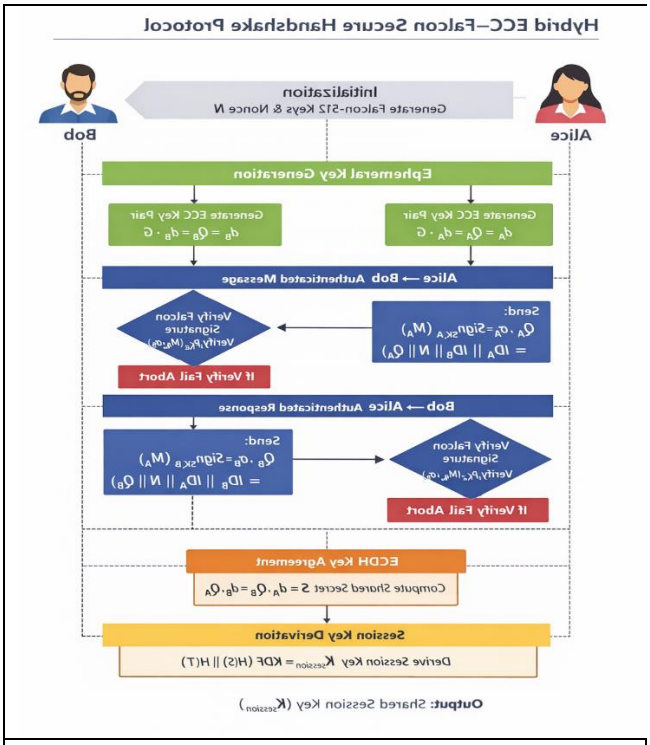

Figure 2. Hybrid ECC–Falcon Key Exchange Protocol

4.4 Correctness of the Hybrid ECC–Falcon Handshake Protocol

Given the algebraic properties of the scalar multiplication of elliptic curves and the functional correctness of the Falcon digital signature scheme, the proposed hybrid ECC–Falcon handshake protocol is correct. In the key agreement phase, Alice and Bob each generate their own ephemeral elliptic curve key pairs $(d_A, Q_A = d_A \cdot G)$and $(d_B, Q_B = d_B \cdot G)$ such that G is a generator of cyclic group over an elliptic curve. Because of the bilinear property of scalar multiplication on elliptic curves, both parties end up with the same shared secret point: $S = d_A \cdot Q_B = d_B \cdot Q_A = d_A d_B \cdot G$.Thus, Alice and Bob obtain the same X-coordinate X(S), and this value is then deterministically converted into a symmetric secret using a cryptographic hash function, so that the key derived from the ECDH exchange reads K_ECC=H(X(S)).

The Falcon post-quantum signature scheme guarantees the correctness of the authentication. The signatures are on the ephemeral public key generated by the party we are verifying identities for along with the other party's identity and the session nonce -- the verification guarantees that only a holder of the matching Falcon private key can generate a valid signature. Thus, any filing of the messages sent is modified, or impersonates an able is noticed, and therefore abortion of the protocol. Finally, both sides build the same transcript of the session and then compute the session key from the ECDH secret combined with the transcript hash using a key derivation function. On the other hand, the key derivation phase is fed with the same input in both cases therefore both session keys will be equal resulting in a correct and consistent key establishment.

4.5 Security Analysis

- The Hybrid ECC–Falcon handshake protocol is mathematically secure and practically secure. It combines ephemeral ECDH for forward secrecy with Falcon512 post-quantum signatures for authentication, achieving resistance against both classical and quantum adversaries under standard cryptographic assumptions.

4.5.1 Security Model

- In a Dolev–Yao communication control model, the adversary is fully controlling the communication channel and can:
- Interception, modification, deletion, replay, and injection of messages on public channel Be an intermediary to forge and relay messages or perform man-in-the-middle impersonation attacks. In some, additionally extract secrets stored in extracted devices, except protected

parts (like secrets in PUF or in server keys). However, your very own words that the adversary can "eavesdrop, modify, inject, replay, and delay messages" is therefore completely consistent with out-of-the-box DY assumptions [22].

• Computational / AKE security games. For reduction-based AKE models (Bellare–Rogaway, CK, eCK, multi-stage KE, Real-or-Random / IND-style games), this refines this by providing oracle access to a PPT adversary representing its capabilities. Execute / eavesdrop passive whomping of honest protocol runs. Send: layer 3 attack, replay166 Send: active interference, arbitrary message injection/modification, modeling MitM and impersonation. Reveal: Check forward secrecy and known-key security of learning session keys. Vulnerable: breakage of long-term keys or state (forward secrecy, KCI, insider attacks). Test/IND game: the enemy must distinguish a real session key or ciphertext from random capturing key indistinguishability [23].

4.5.2 Cryptographic Assumptions

➢ Assumption A1: ECDH Hardness

• Any elliptic-curve component will base its security on the on assumption that the of the Elliptic Curve Diffie–Hellman (ECDH) problem is hard:

•

it is hard to compute $d_A d_B G$ given $(G, d_A G, d_B G)$

➢ Assumption A2: Falcon Signature Security

• The Falcon signature scheme is assumed to be existentially unforgeable under chosen-message attacks (EUF-CMA). Its security is based on the hardness of lattice problems, including: NTRU-SIS, GPV trapdoor framework[24].

➢ Assumption A3: Hash Function and KDF

• We model the hash function (H (·)) and the KDF as random oracles [101], i.e., as ideal random functions to which all parties have access. They are presumed to provide preimage resistance, (second-)collision resistance, and (intrapartition) pseudorandom outputs, meaning that their outputs are indistinguishable from truly random strings of the same length[25].

4.5.3 Theorem 1: Mutual Authentication

• Claim:
• Given that the adversary cannot impersonate Alice nor Bob
• Proof Sketch:
• Falcon is used for digitally signing each authentication message:
• $\sigma \leftarrow \text{Falcon.Sign}(sk_F, M)$
• If an adversary outputs a valid signature without knowing the secret key, it breaks EUF-CMA security of Falcon, contradicting Assumption A2[26].
• Hence, this presents itself to be computationally infeasible to impersonate it.

4.5.4 Theorem 2: Session Key Secrecy

Claim:
The derived session key is indistinguishable from a random key.
The session key is computed as:

$$K_{session} = \text{KDF}(x(d_A Q_B) \parallel H(T))$$

Proof Sketch:
Without knowledge of the ephemeral private keys $d_A$or d_B, the adversary cannot compute the ECDH shared secret. Any successful key derivation would imply solving the ECDH problem, contradicting Assumption A1. The transcript hash binds all exchanged values, preventing partial manipulation[27].

4.5.5 Security Properties

➢ Mutual authentication: Both parties communicating cryptographically authenticate to each other with Falcon-512 digital signatures.
➢ Forward secrecy: Ensured through the use of ephemeral ECC key pairs, so past session keys are not compromised, even if long term keys are revealed.

- Man-in-the-middle resistance: Falcon signatures authenticate ephemeral public keys to prevent malicious key substitution.
- Replay attack resistance: session nonces are fresh and associate each handshake to a single execution instance.
- Quantum-resistant authentication: Falcon-512 provides security against quantum adversaries based on lattice hardness assumptions.

4.5.6 Hybrid ECC–Falcon Protocol Verification

The Hybrid ECC–Falcon protocol was formally verified using Tamarin Prover, ProVerif, and Verifpal. The verification results confirmed successful mutual authentication, secure session establishment, resistance to replay and impersonation attacks, and satisfaction of all symbolic security queries. Mutual authentication properties were verified through formal symbolic verification by ProVerif by the following correspondence queries:

$$event\ (Alice\ Finish(n)) \Rightarrow event\ (Bob\ Start(n))$$

And

$$event\ (Bob\ Finish(n)) \Rightarrow event\ (Alice\ Start(n))$$

The verification results show that neither communicating party can finish the protocol execution unless the corresponding peer legitimately started the matching session with the same nonce value.

Additionally, the Tamarin authentication lemmas and Verifpal symbolic analysis showed that replay attacks and man-in-the-middle attacks during protocol execution do not affect authentication consistency.

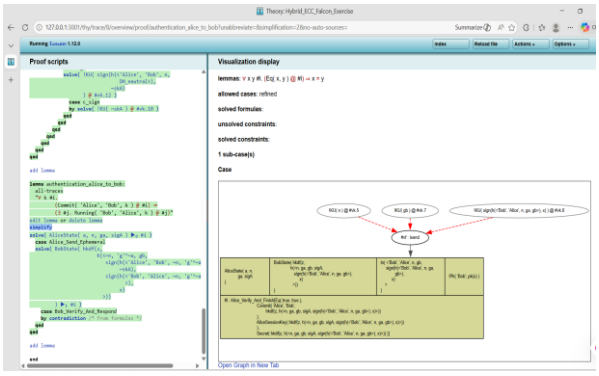

Figure 3. Tamarin Result for Hybrid ECC–Falcon Mutual Authentication

Figure 3: Tamarin Result for Hybrid ECC–Falcon Mutual Authentication. The Tamarin verification result confirms that the mutual authentication lemma of the Hybrid ECC–Falcon protocol was successfully satisfied. The analysis shows that both communicating parties complete the protocol only after successful verification of the Falcon signatures and session parameters, while no attack trace violating the authentication property was detected during symbolic verification.

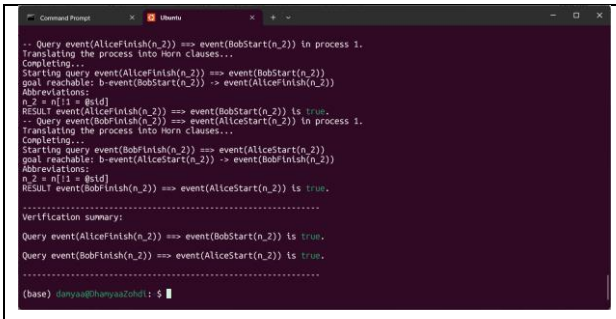

Figure 4. ProVerif Mutual Authentication Verification Result for Hybrid ECC–Falcon Protocol

Figure 4: ProVerif Mutual Authentication Verification Result for Hybrid ECC–Falcon Protocol. The ProVerif verification result confirms that the mutual authentication queries of the Hybrid ECC–Falcon protocol were successfully satisfied. The outputs event(Alice Finish(n_2)) ==> event(Bob Start(n_2)) is true, and event(Bob Finish(n_2)) ==> event(Alice Start (n_2)) is true, indicating that both communicating parties complete the protocol only after successful participation of the corresponding peer, while no executable attack trace violating the authentication property was detected.

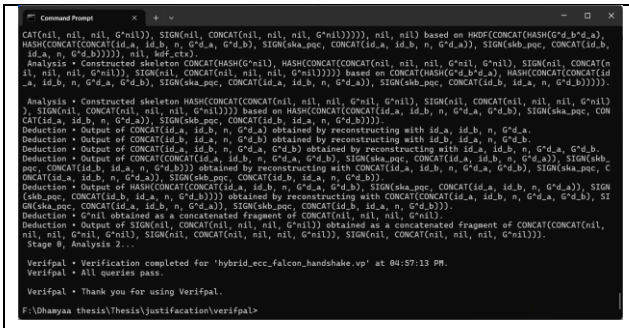

Figure 5. Verifpal Result for Hybrid ECC–Falcon Protocol Verification

Figure 5: Verifpal Result for Hybrid ECC–Falcon Protocol Verification. The Verifpal verification result confirms that all symbolic security queries for the Hybrid ECC–Falcon protocol were satisfied. The analysis indicates that no executable attack trace was detected, thereby supporting the authentication and session-key secrecy properties of the proposed hybrid protocol.

5. Results and Analysis

Statistical robustness ensured over 2000 independent runs of the Hybrid ECC–Falcon-512 secure handshake protocol. The average handshake latency for the protocol was 41.6 ms (stdev: 8.93 ms) and the minimum and maximum latencies observed were 29.0 ms and 87.5 ms, respectively. The tests were repeated multiple times, and a constant 24.03 handshakes/sec was observed. As far as the component-level analysis is concerned, we can observe that most of the primary computational cost is attributed to Falcon-512 signature generation (2.05 ms) and ECC-based ECDH computation (2.29 ms); whereas signature verification (0.11 ms) and HKDF-based key derivation (0.03 ms) incur very little overhead. Consequently, it shows that post-quantum operations are efficiently limited to authentication, whereas session key establishment uses fast elliptic-curve primitives. In terms of communication overhead, there's a 64-byte ECC public key and a 653-byte Falcon signature per authenticated message, so 717 bytes / message and about 1434 bytes total / handshake. This overhead is moderate when compared to PQC-only TLS approaches (that must use oversized certificates), while offering both post-quantum authentication and forward secrecy.

In conclusion the results prove that the balance between security and efficiency is ensured with the proposed hybrid protocol so that the protocol can be used in a post-quantum transition scenarios and in resource constrained environments as well. Table 1. Overall Handshake Performance of the Proposed Hybrid ECC–Falcon Protocol. Our findings indicate a total handshake latency of 41.61 ms over 2000 runs where standard deviation is 8.93 ms which shows the performance stability of the Hybrid ECC–Falcon protocol. Such a throughput of 24.03 handshakes/sec exhibits that the protocol can work in real-time for secure communications as shown in Table 1.

Table 1: Overall Handshake Performance

Metric	Value
Number of rounds	2000
Average handshake time	41.61 ms
Standard deviation	8.93 ms
Min / Max handshake time	29.03 / 87.49 ms
Throughput	24.03 handshakes/sec

From the component-level view, we observe that most of the raw computational costs are attributed to Falcon-512 signing and ECC-based ECDH computation, whereas the costs of signature verification and key derivation are negligible. This confirms the efficient confinement of post-quantum operations into authentication with marginal loss to total performance as shown in Table 2.

Table 2: Average Component-wise Computation Cost

Cryptographic Component	Average Cost
Falcon-512 signing	2.05 ms
Falcon-512 verification	0.11 ms
ECC ECDH computation	2.29 ms
HKDF derivation	0.03 ms

- In terms of communication costs, it's still a moderate 717 bytes per authenticated message, and a total handshake size of 1434 bytes. This overhead is lower than previously observed with PQC-only TLS solutions, while also providing post-quantum authentication and forward secrecy as shown in Table 3.

Table 3: Communication Overhead of the Proposed Protocol

Message Element	Size
ECC ephemeral public key	64 bytes
Falcon-512 signature	653 bytes
One message size	717 bytes
Total handshake size	1434 bytes

6.Comparison with Related Work

In this subsection, we comparatively evaluate the Hybrid ECC–Falcon key-exchange protocol against some representative classical, post-quantum and hybrid cryptographic mechanisms reported in the literature. Together with a thorough discussion on widely used evaluation metrics, such as computation efficiency, communication overhead, and security properties. For this reason, this article is meant to place the protocol in context with established literature, identifying its advantages and tradeoffs in relation to existing designs for hybrid and post-quantum secure key-exchange. Key generation costs are excluded, as they are not part of the handshake critical path. performance comparison of the proposed ECC-Falcon protocol with existing authentication and secure communication schemes as shown in Table 4.

Table 4: Performance Comparison of The Proposed ECC-Falcon Protocol with Existing Authentication and Secure Communication Schemes

Work	Cryptographic Approach	Authentication Method	Avg. Handshake / Crypto Cost	Communication Overhead	Evaluation Metrics Used
Hybrid PQC-TLS (2024) [28]	PQC-only (Lattice-based)	Dilithium signatures	PQC-only TLS improves handshake performance by ≈ 9%; Hybrid PQC-QKD TLS incurs ≈ 117% overhead during key establishment	High due to PQC certificates and additional key exchange operations	Handshake latency, bandwidth overhead, compatibility
Post-Quantum Hybrid KEMTLS[29]	Hybrid Classical KEM + PQC KEM	Hybrid KEMTLS	Moderate handshake overhead	High	Handshake time, application-data latency, hybrid penalty, memory usage
Falcon Lattice Signature (2020)[30]	PQC-only (NTRU lattice)	Falcon	Fast verification, moderate signing cost	Signature ≈ 666 bytes	Signature size, sign/verify time
Hybrid Encryption for Smart Healthcare (2024)[31]	ECC + symmetric + PQC primitives	ECC-256r1 + AES-128	Processing time ≈ 0.006 s; improved processing speed and energy efficiency	Moderate overheads suitable for IoT healthcare environments	Encryption time, throughput, energy
Lightweight Authenticated Encryption IoT (2020)[32]	ECC-based lightweight crypto	ECC authentication	Low computational cost and reduced handshake operations	≈ 184 bytes per handshake compared with ≈ 332 bytes for TLS	Computation cost, energy, latency
Proposed Hybrid ECC–Falcon Protocol	Hybrid ECC + PQC	Falcon-512 signatures	≈ 41.6 ms avg handshake (2000 runs)	1434 bytes per handshake	Latency, throughput, computational cost comm. overhead

Limitations

The proposed Hybrid ECC–Falcon protocol was evaluated primarily in terms of handshake latency, throughput, communication overhead, and security properties. Memory consumption and energy usage were not experimentally measured and therefore remain outside the scope of the current study. In addition, the

protocol relies on ECDH for session key establishment, which provides forward secrecy under classical security assumptions but is theoretically vulnerable to large-scale quantum attacks. Consequently, the protocol should be viewed as a practical transitional solution that combines post-quantum authentication with efficient classical key exchange during the migration toward fully post-quantum secure communication systems.

7. Conclosin

This paper presented an efficient secure handshake protocol that combines classical elliptic-curve cryptography with the post-quantum digital signatures of Falcon, called Hybrid ECC–Falcon. Combining ephemeral ECC-based ECDH for session key establishment with Falcon-512 lattice-based signatures for authentication, our protocol passes the comprehensive design mentioned above, all while preserving forward secrecy, mutual authentication, and quantum-resistance. Through extensive experimental evaluation of over 2000 independent runs, we show that the average handshake latency of our proposed protocol is only 41.6 ms, while maintaining stable throughput and moderate communication overhead. Component-wise analysis demonstrated that the post-quantum operations are efficiently limited to the authentication phase and that the session key establishment benefits from the rapid elliptic-curve primitives, making it suitable for in post-quantum transition environments .The novel hybrid approach overcomes the challenges of the result of big signatures of post-quantum algorithms and the lack of quantum resistance of classical schemes by achieving a pragmatic balance between security strength and performance efficiency when compared to state-of-the-art PQC-only and ECC-only solutions. The results reflect that our protocol is a good candidate for post-quantum transition period, especially for IoT and other lightweight secure communication scenarios.

Upcoming efforts will target formal security proofs in accepted authenticated key exchange models, hardware-oriented acceleration of post-quantum components, and embedding into protocols like TLS 1.3 hybrid key exchange to increase real-world relevance.

References

[1] Baseri Y, Chouhan V, Ghorbani A, Chow A. Evaluation framework for quantum security risk assessment: A comprehensive strategy for quantum-safe transition. Comput Secur 2025;150. https://doi.org/10.1016/j.cose.2024.104272.

[2] Kinyua CG. The Impact of Quantum Computing on Cryptographic Systems: Urgency of Quantum-Resistant Algorithms and Practical Applications in Cryptography. European Journal of Information Technologies and Computer Science 2025;5. https://doi.org/10.24018/ejcompute.2025.5.1.146.

[3] Bernstein DJ, Niederhagen R, Hülsing A, Rijneveld J, Kölbl S, Schwabe P. The SpHiNCS+ signature framework. Proceedings of the ACM Conference on Computer and Communications Security, Association for Computing Machinery; 2019, p. 2129–46. https://doi.org/10.1145/3319535.3363229.

[4] Rubio Garcia C, Cano Aguilera A, Stan C, Jose Vegas Olmos J, Rommel S, Tafur Monroy I. Enhanced Network Security Protocols for the Quantum Era: Combining Classical and Post-Quantum Cryptography, and Quantum Key Distribution. IEEE Journal on Selected Areas in Communications 2025;43:2765–81. https://doi.org/10.1109/JSAC.2025.3568011.

[5] Gupta A, Adhikari RS, Rani A, Ai X, Malaney R. Combined Quantum and Post-Quantum Security Performance Under Finite Keys 2025.

[6] Fernandez-Carames TM. From Pre-Quantum to Post-Quantum IoT Security: A Survey on Quantum-Resistant Cryptosystems for the Internet of Things. IEEE Internet Things J 2020;7:6457–80. https://doi.org/10.1109/JIOT.2019.2958788.

[7] Giron AA. UNIVERSIDADE FEDERAL DE SANTA CATARINA CENTRO TECNOLÓGICO PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO Hybrid Post-Quantum Cryptography in Network Protocols. 2023.

[8] Rubio García C, Rommel S, Takarabt S, Vegas Olmos JJ, Guilley S, Nguyen P, Tafur Monroy I. Quantum-resistant Transport Layer Security. Comput Commun 2024;213:345–58. https://doi.org/10.1016/j.comcom.2023.11.010.

[9] Cherkaoui Dekkaki K, Tasic I, Cano MD. Exploring Post-Quantum Cryptography: Review and Directions for the Transition Process.

Technologies (Basel) 2024;12. https://doi.org/10.3390/technologies12120241.

[10] Egbuagha O, Ikwunna E. Post-Quantum Cryptography in Practice: A Literature Review of Protocol-Level Transitions and Readiness. n.d.

[11] Wang Y, Shahril Ismail E. A Review on the Advances, Applications, and Future Prospects of Post-Quantum Cryptography in Blockchain and IoT. IEEE Access 2025;13:112962–77. https://doi.org/10.1109/ACCESS.2025.3584473.

[12] Aranha DF, El Housni Y, Guillevic A. A survey of elliptic curves for proof systems. Des Codes Cryptogr 2023;91:3333–78. https://doi.org/10.1007/s10623-022-01135-y.

[13] Awaludin AM, Larasati HT, Kim H. High-speed and unified ecc processor for generic weierstrass curves over gf(P) on fpga. Sensors 2021;21:1–20. https://doi.org/10.3390/s21041451.

[14] Di Matteo S, Baldanzi L, Crocetti L, Nannipieri P, Fanucci L, Saponara S. Secure elliptic curve crypto-processor for real-time iot applications. Energies (Basel) 2021;14. https://doi.org/10.3390/en14154676.

[15] AbdElHaleem SH, Abd-El-Hafiz SK, Radwan AG. A generalized framework for elliptic curves based PRNG and its utilization in image encryption. Sci Rep 2022;12. https://doi.org/10.1038/s41598-022-17045-x.

[16] Parida P, Pradhan C, Gao XZ, Roy DS, Barik RK. Image Encryption and Authentication with Elliptic Curve Cryptography and Multidimensional Chaotic Maps. IEEE Access 2021;9:76191–204. https://doi.org/10.1109/ACCESS.2021.3072075.

[17] Kumar S, Sharma D. A chaotic based image encryption scheme using elliptic curve cryptography and genetic algorithm. Artif Intell Rev 2024;57. https://doi.org/10.1007/s10462-024-10719-0.

[18] Qiu J, Aysu A. SHIFT SNARE: Uncovering Secret Keys in FALCON via Single-Trace Analysis 2025.

[19] Nguyen TT, Nguyen DD, Dao TT, Luc NQ. Implementation Efficiency of Falcon Digital Signature Scheme on Arty-7 XC7A35T Board. Electronics (Switzerland) 2025;14. https://doi.org/10.3390/electronics14224504.

[20] Fouque P-A, Hoffstein J, Kirchner P, Lyubashevsky V, Pornin T, Prest T, Ricosset T, Seiler G, Whyte W, Zhang Z. Falcon: Fast-Fourier Lattice-based Compact Signatures over NTRU Specifications v1.0. n.d.

[21] Dey K, Goyal M, Singh B, Gangopadhyay AK. An Undeniable Signature Scheme Utilizing Module Lattices 2024. https://doi.org/10.48550.

[22] Su X, Xu Y. An Efficient Cluster-Based Mutual Authentication and Key Update Protocol for Secure Internet of Vehicles in 5G Sensor Networks. Sensors 2025;25. https://doi.org/10.3390/s25010212.

[23] Dowling B, Fischlin M, Günther F, Stebila D. A Cryptographic Analysis of the TLS 1.3 Handshake Protocol. Journal of Cryptology 2021;34. https://doi.org/10.1007/s00145-021-09384-1.

[24] Liu F, Zheng Z, Gong Z, Tian K, Zhang Y, Hu Z, Li J, Xu Q. A survey on lattice-based digital signature. Cybersecurity 2024;7. https://doi.org/10.1186/s42400-023-00198-1.

[25] Brzuska C, Couteau G, Egger C, Karanko P, Meyer P. Instantiating the Hash-then-evaluate paradigm: Strengthening PRFs, PCFs, and OPRFs. Cryptography and Communications 2025;17:1325–66. https://doi.org/10.1007/s12095-025-00825-3.

[26] Chia J, Chin JJ, Yip SC. Digital signature schemes with strong existential unforgeability. F1000Res 2021;10. https://doi.org/10.12688/f1000research.72910.1.

[27] Chuah CW, Harun NZ, Hamid IRA. Key derivation function: key-hash based computational extractor and stream based pseudorandom expander. PeerJ Comput Sci 2024;10. https://doi.org/10.7717/PEERJ-CS.2249.

[28] Rubio García C, Rommel S, Takarabt S, Vegas Olmos JJ, Guilley S, Nguyen P, Tafur Monroy I. Quantum-resistant Transport Layer Security. Comput Commun 2024;213:345–58. https://doi.org/10.1016/j.comcom.2023.11.010.

[29] Giron AA, Adami Do Nascimento JP, Custódio R, Perin LP. Post-Quantum Hybrid KEMTLS Performance in Simulated and Real Network Environments. n.d.

[30] Fouque P-A, Hoffstein J, Kirchner P, Lyubashevsky V, Pornin T, Prest T, Ricosset T, Seiler G, Whyte W, Zhang Z. Falcon: Fast-Fourier Lattice-based Compact Signatures over NTRU. n.d.

[31] Popoola O, Rodrigues MA, Marchang J, Shenfield A, Ikpehai A, Popoola J. An optimized hybrid encryption framework for smart home healthcare: Ensuring data confidentiality and security. Internet of Things (Netherlands) 2024;27. https://doi.org/10.1016/j.iot.2024.101314.

[32] Diro A, Reda H, Chilamkurti N, Mahmood A, Zaman N, Nam Y. Lightweight Authenticated-Encryption Scheme for Internet of Things Based on Publish-Subscribe Communication. IEEE Access 2020;8:60539–51. https://doi.org/10.1109/ACCESS.2020.2983117.