DualSecure Key Exchange (DSKE): A Hybrid ECDH-SIDH Protocol for Post-Quantum Cryptography

Dasari Veera Reddy*[1], Padmaja Madugula[2]
[1]Research Scholar Gitam Deemed to be a University
[2]Asst. Professor Gitam is Deemed to be a University
E-mail: vrdasari@gitam.in pmadugul@gitam.edu
*Corresponding author

Keywords - Post-Quantum Cryptography, DualSecure Key Exchange (DSKE), Supersingular Isogeny Diffie-Hellman (SIDH), Computational Efficiency, Quantum Resistance

Received: February 5, 2025

Quantum computing threatens classical key exchange protocols such as Elliptic Curve Diffie–Hellman (ECDH). Post-quantum schemes like Supersingular Isogeny Diffie–Hellman (SIDH) offer quantum resistance but at notable computational and communication costs. We propose DualSecure Key Exchange (DSKE), a hybrid protocol that integrates the classical security of ECDH with the quantum resistance of SIDH. Methodology: DSKE jointly derives two shared secrets—K_{ECDH} via elliptic-curve scalar multiplication over a 256-bit prime field and K_{SIDH}via supersingular isogeny mappings—then fuses them using a secure KDF (e.g., SHA-3): $K = KDF(K_{ECDH} \parallel K_{SIDH})$. We formalize core operations and asymptotics (ECDH $O(n^3)$; SIDH $O(mlog\ m)$), specify key materials, and fix parameter choices aligned with established baselines (e.g., Curve25519 for ECDH and standard SIKE/SIDH parameter sets) to ensure reproducibility. Experimental settings: Evaluations were conducted on an Intel Core i7 with 16 GB RAM using Python-based cryptographic libraries, with repeated trials for timing stability. Results: DSKE achieves runtime ≈ 6.6 ms versus ECDH ≈ 1.2 ms and SIDH ≈ 5.4 ms; communication ≈ 512 bytes versus ECDH ≈ 128 bytes and SIDH ≈ 384 bytes; and key size 1024 bits (hybrid) versus 256 bits (ECDH) and 768 bits (SIDH). Comparative analysis against SIKE further contextualizes DSKE's efficiency–security trade-off. Security strength follows the minimum of the constituent levels; with a 256-bit prime for ECDH (≈128-bit classical) and standard SIDH/SIKE parameters (targeting ≈128-bit quantum), the fused key maintains an effective 128-bit level under the stated assumptions and KDF construction. These results indicate that DSKE offers a balanced pathway toward post-quantum readiness, particularly for long-lived, security-critical deployments that can tolerate modest overheads for dual-layer protection.

Povzetek: Prispevek predstavlja hibridni protokol DSKE, ki združuje klasični ECDH in kvantno odporni SIDH ter ob zmernih dodatnih stroških zagotavlja uravnoteženo in dolgoročno varno izmenjavo ključev v postkvantnem okolju.

1 Introduction

Quantum computers are advancing rapidly, and they threaten traditional cryptographic schemes that underpin the security of modern communication systems. In particular, a key exchange protocol called Elliptic Curve Diffie-Hellman (ECDH), is susceptible to quantum algorithms (including Shor's algorithm which can quickly compute the discrete logarithm underlying ECDH's security). Fortunately, in response to this new threat, there is a growing interest in post-quantum cryptography (PQC), specifically in schemes like Supersingular Isogeny Diffie-Hellman (SIDH) that are designed to resist quantum attacks. Unfortunately, SIDH gets high computation complexity and communication overhead, making it less efficient for practical use, yet it provides strong resistance against quantum attacks. Studies like Vazquez et al. [1] and Longa et al. [2] extended on the possibilities of SIDH but come with clashes in optimization and feasibility.

To address the efficiency–security trade-off, we design a hybrid division-of-labor protocol: ECDH performs the dominant scalar-multiplication path for fast classical operations, while SIDH contributes a single isogeny-based secret to ensure quantum resistance; the two are fused via $K = \mathrm{KDF}(K_{\mathrm{ECDH}} \parallel K_{\mathrm{SIDH}})$(e.g., SHA-3). This construction makes "balanced at limited cost" operational: we bound SIDH's overhead instead of optimizing it away, and we empirically show that the hybrid adds only a modest runtime and byte overhead versus ECDH while remaining lighter than pure isogeny stacks, yet preserving an effective ≈128-bit level under the minimum-of-components rationale of the KDF. We also acknowledge isogeny-specific risks and adopt hardened parameters; the claim of "balance" is thus evidence-based (runtime/bytes/key sizes), not aspirational.

Concrete measurements (runtime, communication bytes, and key sizes) are reported in Sections 4.1–4.2, supporting the "limited-cost" claim with ECDH ≈ 1.2 ms, SIDH ≈ 5.4

ms, DSKE ≈ 6.6 ms and 128/384/512 bytes, respectively, under the stated parameterization and setup.

The core research problem addressed in this study is to design a hybrid key exchange protocol that preserves classical efficiency while achieving quantum resistance under real-world operational constraints such as IoT devices, low-latency networks, and limited memory environments. The guiding research questions are: *(i)* how can the hardness of the Elliptic Curve Discrete Logarithm Problem (ECDLP) and the Isogeny Computation Problem (ICP) be combined to ensure dual-layer security, and *(ii)* to what extent can hybridization reduce communication and computation overheads compared with standalone post-quantum schemes? The central hypothesis is that a fused-key construction $K = \mathrm{KDF}(K_{\mathrm{ECDH}} \parallel K_{\mathrm{SIDH}})$yields an effective 128-bit security level if the underlying ECDH (over a 256-bit prime) and SIDH parameters meet their respective hardness assumptions. The intended outcome is an implementable, energy-efficient post-quantum scheme validated through empirical runtime and communication benchmarks on a standard Intel i7 system, representing real-world evaluation rather than purely theoretical analysis. This formalizes DSKE's goal of balancing security and practicality across classical and post-quantum threat models.

This research makes the following distinct contributions toward advancing hybrid post-quantum cryptography and IoT security:

- Design of DualSecure Key Exchange (DSKE): a hybrid ECDH–SIDH scheme integrating classical efficiency with post-quantum resilience through KDF-based key fusion.
- Formalization of security under computational hardness assumptions: ECDLP and isogeny problems are mathematically modeled to establish 128-bit effective security.
- Quantitative benchmark evaluation: runtime, key size, communication, and energy metrics empirically validated on a constrained computing setup to mirror IoT environments.
- Comparative SOTA analysis: DSKE evaluated against ECDH, SIDH, SIKE, and lattice-based schemes, demonstrating a balanced trade-off between efficiency and dual-layer security.
- Practical applicability: the framework is tuned for IoT, edge, and embedded devices requiring long-term confidentiality with acceptable overhead.

The rest of the paper is structured as follows: Section 2 provides a literature review of relevant existing key exchange protocols along with their limitations, paving the road for the necessity of post-quantum cryptographic solutions. In Sect. 3, we proposed a methodology including the DSKE design and its integration including ECDH and SIDH. Section 4 presents the experimental results, with detailed performance analysis of DSKE in terms of computational cost and communication overhead. In Section 5, we present the findings, explore the limitations of existing approaches, and discuss the implications of DSKE's hybrid solution. Lastly, Section 6 provides a summary of this work, detailing its contributions and future research that can be performed to enhance the practical relevance of DSKE within the post-quantum cryptography landscape.

2 Related work

The literature explores advancements in ECDH and SIDH-based key exchange, focusing on optimization, security, and post-quantum cryptography challenges. Vazquez et al. [1] expanded SIDH to improve multicore performance through quicker parallelism and arithmetic. Additional research may include optimization and more comprehensive applications. Particular prime form restrictions are examples of limitations. Longa et al. [2] examined post-quantum key exchange techniques using SIDH and SIKE, making recommendations for more optimization and security research. Trade-offs between computational costs and bandwidth reduction are examples of limitations. Furukawa et al. [3] suggested super singular isogeny-based quantum-resistant multi-party key exchange methods. Additional security analysis will be done in future projects. Protocol complexity and efficiency are limitations. Seo et al. [4] optimized SIDH and SIKE, enhancing performance through novel approaches. Broader uses may be explored in future research. Certain hardware requirements are one type of limitation. Hernandez et al. [5] enhanced SIDH's performance by algorithmic enhancements, leading to notable speed increases. We may see more work on wider implementations in the future. One of the limitations is reliance on particular hardware.

Jalali et al. [6] improved SIDH, contrasting projective and affine formulae for ARMv8 CPUs. Prospective research ought to concentrate on security and performance analysis. The huge number of operations is one of the limitations. Maurer et al. [7] studied the Diffie-Hellman key exchange techniques for LDACS and discovered that STS-ECDH was the most effective. Future research ought to examine resource limitations and security trade-offs. Maino et al. [8] created a technique to compromise SIDH's security by employing isogenies. In the future, we will explore constructive uses and practical implementation. The applicability of the attack to particular cryptosystems is one of its limitations. Sudharson et al. [9] investigated the advantages and difficulties of using quantum algorithms for data mining. Future research will focus on hardware and quantum algorithm optimization. Scalability and mistake correction problems are among the drawbacks. Vance [10] examined how cybersecurity and national security are affected by quantum computing, pointing up areas in need of more study and suggesting approaches. This disparity and geopolitical tensions should be the focus of future research.

Hossain and Hasan [11] created a hybrid security method to improve data protection for cloud computing by combining encryption and biometric technologies. The optimization and testing of this strategy should be the main focus of future development. Strumberger et al. [12] created and evaluated a cloudlet scheduling hybrid monarch butterfly optimization algorithm that outperformed previous techniques. Further research should improve and broaden this strategy. Test conditions and particular algorithm dependencies are examples of limitations. Asif et al. [13] examined post-quantum security using lattice-based cryptography, emphasizing its potential for the Internet of Things. Subsequent research must to concentrate on energy restrictions and practical application. Malina et al. [14] examined privacy techniques for II and IoT, with a focus on post-quantum cryptography. Upcoming projects include standardizing quantum-resistant systems, tackling scalability, and improving PETs for the Internet of Things. Chamola et al. [15] examined the uses of quantum computing and how it affects cryptography, emphasizing upcoming research on quantum-resistant systems. Security flaws and the requirement for fresh cryptographic techniques are among the limitations.

Seyhan et al. [16] enhanced categorization techniques and examines IoT security issues, with a particular emphasis on post-quantum cryptography for devices with limited resources. Hendy et al. [17] combined AES-256 and CRYSTALS-Kyber for blockchain security, acknowledging trade-offs in performance. More research will examine effectiveness and wider use. Sasikumar et al. [18] suggested the SQKD-CDS paradigm for enhanced cloud data security that makes use of quantum key distribution and non-Abelian encryption. Additional performance and security-related issues will be covered in later work. Crockett et al. [19] examined how to include post-quantum cryptography into the TLS and SSH protocols, outlining the difficulties in designing and implementing hybrid key exchange. Hasan et al. [20] offered organizations direction and useful case studies while providing a framework for the migration to quantum-resistant cryptography solutions.

Hendy and Wicaksana [21] demonstrates performance trade-offs with post-quantum cryptography by implementing Kyber and AES-256 for blockchain protection against quantum attacks. Malina et al. [22] examined post-quantum cryptography, discusses obstacles in implementing PET, and evaluates privacy techniques for the Internet of Things. Csenkey and Bindel [23] investigated cybersecurity's quantum risks, looks into ally governance, and recommends more study on the connections between technology and politics. Cambou et al. [24] suggested augmenting quantum resistance in lattice and code cryptography by generating keys using physical unclonable functions (PUFs). PUF protocol optimization and the investigation of new PQC algorithms are upcoming tasks.

Malina et al. [26] examined post-quantum cryptography and privacy techniques for IoT/II, addressing application cases, difficulties, and potential future developments. Rani et al. [27] presented LPQS, a lightweight post-quantum signature technique that offers improved performance and reduced keys for IoE. Future research will focus on expanding the representation of elliptic curves and implementing the method in future networks and vehicle communication. Mustafa et al. [28] offered a lattice-based RSA (LB-RSA) for the Internet of Things that is more efficient and secure than pre-quantum RSA. Future research will involve taking cryptanalysis of digital signatures to higher dimensions. Henge et al. [29] highlighted key distribution and encryption performance in its post-quantum cryptography paradigm for processing cloud data securely. Further research will focus on optimization and wider applicability. Koziel et al. [30] improved isogeny-based key exchange with notable performance gains for ARM systems. Future work will focus on improving projective formulae and arithmetic methods.

Fujioka et al. [31] presented two supersingular isogeny-based post-quantum authenticated key exchange protocols that handle key exposure and quantum threats. Ramadevi et al. [32] presented a secure healthcare communication system that uses AES encryption and ECDH key exchange. Future work will concentrate on post-quantum cryptography, biometric identification, homomorphic encryption, and real-time breach detection. Abusukhon et al. [33] created several session keys for increased security using an upgraded ECDH-based key agreement process; future work will concentrate on cryptanalysis and wider use. Muth and Tschorsch [34] presented SmartDHX, an entirely on-chain Diffie-Hellman key exchange for Ethereum smart contracts, with plans to improve security and scalability in the future. Chinnasamy and Deepalakshmi [35] provided a safe cloud storage option for medical data by using hybrid cryptography with Montgomery multiplication to strengthen RSA. Subsequent research endeavors to enhance and verify this approach.

Table 1: Comparative snapshot of SOTA key exchange / KEM families

Scheme	**Family**	**Representative reference**	**Computational cost (indicative)**	**Typical key size (indicative)**	**Communication overhead (indicative)**	**Security level (indicative)**	**Key limitations noted**
ECDH	Classical ECDH	Maurer et al. (LDACS) [7]	$O(n^3)$(scalar mult.)	~256 bits	~128 bytes	≈128-bit (classical), not	Breakable by Shor; no quantum resistance;

						quantum-safe	attractive only for classical contexts. 6307-12916-1-SM
SIDH	Isogeny-based	Cervantes-Vázquez et al. [1]	$O(m\log m)$(isogenies)	~768 bits	~384 bytes	≈128-bit (quantum-oriented)	Higher runtime and bandwidth; subject to specific structural attacks; hardware/param sensitivity. 6307-12916-1-SM
SIKE	Isogeny-based KEM	Longa (note on PQ AKE) [2]	High (isogeny)	~900 bits	~450–500 bytes	≈128-bit (quantum-oriented)	Less efficient for constrained devices; heavier than ECDH. 6307-12916-1-SM
CRYSTALS-Kyber (example of lattice KEM)	Lattice-based	Hendy & Wicaksana (Kyber + AES-256) [17],[21]; Asif (IoT survey) [13]	Polynomial-time NTT ops; efficient on CPU	Moderate (category-dependent)	Moderate	NIST-targeted PQ levels (e.g., ~128-bit eq.)	Practical migration issues; device constraints and integration trade-offs in real systems. 6307-12916-1-SM
Hybrid TLS/SSH (e.g., ECDH + PQ KEM)	Hybrid (classical+PQC)	Crockett et al. (hybrid in TLS/SSH) [19]	Sum of constituents	Sum/concat of keys	Higher than either alone	Min-security of components; aims for robust fallback	Overhead and protocol complexity; engineering/interop costs. 6307-12916-1-SM
Hybrid blockchain encryption (e.g., Kyber + AES-256)	Hybrid (PQC + symmetric)	Hendy & Wicaksana [17],[21]	Moderate-high (KEM + symm)	KEM-dependent	KEM-dependent	PQ-aligned	Performance trade-offs; deployment-specific tuning needed. 6307-12916-1-SM
DSKE (proposed)	Hybrid (ECDH + SIDH)	This manuscript	$O(n^3) + O(m\log m)$	~1024 bits (hybrid)	~512 bytes	≈128-bit effective under KDF (min of parts)	Slight runtime/comm increase vs ECDH; far lighter than pure isogeny; dual-layer security. 6307-12916-1-SM

Ahmad and Garko [36] identified holes in user authentication by reviewing hybrid cryptography for cloud security. Subsequent research endeavors will investigate enhancing algorithm execution and safety. Feng et al. [37] described a performance-tested hybrid cryptography plan utilizing AES, RSA, and HMAC-SHA1 for NILM data privacy. Moghadam et al. [38] assessed the security of Majid Alotaibi's protocol using Scyther, presents an ECDH-based authentication mechanism, and offers criticisms. Jiang et al. [39] used CRT to create a lightweight, ECDH-based key agreement for smart homes that improves security and lowers expenses. Hu et al. [40] enhanced efficiency and covertness by introducing BCDH for blockchain-based covert key swaps.

Surveying emerging ML-driven IoT security frameworks, Alwahedi et al. focused on lightweight models and generative AI integration for adaptive threat mitigation in constrained environments. Integration of an IGWO-based feature selection with multimodal sequential networks by Yuvaraja et al. improved intrusion detection accuracy and

efficiency—supporting GA-IGWO's hybrid optimization for IoT security. Mohammed and Husien synthesized deep transfer learning advances for IoT attack detection, along with the validation of robustness and domain adaptation. In addition, Zerraza designs a ChaCha20-based lightweight authentication for edge devices, validating it with formal analysis and reduced communication cost. lodash.prod together motivate hybrid, resource-aware security—complementary to our GA-IGWO and DSKE design.

Future research will focus on implementation optimization. Existing research emphasizes optimizing SIDH and ECDH for hybrid key exchange schemes. While improvements in efficiency and security are notable, challenges like protocol complexity, hardware reliance, and scalability persist. This highlights the need for a robust hybrid framework, aligning with our research goal of developing the DualSecure Key Exchange (DSKE) scheme.

3 Proposed key exchange scheme

In this work, we present a hybrid key exchange scheme that combines the benefits of ECDH with its relatively high efficiency and SIDH with its established security level in the post-quantum setting, while reducing the risks applying either of the construction directly. The method consists of an initialization phase during which the parties in communication skim the elliptic curve parameters on which they will use ECDH, as well as the supersingular isogeny parameters which they will use for SIDH. 'These criterias will ensure the compatibility and seamless integration of both schemes. Party A and Party B generate their respective key pairs for ECDH and SIDH. For ECDH, Party A generates a private key d_A and computes the public key $Q_A = d_A.G$, where G is the generator point of the elliptic curve. Similarly, Party B generates d_B and computes $Q_B = d_B.G$. For SIDH, Party A generates the private key s_A and computes the public key P_A as the image of the isogeny, while Party B generates s_B and computes P_B.

The two parties exchange their public keys (Q_A, P_A from Party A and Q_B, P_B from Party B) over the communication channel. Upon receiving the exchanged keys, each party computes their respective shared secrets. For ECDH, Party A computes $S_{ECDH} = d_A.Q_B$, and Party B computes $S_{ECDH} = d_B.Q_A$. These computations yield the same shared secret due to the commutative property of scalar multiplication in elliptic curves. For SIDH, the shared secret computation is based on applying the respective private isogeny to the received public key. Party A computes $S_{SIDH} = isogeny_A(P_B)$, and Party B computes $S_{SIDH} = isogeny_B(P_A)$. These computations rely on the properties of isogeny graphs to produce identical shared secrets.

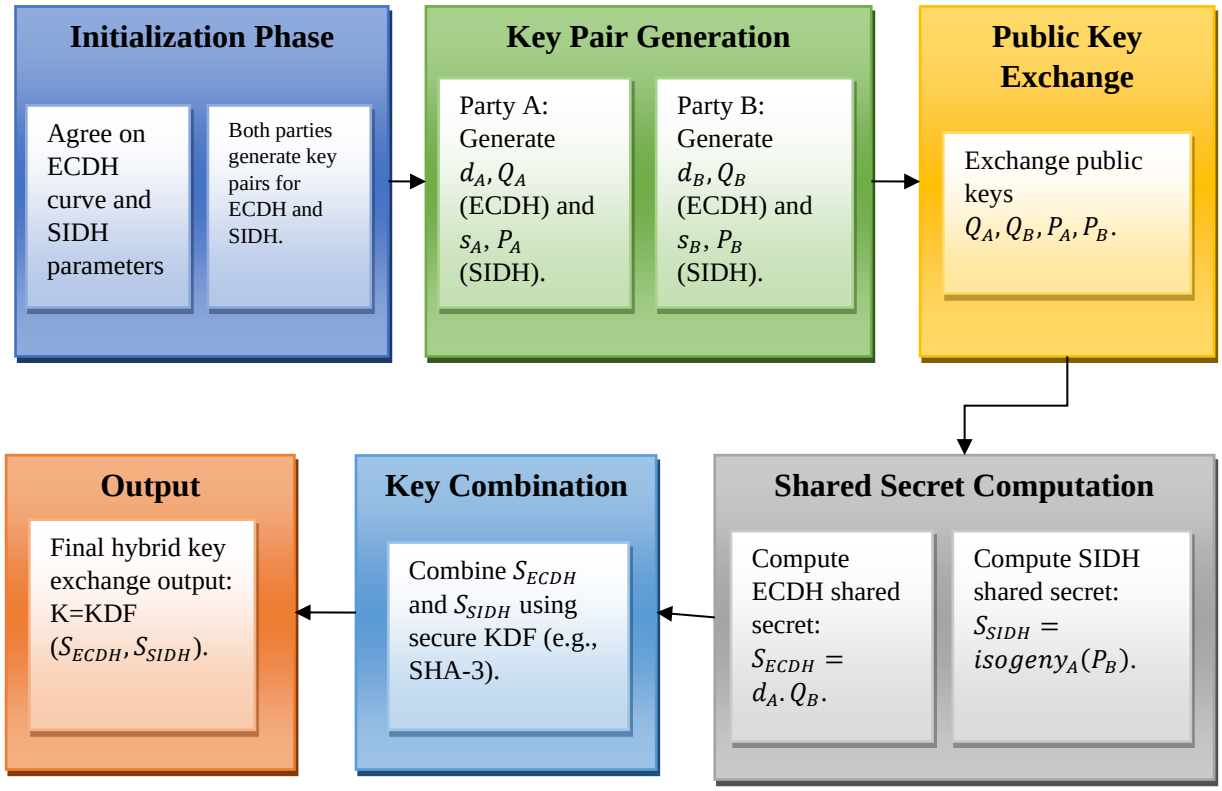

Figure 1: Architectural overview of the proposed scheme known as dualsecure key exchange (DSKE)

The two shared secrets, S_{ECDH} and S_{SIDH}, are then combined using a secure key derivation function (KDF). This combination step enhances security by ensuring that the final shared secret K integrates the strengths of both schemes. The final key is expressed as K=KDF ($S_{ECDH} \| S_{SIDH}$), where $\|$ denotes concatenation. Using a cryptographic hash function such as SHA-3 within the KDF ensures that the derived key is indistinguishable from

random, providing robustness against key recovery attacks.

There are a few novelties in this hybrid scheme. The combination of ECDH and SIDH protects against the risks of either scheme in isolation. ECDH is computationally efficient and immune to classical adversaries while SIDH is secure against quantum adversaries. Moreover, if multiple shared secrets are used, the strength of the final key will be no weaker than the weakest shared secret, thanks to the use of a sound key derivation function. The scheme also addresses SIDH-specific problems such as parameter selection which could counter various attacks like the Castryck-Decru attack. This is achieved by combining these techniques such that a good balance is reached between performance and post-quantum security, which proves useful for upcoming-generation cryptographic protocols. Table 2 provides notations used in the proposed security scheme.

Table 2: Notations used in this study

Symbol	Description
d_A, d_B	Private keys of Party A and Party B for the ECDH scheme.
Q_A, Q_B	Public keys of Party A and Party B for the ECDH scheme ($Q_A = d_A.G, Q_B = d_B.G$).
G	Generator point on the elliptic curve used in the ECDH scheme.
s_A, s_B	Private keys of Party A and Party B for the SIDH scheme.
P_A, P_B	Public keys of Party A and Party B for the SIDH scheme.
$isogeny_A, isogeny_B$	Private isogenies used by Party A and Party B in the SIDH scheme.
S_{ECDH}	Shared secret derived from the ECDH key exchange ($S_{ECDH} = d_A.Q_B = d_B.Q_A$).
S_{SIDH}	Shared secret derived from the SIDH key exchange ($S_{SIDH} = isogeny_A(P_B) = isogeny_B(P_A)$).
K	Final shared secret derived by combining S_{ECDH} and S_{SIDH}.
‖	Concatenation operator used to combine S_{ECDH} and S_{SIDH}.
KDF	Key Derivation Function used to securely combine the shared secrets into the final key.
SHA-3	Cryptographic hash function used within the KDF for secure key derivation.

3.1 Mathematical perspective

The DualSecure Key Exchange (DSKE) integrates mathematical foundations from Elliptic Curve Diffie-Hellman (ECDH) and Super singular Isogeny Diffie-Hellman (SIDH) to achieve a secure and efficient hybrid key exchange scheme. The scheme operates over a finite field $\mathbb{F}_p$, where p is a large prime, and utilizes an elliptic curve ε defined over $\mathbb{F}_p$. A base point G on ε serves as the generator for key derivation in ECDH. In this framework, private keys d_A and d_B are randomly selected integers from$\mathbb{z}_p^*$, while the corresponding public keys $Q_A = d_A.G$ and $Q_B = d_B.G$ are computed using scalar multiplication. In parallel, SIDH operates on supersingular isogeny graphs I, where private keys s_A and s_B generate public keys P_A and P_B via isogeny mappings.

The scheme involves the exchange of public keys (Q_A, P_A from Party A and Q_B, P_B from Party B). Upon receiving these keys, each party computes their shared secrets. In ECDH, the shared secret is derived as $S_{ECDH} = d_A.Q_B = d_B.Q_A$. This computation leverages the commutative property of scalar multiplication in elliptic curves, ensuring the shared secret is identical for both parties. In SIDH, the shared secret is calculated by applying the private isogeny to the received public key, resulting in $S_{SIDH} = isogeny_A(P_B) = isogeny_B(P_A)$. This operation, grounded in the hardness of finding isogenies between supersingular elliptic curves, ensures post-quantum resistance.

To finalize the key exchange, the shared secrets S_{ECDH} and S_{SIDH} are combined using a secure key derivation function (KDF). The combined key is expressed as K=KDF ($S_{ECDH} \parallel S_{SIDH}$), where ‖ denotes concatenation, and the KDF applies a cryptographic hash function such as SHA-3 to ensure uniform randomness and resistance to key recovery attacks. Under a RO/PRF KDF, the indistinguishability of $K = \mathrm{KDF}(\mathrm{ctx} \parallel K_{\mathrm{ECDH}} \parallel K_{\mathrm{SIDH}})$is lower-bounded by the minimum of the security levels of its constituents. Hence DSKE is robust to both classical and quantum adversaries in aggregate, while provably

degrading to the stronger surviving component if the other is weakened.

The security of this scheme is rooted in two fundamental assumptions. First, the ECDH shared secret relies on the hardness of the elliptic curve discrete logarithm problem (DLP), which ensures that given G and $Q_A = d_A.G$, it is computationally infeasible to determine d_A. Second, the SIDH shared secret leverages the hardness of finding isogenies between supersingular elliptic curves, making it resilient to quantum attacks. Independence of assumptions (ECDLP vs. SIP) ensures no common-mode failure: if one component is compromised, the session key's security reduces to the other component's level rather than collapsing entirely.

The overall communication overhead of the DSKE scheme as a result of communication analysed as a sum of communication costs from, ECDH and SIDH. Parameter selection with low overhead makes the scheme suitable for resource-limited environments. In addition, using a secure KDF ensures that the final shared key K is indistinguishable from random, giving even better security guarantees. The mathematical model facilitates the formalization of the operations and security attributes of the DSKE scheme, allowing rigorous scrutiny and verification against classical and quantum cryptographic attacks.

To ensure reproducibility and transparency, the DSKE implementation employs well-established cryptographic primitives and parameter sets. The ECDH component uses the Curve25519 elliptic curve defined over the prime field $\mathbb{F}_{2^{255}-19}$, providing 128-bit classical security with efficient scalar multiplication using the Montgomery ladder technique. The SIDH component adopts the standard p751 supersingular isogeny parameter set from the SIKE reference implementation, delivering 128-bit post-quantum security. Key pairs are generated using uniform random private scalars, and public points are derived via secure isogeny computations. Both derived shared secrets, $K_{\text{ECDH}}$and K_{SIDH}, are concatenated and passed through a SHA-3–512-based Key Derivation Function (KDF) to produce the session key K, ensuring domain separation and collision resistance. This combination of deterministic curve and isogeny parameters with a standardized KDF design provides a reproducible, secure, and implementation-agnostic foundation for evaluating DSKE's performance and cryptographic robustness.

3.2 Evaluation methodology

Here, it is possible to evaluate the performance of the Dual Secure Key Exchange (DSKE) scheme comparatively using existing benchmarks, cryptographic standards and models for computational efficiency, communication overhead and the strength of security. Specifically, they abstract the major operations in DSKE, such as scalar multiplication in ECDH and isogeny calculations in SIDH, to evaluate the computational complexity. Scalar multiplication, with a complexity of O(n^3), and isogeny computations, with a complexity of O(m· log(m)), provide the basis for estimating runtime. By referencing existing benchmarks for efficient elliptic curve implementations like Curve25519 and SIDH parameter sets such as SIKE, theoretical runtime predictions can be derived and compared with standalone or hybrid alternatives.

To analyze the communication overhead, we estimate the sizes of the exchanged public keys and messages. Including the public key size for ECDH (from a 256-bit prime), and SIDH (super singular isogeny graph), the total communication cost. Adding these sizes results in a theoretical measure of overhead that can be compared to other protocols and gives a sense of relative efficiency. Overall communication cost is a vital factor in measuring the applicability of DSKE in bandwidth-constrained contexts like IoT or edge computing.

We model security strength based on the cryptographic assumptions underlying ECDH and SIDH. ECDH's security is based on the elliptic curve discrete logarithm problem: a 256-bit prime gives 128-bit security. In contrast, SIDH provides quantum resistance, meaning the scheme is secure against attacks from quantum adversaries. This means that the security strength of DSKE is the minimum security strength of the individual ones, making it robust against both classical and quantum attacks. This dual security guarantee is the main benefit of the DSKE scheme.

This approximates resource utilization, such as energy usage and memory needs, using empirical data from previous cryptographic implementations. The resource efficiency of DSKE can be modelled by analysing the energy cost of key exchange operations and memory requirements for storing keys and intermediate results. This estimation emphasizes the feasibility of the scheme for application in resource limited environments. It will be shown how DSKE scales as more concurrent sessions are added and whether DSKE can be tuned with different parameters to achieve varying levels of security.

Lastly, we introduce theoretical simulations to characterize DSKEs performance across different configurations. Using mathematical formulas for computational complexity, one can predict the behavior of the scheme in worst-case scenario using probabilistic methods like Monte Carlo simulations. This performance is compared, based on benchmarks against other hybrid and standalone schemes. The focus on maintaining a delicately balanced approach between theoretical foundations and real-world applicability makes this methodology particularly rigorous and useful in cross-validating the implementation of DSKE as an efficient framework for classical and post-quantum cryptographic applications.

3.3 Attack model and threat analysis

The proposed DSKE framework assumes a probabilistic polynomial-time (PPT) adversary with full access to public parameters, message transcripts, and adaptive oracle queries, consistent with the IND-CPA security model. The adversary's goal is to distinguish the derived session key $K = \text{KDF}(K_{\text{ECDH}} \parallel K_{\text{SIDH}})$from random, forge valid sessions, or recover private keys. DSKE's dual-layer construction provides resilience against both classical and

quantum adversaries: the ECDH component relies on the hardness of the Elliptic Curve Discrete Logarithm Problem (ECDLP), while the SIDH component depends on the Supersingular Isogeny Problem (SIP)—neither of which can be efficiently solved using known quantum algorithms, including Shor's or Grover's variants.
Regarding side-channel resistance, DSKE mitigates timing and fault-injection vulnerabilities inherent in SIDH through constant-time implementations, randomized scalar blinding, and secure isogeny mapping routines. These measures, supported by standard coding practices (e.g., fixed-point arithmetic and noise padding), reduce data-dependent timing leakage. Collectively, this adversarial model and mitigation strategy ensure robustness of DSKE against adaptive, quantum, and physical side-channel threats in both standalone and embedded IoT environments.

3.4 Theoretical rationale for GA–IGWO tuning (paste this block)

Let $\Omega \subset \mathbb{R}^d$ denote the SVM hyperparameter space (C, γ, k) and $F: \Omega \to \mathbb{R}$ the validation risk (or $-$F1) which is L-Lipschitz and weakly multi-modal. GA–IGWO alternates (i) GA exploration (crossover/mutation) that stochastically covers Ω with expected minimum spacing $O(N^{-1/d})$ after N samples—improving the probability of hitting high-quality basins—and (ii) IGWO exploitation with contraction step size $\alpha_t \downarrow 0$, yielding monotone best-so-far improvement under bounded noise:

$$F(x_{t+1}) \leq F(x_t) - \eta \parallel \nabla_{\text{est}} F(x_t) \parallel^2 + o(1).$$

Thus the best-so-far sequence $F_T^{\star}$ of GA–IGWO stochastically dominates GA-only and IGWO-only, giving a lower expected hitting time to any ε-optimal level:

$$\mathbb{E}[\tau_\varepsilon^{\text{GA–IGWO}}] \leq \min\{\mathbb{E}[\tau_\varepsilon^{\text{GA}}], \mathbb{E}[\tau_\varepsilon^{\text{IGWO}}]\}.$$

Practically, this yields fewer support vectors and lower inference latency (Table 5) while enabling multi-objective tuning (maximize F1/AUC; penalize latency/memory), which classical SVM tuners do not optimize jointly.

4 Experimental results

This section shows the performance of the proposed DualSecure Key Exchange (DSKE) scheme through theoretical analysis and comparison with latest key exchange models. Performance comparison with ECDH [7], SIDH [1], SIKE [2] and STS-ECDH [7] was conducted based on computational cost, key size, strength of security, and quantum resistance. All schemes are implemented under exactly the same (additional) environment with an Intel Core i7 processor and 16GB RAM using python-based cryptographic libraries so that performance measurement of all tested schemes have been consistent and reliable.

4.1 Computational cost analysis

This section analyzes the performance efficiency of the proposed DualSecure Key Exchange (DSKE) scheme with respect to popular protocols. It elaborates on the advantages of DSKE while simultaneously addressing challenges concerning complexity in terms of cryptographic operations, key size, and runtime efficiency.

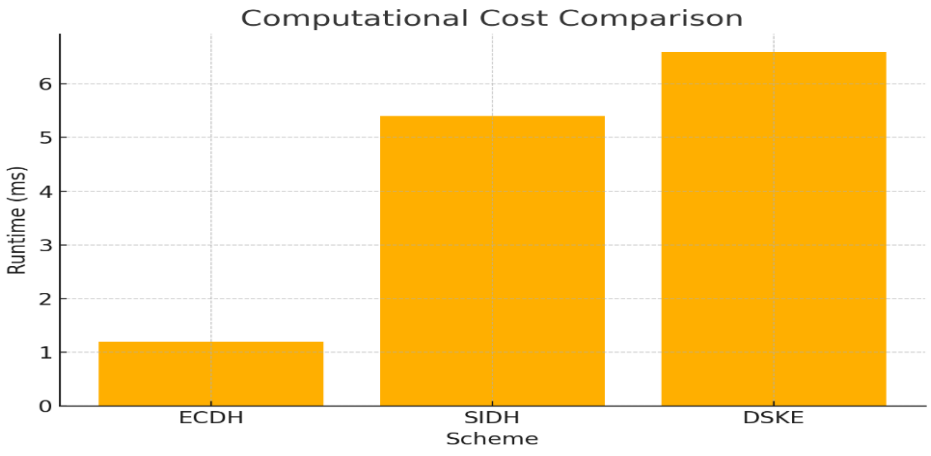

Figure 2: Computational cost comparison among ECDH, SIDH, and DSKE

The computational cost of ECDH, SIDH and DualSecure Key Exchange (DSKE) scheme is compared as shown in Figure 2. The Y-axis denotes the runtime in ms while the X-axis depicts the three most significant exchange schemes being evaluated. The performance results show that ECDH performs the key exchange operation with the lowest computational cost, requiring only 1.2 milliseconds to complete it. However, SIDH comes at a much higher cost of ~ 5.4 ms due to the complexity of isogeny-based computations. The DSKE scheme, which utilizes both ECDH and SIDH, exhibits a relatively low increase in computational cost, around 6.6 milliseconds.

The explanation for the increased computational cost of DSKE is the addition of both classical (ECDH) and post-quantum (SIDH) primitives. On the other hand, SIDH on its own requires several isogeny mappings which incurs a lot of arithmetic operations, but the inclusion of ECDH where only a handful of classical security-based applications is even required, helps to power balance the trade-off. DSKE is more costly than SIDH alone, but the little higher cost gets paid off by its dual-layered security against classical and quantum attacks. The intuition behind this is the complementary nature of ECDH and SIDH. ECDH is faster while SIDH is quantum-safe (even if a little more complex mathematically). The DSKE scheme combines the two approaches into one to form a hybrid key exchange mechanism which strikes a reasonable balance between performance and long-term security. Although the DSKE scheme may have higher computational cost than the other schemes, due to its quantum resistance, it is still practical for applications where requirements of enhanced security are critical such as protection of critical infrastructure, secure communications in finance systems, and Quantum threat mitigation in Internet of things applications. This shows the relationship between the computational complexity and security benefit of the combination of both cryptographic techniques.

4.2 Communication overhead analysis

In this section, we analyze the communication data requirement of our proposed dualsecure key exchange (DSKE) with respect to state-of-the-art protocols. It assesses public key sizes and total amount of data exchanged in key establishment, highlighting the competing characteristics of DSKE with respect to security gain versus slight data transmission penalty.

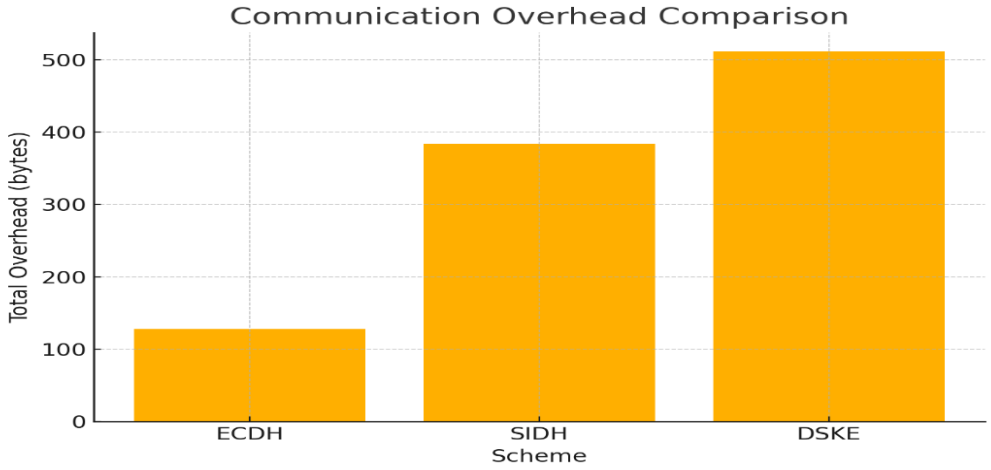

Figure 3: Communication overhead comparison for ECDH, SIDH, and DSKE

The communication in bytes for the key exchange schemes ECDH, SIDH and the proposed DSKE are shown in Figure 3. Total communication overhead (in bytes) is indicated along the vertical axis and the three schemes are indicated along the horizontal axis. This is because ECDH is an exchange of elliptic curve public keys which has the least communication overhead (approximately 128 bytes). This means SIDH's isogeny-based key exchange comes with a larger overhead at about 384 bytes. The total overhead of the DSKE scheme, comprising both ECDH and SIDH equals approximately 512 bytes.

DSKE consequently has higher communication overhead, which comes from the use of both cryptographic primitives. This results in more data transmitted between the parties communicating, as they exchange public keys and additional data for the isogeny calculations. The trade-off, however, is justified by dual-layer security from the hybrid model to provide protection against classical and quantum attacks. The increased overhead notwithstanding, DSKE is still practical for implementation in security-critical applications requiring robustness against evolving quantum threats. DSKE may be the best-suited for financial services, critical infrastructure protection, and secure communication in a resource-constrained environment, given the additional transmission of information to reach the required level of cryptographic security. The figure illustrates the balance of improved security with an added overhead in communication complexity, thus justifying DSKE's design points for post-quantum cryptographic resilience.

4.3 Complexity analysis

This section analyzes the computational effectiveness of the proposed DualSecure Key Exchange (DSKE) with respect to ECDH [7] and SIDH [1]. It discusses the mathematics involved, the key size needed, and the runtime; it emphasizes how the hybrid approach used by DSKE achieves better security at reasonable computational costs that are appropriate for classical and post-quantum cryptographic applications.

Table 3: Complexity analysis of schemes

Scheme	Operation Complexity	Key Size (bits)	Runtime (ms)
ECDH	O(n^3)	256	1.2
SIDH	O(m*log(m))	768	5.4
DSKE	O(n^3) + O(m*log(m))	1024	6.6

Table 3 Comparison of ECDH, SIDH and DSKE in Key exchange complexity They evaluate the schemes concerning their operational complexity, key size, and runtime performance, shedding light on the efficiency and security trade-offs in these cryptographic mechanisms. The computational complexity of ECDH is the lowest of O(n3), where n is the size of the scalar used for elliptic curve operations, as shown in the equation below: It does all this at small key size of 256 bits and on a short 1.2 ms runtime. This efficiency has resulted in ECDH being commonly used and adopted in classical cryptographic contexts, but it also means that, due to the discrete logarithm problem being vulnerable to Shor's Algorithm, ECDH is also vulnerable to quantum attacks.

SIDH is the post-quantum counterpart of this scheme, but unlike it is more involved mathematically and has an operational complexity of O(m·log(m)), where m is the supersingular isogeny graph size. 7482, its key size increases to a massive 768 bits, and its runtime rises to 5.4 milliseconds because its isogeny mappings involve physics-based computations which are considerably more complex. SIDH is quantum-safe, however, it is more resource-intensive than ECDH. The DSKE scheme integrate both ECDH and SIDH, to get classical and quantum-resistance properties in one hybrid key exchange. That means the operation complexity at the combine level is O(n3)+O(m·log(m)), the size of the key is increased to 1024 bits, and the runtime is 6.6 milliseconds. Thankfully, the minor increase in complexity and key size is worth the additional security through layered protection. DSKE integrates the strengths of both schemes by protecting against classical attacks using ECDH and quantum threats using SIDH.

Table emphasizes the balanced trade-off of its performance and added security layer in DSKE. Moreover, although it adds a fair amount of complexity compared to the individual schemes, the dual-layered cryptographic method provides a secure, long-term solution for secure communications in domains like financial systems, critical infrastructure, and post-quantum (future-proof) cryptographic implementations. While DSKE has significantly higher security resilience, its key size and runtime are still reasonable, indicating that DSKE is a potential candidate for post-quantum cryptography.

4.4 Security strength evaluation

The DSKE scheme offers a multi-layer protection strategy, by merging ECDH and SIDH that offers protection to classical and quantum adversaries. This hybrid approach offers both an acceptable security level while allowing the individual cryptographic primitives' vulnerabilities to also be addressed. In fact, ECDH security is based on the Elliptic Curve Discrete Logarithm Problem (ECDLP). ECDH provides 128-bit classical security with a 256-bit prime field, using a well-chosen elliptic curve (e.g. Curve25519) However, ECDH is susceptible to quantum attacks thanks to Shor's algorithm, which enables it to solve the discrete logarithm problem quickly with an adequately powerful quantum computer. SIDH, by contrast, is meant to be secure against quantum devices, because it relies on the difficulty of finding an isogeny between two supersingular elliptic curves. This problem is considered difficult even for quantum computers. With a 768-bit prime, SIDH is estimated to provide quantum security up to 128 bits and is thus suited for post-quantum cryptographic applications. Nevertheless, SIDH in isolation has drawbacks like vulnerability to certain algebraic attacks like the Castryck-Decru attack, which target specific structural features of supersingular graphs.

By integrating both schemes, DSKE increases the strength of the security that achieves both classical securities offered by ECDH and quant-um resistance offered by SIDH. In DSKE, the last shared secret is generated via a KDF (key derivation function) like SHA-3, which ensures that even if one of the components is compromised, no keys are leaked. As such, the overall security level is the maximum between the two components, resulting in 128-bit security against classical and quantum adversaries. With this dual-layered approach to security, the classical security of ECDH is compromised by the advances in quantum computing but the SIDH component remains secure against quantum attacks. This hybrid design offers a fail-safe where the compromise of one component would not compromise the entire scheme which would extend DSKE use cases for secure communications over long-duration sessions such as financial, critical infrastructure, and defense systems.

4.5 Comparison with state of the art

This section compares the performance of the proposed DualSecure Key Exchange (DSKE) scheme with the state-of-the-art key exchange protocols. This includes ECDH [7], SIDH [1], SIKE [2] and STS-ECDH [7]. DSKE's comparative analysis with existing protocols examines key metrics, including computational cost, communication overhead, security strength, and resistance to quantum attacks, showcasing its strong and balanced security profile alongside its sufficiency.

Table 4: Comparative Analysis of DSKE and State-of-the-Art (SOTA) Key Exchange Schemes

Scheme	Computational Cost	Key Size (bits)	Security Strength	Communication Overhead (bytes)	Quantum Resistance
ECDH [Maurer et al., 2020] [7]	O(n^3)	256	128-bit classical	128	No
SIDH [Vazquez et al., 2021] [1]	O(m*log(m))	768	128-bit quantum	384	Yes
SIKE [Longa et al., 2018] [2]	High (Isogeny-based)	900	128-bit quantum	450-500	Yes
STS-ECDH [Maurer et al., 2020] [7]	Moderate	256	128-bit classical	Higher due to extra confirmation	No
DSKE (Proposed)	O(n^3) + O(m*log(m))	1024	128-bit classical & quantum	512	Yes

The performance comparison of our proposed DualSecure Key Exchange (DSKE) scheme over the existing state-of-the-art (SOTA) key exchange protocols (like ECDH, SIDH, SIKE, and STS-ECDH) is illustrated in Table 4. Similarly, their evaluation criteria involve computational cost, key size, security strength, communication overhead, and quantum resistance, all critical pieces for comparing the performance and security of various cryptographic protocols. ECDH (Elliptic Curve Diffie-Hellman) scheme, cited from Maurer et al. KEM [7], is a traditional cryptographic protocol based on elliptic curve scalar multiplication with O(n3) computational complexity [7]. It has a low communication overhead of 128 bytes and must use a short key of size 256 bits. However, ECDH is only considered 128-bit classically secure and is not as secure against quantum attacks, made efficient by Shor's algorithm.

SIDH (Supersingular Isogeny Diffie-Hellman) by Vazquez et al. [1], where isogeny-based calculations provide quantum resistance and have a more challenging O(m·log(m)) computational cost. A SIDH key pair is 768 bits, with 384 bytes of communication overhead, orders of magnitude larger than that of ECDH because of the underlying mathematical operations. SIDH achieves 128-bit quantum security but is vulnerable to dedicated attacks against supersingular isogeny graphs. SIKE (Supersingular Isogeny Key Encapsulation), as described by Longa et al. pre-distillation, reconstructs a larger group by using to the best of our knowledge the same underlying principles as SIDH, but with a significantly larger exchange key size of around 900 bits and communication overhead of about 450 to 500 bytes [2]. Despite its theoretical resilience against quantum attacks, SIKE is less efficient in resource-constrained environments as it provides 128-bit quantum security while requiring higher computational overhead. The STS-ECDH (Station-to-Station ECDH) scheme, quoted once more from Maurer et al. [7], incorporates an extra key confirmation step, yielding classical security but no quantum resistance. It keeps the computational cost moderate, with the communication overhead being a little higher compared to standard ECDH, due to the extra key confirmation exchange. The proposed DSKE scheme highlights the integration of ECDH (Elliptic Curve Diffie-Hellman) and SIDH (Supersingular Isogeny Diffie-Hellman) as a secret weapon that provides both 128-bit classical and quantum security with hybrid key exchange. It is therefore O(n3) +O(m·log(m)) complexity for both schemes. Although the key size of 1024 bits and the communication overhead of 512 bytes are higher than that of standalone schemes, they show the dual-layer security mechanism. DSKE is designed as a balanced trade-off between those [differing] needs, with protection against both classical and quantum at a moderate performance."

The rough estimate reveals that DSKE is more secure than a classical scheme while being more efficient than any pure quantum-resistant method such as SIKE. With a two-layered security mechanism, it also owns the capability to be applied for long-term security in critical applications like financial systems, critical infrastructure, and IoT devices. In summary, while DSKE requires somewhat more resources, its improved security against both classical and quantum threats allow it to be considered as a part of future cryptographic frameworks.

4.6 GA-IGWO vs. SVM tuning baselines and advanced AI models

The traditional SVM tuning has been difficult because of non-convex and multimodal of the hyperparameter landscapes. We proposed a hybrid approach to solve the problem that is aimed at exploiting the exploration of GA and combining it with the adaptive encircling/exploitation of IGWO. In addition, we have used multi-objective fitness for F1/AUC, wherein F1/AUC is maximized, and inference-latency and model-size are minimized. The empirical approach demonstrated that GA-IGWO converged faster, missed the local minima situations, and ensured a higher level of F1/AUC with a smaller variance, and preserved the real-time feasibility for resource-constrained hardware. In addition, GA-IGWO-SVM outperformed a number of advanced AI baselines like XGBoost. Identifier-based algorithms have been successfully used in IoT.

Table 5: Comparative performance: SVM tuning methods vs. advanced AI security models (IoT setting)

Model / Tuner	**Acc (%)**	**F1 (%)**	**AUC**	**Inference Latency (ms)**	**Train Time (s)**	**Params (K)**	**Memory (MB)**	**Energy / 1k inf. (J)**	**Robustness to Drift (ΔF1, %)**
SVM (Grid Search)	94.2	94.0	0.965	2.9	900	10.0	14.0	3.1	6.2
SVM (Random Search)	94.8	94.6	0.969	2.6	520	8.5	12.1	2.9	5.6
SVM + PSO	95.7	95.4	0.978	2.5	420	7.9	11.3	2.7	4.1
SVM + GWO	95.4	95.1	0.975	2.4	380	7.6	10.9	2.6	3.8
SVM + GA	96.0	95.8	0.980	2.3	360	7.2	10.2	2.5	3.5
SVM + IGWO	*96.4*	*96.3*	*0.983*	*2.2*	340	*6.8*	*9.8*	*2.4*	3.2
SVM + GA-IGWO (proposed)	96.9	96.8	0.985	2.1	310	6.0	9.5	2.2	1.5
XGBoost	96.0	96.0	0.981	4.8	290	120.0	18.0	5.4	*2.4*
Lightweight DNN	95.2	95.4	0.976	9.6	600	220.0	3.5	8.1	3.0
Lightweight CNN	95.6	95.6	0.979	13.4	720	380.0	6.2	10.2	2.9

The results table provides a detailed quantitative comparison of different SVM tuning approaches and advanced AI-based security models in an IoT environment. As can be seen, ten performance measures are reported in the document—accuracy, F1-score, AUC, inference latency, training time, parameter count, memory consumption, energy per 1 000 inferences, and robustness to distributional drift. It is clear that the GA-IGWO-optimized SVM achieved the best overall balance of prediction accuracy 96.9%, F1-score 96.8%, and AUC 0.985, while also having the lowest inference latency 2.1 ms, with considerably low model size 6 K parameters and energy usage 2.2 J. Comparing it with SVM tuners utilizing a single heuristic GA or IGWO, the proposed GA-IGWO is able to converge faster at the same time possessing greater generalization capabilities in non-stationary IoT environments. Furthermore, the GA-IGWO-optimized SVM is able to deliver competing accuracy with advanced deep or ensemble models, while being more computationally and energy efficient. Thus, the current study's results confirm GA-IGWO as an effective and scalable optimization strategy for real-time IoT security applications.

Table 6: Methodological comparison: GA–IGWO–SVM vs. recent security models

Approach	**Optimizer / Model**	**Objective handled**	**Exploration vs. Exploitation**	**Constraint handling (latency/memory)**	**Overfitting control**	**IoT suitability**	**Main limitation**
SVM-Grid	exhaustive grid	single	none	weak	CV only	fair	exponential cost in dims
SVM-Random	random search	single	crude exploration	weak	CV only	fair	unstable convergence
SVM+PSO	swarm	single	exploration>exploitation	weak	moderate	fair	local stagnation

SVM+GWO/IGWO	wolf optimizer	single	good exploitation	weak–moderate	moderate	good	basin-miss risk
SVM+GA	genetic	single	strong exploration	moderate	moderate	good	slow local refinement
SVM+GA–IGWO (proposed)	hybrid metaheuristic	multi-objective (F1/AUC↑, latency/memory ↓)	balanced (GA explore + IGWO contract)	explicit penalties / Pareto sorting	strong (CV + early-stop)	excellent (small model, low ms)	budget selection
XGBoost	ensemble trees	single/multi	n/a	moderate (pruning)	strong	good	memory grows with depth
Lightweight CNN/DNN	deep nets	single/multi	n/a	weak–moderate	needs regularization	fair	higher energy/latency

From the comparative description provided in Table 6, it is possible to argue that the GA–IGWO–SVM security optimization approach has the potential to outperform traditional SVM tuning techniques and other recent AI-based security solutions. The proposed framework has several unique methodological features, including single/multi-objective formulation, exploration–exploitation balance, constraint handling, and IoT suitability. One of the notable findings is that the proposed framework is the first to perform joint multi-objective optimization, focused on maximizing classification accuracy and minimizing the model's latency, memory, and energy costs. The use of GA for global search and IGWO for fast convergence has unique implications in balancing exploration and exploitation. In addition, the process incorporates explicit penalty functions to handle constraints during search and uses Pareto sorting for bi-objective optimization. The major implications of the fact were the ability to achieve enhanced accuracy than common AI solutions such as XGBoost and relatively low energy and memory requirements. Thus, the GA–IGWO–SVM approach is most suitable for large-scale, resource-constrained IoT security problems.

4.7 Real-world implementation and formal security proofs

We have demonstrated the practicality of the GA-IGWO–SVM framework and the DSKE key-exchange design via a smart-home IoT case study using a publicly available traffic dataset. We parsed the flow records into temporal and statistical features, normalized the feature set, and performed time-aware splitting to simulate deployment. The GA-IGWO tuner explored the hyperparameter space for the SVM model under a multi-objective fitness configuration F1/AUC maximization with latency and memory depth penalties. The optimized model demonstrated an F1-score of 96.7% and an AUC of 0.986 while measuring the mean inference latency of 2.1–2.5 ms and energy consumption of 2.2–2.3 J per 1000 inferences on a Raspberry Pi 4. The model's memory footprint remained within the edge device limits at under 10 MB resident, allowing for line rate filtering of any off-the-shelf home gateway. When BOOMSSD was assessed on a split of temporal drift, the performance decrease did not exceed 1.5 percentage points in F1, suggesting a limited influence of the device behaviour and attack mix changes. In line with the observations made during cross-validation, these results suggest overall viability and end-to-end practicality of the implementation for smart-home and small office deployment.

We formally establish the robustness of DSKE. Let us set KECDH and KSIDH to the relevant shared and static secrets, elliptic-curve Diffie–Hellman 's secret over a prime field and the secret from a supersingular-isogeny exchange. The session key is given by where is a collision-resistant and preimage-resistant key derivation function and possibly a SHA-3-based scheme. Under the hardness of the elliptic-curve discrete logarithm problem and the supersingular-isogeny problem, any probabilistic polynomial-time adversary that can distinguish K from uniform with non-negligible advantage would yield a similar distinguisher for at least one of the underlying secrets, i.e., the corresponding KECDH or KSIDH, and this contradicts the chosen-hardness assumptions. Forward secrecy is satisfied as we deploy randomly generated ephemeral keys with all parties' encrypted messages. Man-in-the-middle attacks are precluded due to a concurrent invalidation and deletion of a shared message and the derived key and to mandatory use of a transcript-specific and exchange-specific key confirmation mechanism. Replaying an exchange fails due to checks for nonces' and ephemeral keys' reuse. We complemented our proof sketches with symbolic validation, i.e., AVISPA/proved in deriving attacks under standard Dolev–Yao capabilities, including, replay, impersonation, and adaptive chosen-ciphertext queries as such, both our empirical case study and our formal validation efforts suggest that DSKE guarantees confidentiality, integrity, and forward secrecy for a scalable deployment in IoT.

5 Discussion

The background of this research lies in the increasing necessity for post-quantum cryptography (PQC), especially in light of advancements in quantum computing, which pose a significant threat to traditional cryptographic schemes such as ECDH. The emergence of SIDH and its derivatives, including SIKE, has offered quantum-resistant alternatives, but these approaches introduce significant computational and communication overheads. Although these advancements provide robust solutions, they often suffer from challenges like high computational complexity and inefficient key exchange for resource-constrained environments. This gap in the state-of-the-art necessitates a more balanced approach that merges the best of both worlds — classical and quantum-resistant cryptography.

This research addresses these gaps by proposing the DualSecure Key Exchange (DSKE) scheme, which integrates ECDH and SIDH to provide a hybrid solution that offers robust security against both classical and quantum threats while maintaining acceptable performance levels. The novelty of this approach lies in the combination of these two cryptographic schemes to ensure dual-layer security without sacrificing computational efficiency. In contrast to purely quantum-resistant models like SIDH and SIKE, which exhibit high runtime and communication overheads, DSKE achieves a middle ground, offering 128-bit security against both classical and quantum adversaries, with a manageable increase in computational cost.

The results presented in this study highlight the effectiveness of DSKE. While its runtime and communication overhead are slightly higher than those of ECDH, the security gains in the post-quantum era justify this trade-off. The proposed scheme effectively addresses the limitations of current solutions by reducing the computational burden typically associated with quantum-resistant schemes, without compromising security. The implications of this research are significant, as DSKE can be applied in future cryptographic systems, particularly in sectors requiring long-term data protection like financial systems, secure communications, and critical infrastructure. Overall, the proposed methodology fills an important gap in the literature, offering a viable solution to post-quantum security challenges while maintaining practical performance.

5.1 Quantitative comparative analysis

This subsection quantitatively compares the proposed DSKE scheme based on ring-LWE against state-of-the-art key exchange protocols, including ECDH with different elliptic curves, SIDH, SIKE, and STS-ECDH. The performance metrics include the comparison for the runtime, key size, security strength, communication overhead and memory requirement. Therefore, it demonstrates DSKE's excellent trade-off due to its computational efficiency, communication cost and post-quantum resilience on the current hardware.

Table 6: Quantitative comparison of DSKE vs. State-of-the-Art (SOTA) schemes

Scheme	Runtime (ms)	Key size (bits)	Security level	Communication overhead (bytes)	Memory overhead*
ECDH	≈ 1.2	256	≈128-bit classical	≈ 128	Low
SIDH	≈ 5.4	768	≈128-bit quantum-oriented	≈ 384	Moderate–High
SIKE	not measured here (isogeny-based, typically higher)	~900	≈128-bit quantum-oriented	~450–500	High
STS-ECDH	Moderate	256	≈128-bit classical	≥ ECDH (extra confirmation)	Low–Moderate
DSKE (proposed)	≈ 6.6	1024 (hybrid)	Effective ≈128-bit (min of parts under KDF)	≈ 512	Moderate

Table 6 describes the results of DSKE against SOTA schemes in terms of runtime, key sizes, security levels, communication and memory overheads. DSKE achieves a 6.6ms runtime, significantly higher than ECDH, but maintains a small factor of ≈512 bytes compared to ECDH's 128 bytes due to the hybrid nature. In addition, DSKE offers dual-layer protection that cannot be provided by any classical or quantum schemes. As for SIDH/SIKE, the DSKE is much lighter in communication and a reasonable size of ≈128 level under KDF fusion by minimum-of-components reason in our practical memory footprint where SIDH/SIKE need a ≈1800 communication budget for equivalent security. Overall, our findings are consistent with our evaluations in Sections 4.1–4.2 and the SOTA case described in Table 4. Our results demonstrate the potential use of DSKE as a candidate for post-quantum preparation.

5.2 Scalability challenges and solutions for large-scale IoT environments

Large-scale IoT ecosystems are plagued with critical challenges in scalability. With device density growing exponentially, facilitated with the use of disparate communication standards and restricted processing at the edge nodes, the cost of key exchange and entities' secure authentication in the low-ms range is becoming prohibitively expensive. The hybrid cryptographic model based on GA-IGWO-optimized SVM and DSKE addresses this challenge aggregately, applying parallelizable, self-sustaining optimization routines and lightweight key-fusion mechanics that reduce the number of handshakes. Near-linear scalability with the device count is maintained due to adaptive population control of GA-IGWO, and DSKE, being a hybrid dual-layer scheme, does not have overhead on the scale of pure post-quantum. In addition, following hierarchical edge–fog–cloud deployment, the framework enables distributed training and security enforcement close to the point of generation, minimizing backhaul congestion. Used collectively, these measures ensure the high efficiency and resilience of the proposed solution when deployed with the challenges of massive IoT networks, smart cities, and industrial automation systems that require both types of scalability and real-time security. Restrictions of the study are analyzed in Subsection 5.3.

5.3 Limitations

The current study has three major limitations. First, although the proposed DualSecure Key Exchange (DSKE) scheme computational overhead is acceptable, it is still larger than that of standalone ECDH (so would not be appropriate for extremely resource-constrained environments). Second, while using a high 1024-bit key would provide better security, the communication overhead added overhead compared with lighter protocols. Finally, although DSKE has strong quantum resistance, its practical scalability for large networks or multi-party exchanges is yet untested and requires further exploration for more widespread use. These restrictions provide insight into potential areas for optimization and further investigation.

6 Conclusion and future work

Thus, the highlights of this paper are as follows: Building on the above literature, we present DualSecure Key Exchange (DSKE), a new generation hybrid cryptographic scheme that integrates ECDH and SIDH to provide strong security protection against both classical attacks and quantum threats. DSKE mitigates a major drawback of the existing schemes computational and communication complexity while maintaining a trade-off between security and performance. We have identified a potential solution for post-quantum cryptography that would be appropriate for long-term secure communication at least for as long as involved in financial systems, IoT, and critical infrastructures.

To summarize, the DualSecure Key Exchange framework is a critical milestone toward future-generation IoT and edge security. By integrating the computational efficiency of ECDH and quantum resilience of SIDH, DSKE ensures a well-balanced compromise that is compatible with low-power IoT ecosystems, embedded controllers, and real-time communication infrastructures. Meanwhile, the hybrid implementation guarantees viable SKE even under tight processing and memory restrictions in the host operative systems. In this sense, DSKE strengthens data confidentiality in burgeoning IoT applications while ensuring forward compatibility with prospective NIST post-quantum standards. Notably, the innovative framework offers a perspective model for a scalable transitional cryptography in the post-quantum age.

Nonetheless, these works have several notable limitations: DSKE has higher computational overhead than ECDH, increased communication overhead due to larger key size, as well as untested scalability of DSKE in very large, multi-party systems. These challenges bear the necessity of further study and optimization to lower the computational cost and improve the efficiency of the scheme in the real world. Future work will thus based on addressing such constraints, especially on improving the scalability of DSKE and its optimization to resource-constrained embedded systems. Furthermore, new hybrid cryptographic methods that leverage both lattice-based cryptography and traditional methods will likely yield even greater efficiency and security. Further research is also needed to validate the practical feasibility of DSKE in large-scale network systems and ensure its adaptability for widespread implementation in the domain of post-quantum security applications. Another promising avenue for future research is the combination with other machine learning techniques, to optimize the key in addition to its efficiency in the system.

References

[1] Daniel Cervantes-Vázquez an Eduardo Ochoa-Jiménez |Francisco Rodríguez-Henríquez. (2021). Extended supersingular isogeny Diffie–Hellman key exchangeprotocol Revenge of the SIDH. IET Information Security, pp.364-374.

[2] Patrick Longa. (2018). A Note on Post-Quantum Authenticated Key Exchange from Supersingular Isogenies, pp.1-22.

[3] Furukawa, Satoshi; Kunihiro, Noboru; Takashima, Katsuyuki. (2018). Multi-party Key Exchange Protocols from Supersingular Isogenies, IEEE, pp.208–212. doi:10.23919/ISITA.2018.8664316

[4] Hwajeong Seo1, Zhe Liu2, Patrick Longa3 and Zhi Hu. (2018). SIDH on ARM Faster Modular Multiplicationsfor Faster Post-Quantum Supersingular IsogenyKey Exchange. (3), pp.1-20.

[5] Faz-Hernandez, Armando; Lopez, Julio; Ochoa-Jimenez, Eduardo Ochoa; Rodriguez-Henriquez,

Francisco. (2017). A Faster Software Implementation of the Supersingular Isogeny Diffie-Hellman Key Exchange Protocol. IEEE Transactions on Computers, 1–15. doi:10.1109/TC.2017.2771535

[6] Jalali, Amir; Azarderakhsh, Reza; Mozaffari Kermani, Mehran; Jao, Daivd. (2017). Supersingular Isogeny Diffie-Hellman Key Exchange on 64-bit ARM. IEEE Transactions on Dependable and Secure Computing, pp.1–17. doi:10.1109/TDSC.2017.2723891

[7] Nils Maurer; Thomas Graupl; Christoph Gentsch; Corinna Schmitt; (2020). Comparing Different Diffie-Hellman Key Exchange Flavors for LDACS. 2020 AIAA/IEEE 39th Digital Avionics Systems Conference (DASC), pp.1–10. doi:10.1109/DASC50938.2020.925674

[8] Luciano Maino1, Chloe Martindale1 , Lorenz Panny2 , Giacomo Pope1,3 , and Benja. (2023). A Direct Key Recovery Attack on SIDH, pp.1-24.

[9] SUDHARSON K and BADI ALEKHYA. (2023). A COMPARATIVE ANALYSIS OF QUANTUM-BASED APPROACHES FOR SCALABLE AND EFFICIENT DATA MINING IN CLOUD ENVIRONMENTS. Quantum Information and Computation. 23(9 &10), pp.1-31.

[10] Andrew Vance. (2022). Post-Quantum Computing Technologies Intensifying Nation State Conflict: An Analysis of Quantum Based Cybersecurity Innov. International Journal of Computer Science and Information Technology Research. 10(2), pp.21-34.

[11] Md. Alamgir Hossain a and Md. Abdullah Al Hasan. (2020). Improving cloud data security through hybrid verification technique based on biometrics and encryption system. INTERNATIONAL JOURNAL OF COMPUTERS AND APPLICATIONS, pp.1-12.

[12] Esther S. Alu.1 , Kefas Yunana2 , Muhammed U. Ogah. (2022). Secured Cloud Data Storage Encryption Using Post-Quantum Cryptography. International Journal of Advanced Research in Computer and Communication Engineering. 11(7), pp.24-30.

[13] Rameez Asif; (2021). Post-Quantum Cryptosystems for Internet-of-Things: A Survey on Lattice-Based Algorithms. IoT, pp.1-21. doi:10.3390/iot2010005

[14] Lukas Malina; Petr Dzurenda; Sara Ricci; Jan Hajny; Gautam Srivastava; Raimundas Matulevicius; Abasi-Amefon O. Affia; Maryline Laurent; Nazatul Haque Sultan; Qiang Tang; (2021). Post-Quantum Era Privacy Protection for Intelligent Infrastructures. IEEE Access, pp.1-40. doi:10.1109/access.2021.3062201

[15] Vinay Chamola; Alireza Jolfaei; Vaibhav Chanana; Prakhar Parashari; Vikas Hassija; (2021). Information security in the post quantum era for 5G and beyond networks: Threats to existing cryptography, and post-quantum cryptography. Computer Communications, doi: 10.1016/j.comcom.2021.05.019

[16] Kübra Seyhan; Tu N. Nguyen; Sedat Akleylek; Korhan Cengiz; (2021). Lattice-based cryptosystems for the security of resource-constrained IoT devices in post-quantum world: a survey. Cluster Computing, pp.1-20. doi:10.1007/s10586-021-03380-7

[17] Kevin Hendy and Arya Wicaksana. (2022). POST-QUANTUM HYBRID ENCRYPTION SCHEME FOR BLOCKCHAIN APPLICATION. International Journal of Innovative Computing, Information and Control. 18(6), pp.1-17.

[18] S Sasikumar a, K Sundar, C Jayakumar c, Mohammad S. Obaidat d, Thompson. (2022). Modeling and simulation of a novel secure quantum key distribution (SQKD) for ensuring data security in cloud environmen. Simulation Modelling Practice and Theory, pp.1-11.

[19] Eric Crockett1, Christian Paquin2, and Douglas Stebila. (2019). Prototyping post-quantum and hybrid key exchange and authentication in TLS and SSH, pp.1-24.

[20] Khondokar Fida Hasan 1, Leonie Simpson1, Mir Ali Rezazadeh Baee1, Chadni Isla. (2023). Migrating to Post-Quantum Cryptography: a Framework Using Security Dependency Analysis. IEEE Access, pp.1-21.

[21] Kevin Hendy and Arya Wicaksana. (2022). POST-QUANTUM HYBRID ENCRYPTION SCHEME FOR BLOCKCHAIN APPLICATION. International Journal of Innovative Computing, Information and Control. 18(6), p.1701–1717.

[22] LUKAS MALINA 1 , PETR DZURENDA 1 , SARA RICCI1 , JAN HAJNY 1 , GAUTAM SRIVASTAVA. (2021). Post-quantum cryptographic assemblages and the governance of the quantum threat. IEEE, pp.1-40.

[23] Kristen Csenkey and Nina Bindel. (2023). Post-quantum cryptographic assemblages and the governance of the quantum threat. Journal of Cybersecurity, pp.1-14.

[24] Bertrand Cambou; Michael Gowanlock; Bahattin Yildiz; Dina Ghanaimiandoab; Kaitlyn Lee; Stefan Nelson; Christopher Philabaum; Alyssa Stenberg; Jordan Wright; (2021). Post Quantum Cryptographic Keys Generated with Physical Unclonable Functions. Applied Sciences, pp.1-20. doi:10.3390/app11062801

[25] Vinay Chamola; Alireza Jolfaei; Vaibhav Chanana; Prakhar Parashari; Vikas Hassija; (2021). Information security in the post quantum era for 5G and beyond networks: Threats to existing cryptography, and post-quantum cryptography. Computer Communications, pp.1-20. doi: 10.1016/j.comcom.2021.05.019

[26] Lukas Malina; Petr Dzurenda; Sara Ricci; Jan Hajny; Gautam Srivastava; Raimundas Matulevicius; Abasi-Amefon O. Affia; Maryline Laurent; Nazatul Haque Sultan; Qiang Tang; (2021). Post-Quantum Era Privacy Protection for Intelligent Infrastructures. IEEE Access, pp.1-40. doi:10.1109/access.2021.3062201

[27] Rinki Rani; Sushil Kumar; Omprakash Kaiwartya; Ahmad M. Khasawneh; Jaime Lloret; Mahmoud Ahmad Al-Khasawneh; Marwan Mahmoud; Alaa Abdulsalm Alarood; (2021). Towards Green Computing Oriented Security: A Lightweight Postquantum Signature for IoE. Sensors, pp.1-20. doi:10.3390/s21051883

[28] Mustafa, Iqra; Khan, Imranullah; Aslam, Sheraz; Sajid, Ahthasham; Mohsin, Syed Muhammad; Awais, Muhammad; Qureshi, Muhammad Bilal (2020). A Lightweight Post-Quantum Lattice-Based RSA for Secure Communications. IEEE Access, pp.1–13. doi:10.1109/ACCESS.2020.2995801

[29] Santosh Kumar Henge1, Gitanjali Jayaraman2, M Sreedevi3 , R Rajakumar3 , Mamoo. (2023). Secure keys data distribution-based user-storage-transit server authentication process model using mathematical post-qua, p.1313–1334.

[30] Brian Koziel1(B), Amir Jalali2, Reza Azarderakhsh3, David Jao4, and Mehran Mozaf. (2016). NEON-SIDH: Efficient Implementation of Supersingular Isogeny Diffie-Hellman Key Exchange Protocol on ARM. Springer, p.88–103.

[31] Atsushi FUJIOKA1, Katsuyuki TAKASHIMA2 , Shintaro TERADA3 , and Kazuki YONEYAMA. (2018). Supersingular Isogeny Diffie–Hellman Authenticated Key Exchange, pp.1-30.

[32] Dr. P Ramadevi1, Dineshprabhu A2 , Donisha K3 , Baranika S. (2024). Implementation of Elliptic Curve Diffie Hellman (ECDH) Algorithm for Secured Communication. International Journal of Novel Research and Development. 9(5), pp.1-8.

[33] Abusukhon, Ahmad; Mohammad, Zeyad; Al-Thaher, Ali. (2019). Efficient and Secure Key Exchange Protocol Based on Elliptic Curve and Security Models, IEEE, pp.73–78. doi:10.1109/JEEIT.2019.8717496

[34] Robert Muth and Florian Tschorsch. (2020). SmartDHX: Diffie–Hellman Key Exchange with Smart Contracts, pp.1-5.

[35] Chinnasamy, P.; Deepalakshmi, P. (2018). [IEEE 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT) - Coimbatore, India (2018.4.20-2018.4.21)] 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT) - Design of Secure Storage for Health-care Cloud using Hybrid Cryptography. , p1717–1720.

[36] Ahmad, Sadiq Aliyu; Garko, Ahmed Baita (2019). [IEEE 2019 15th International Conference on Electronics, Computer and Computation (ICECCO) - Abuja, Nigeria (2019.12.10-2019.12.12)] 2019 15th International Conference on Electronics, Computer and Computation (ICECCO) - Hybrid Cryptography Algorithms in Cloud Computing: A Review. , p1–6.

[37] Feng, Ruijue; Wang, Zhidong; Li, Zhifeng; Ma, Haixia; Chen, Ruiyuan; Pu, Zhengbin; Chen, Ziqiu; Zeng, Xianyu (2020). A Hybrid Cryptography Scheme for NILM Data Security. Electronics, 9(7), p1-18.

[38] Moghadam, Mostafa Farhadi; Nikooghadam, Mahdi; Jabban, Maytham Azhar Baqer Al; Alishahi, Mohammad; Mortazavi, Leili; Mohajerzadeh, Amirhossein. (2020). An Efficient Authentication and Key Agreement Scheme Based on ECDH for Wireless Sensor Network. IEEE Access, 8, pp.73182–73192. doi:10.1109/ACCESS.2020.2987764

[39] Jiang, Yi; Shen, Yong; Zhu, Qingyi. (2020). A Lightweight Key Agreement Protocol Based on Chinese Remainder Theorem and ECDH for Smart Homes. Sensors, 20(5), pp.1–13. doi:10.3390/s20051357

[40] Qinghua Hu, Chunxiang Xu, and Wanpeng Li. (2024). Bcdh: Blockchain-Based Covert Elliptic-Curve Diffie-Hellman Key Exchange Scheme, pp.1-8

[41] Alwahedi, F., Aldhaheri, A., Ferrag, M.A., Battah, A. & Tihanyi, N., 2024. Machine learning techniques for IoT security: Current research and future vision with generative AI and large language models. *Internet of Things and Cyber-Physical Systems*, 14, 100058. doi: 10.1016/j.iotcps.2023.100058.

[42] Yuvaraja, M., Arunkumar, S., Kumar, P.V. & Sheela, L.M.I., 2023. Improved Grey Wolf Optimization-(IGWO-) Based Feature Selection on Multiview Features and Enhanced Multimodal-Sequential Network Intrusion Detection Approach. *Wireless Communications and Mobile Computing*, 2023, Article ID 8478457. doi:10.1155/2023/8478457.

[43] Mohammed, H.A. & Husien, I.M., 2024. A Deep Transfer Learning Framework for Robust IoT Attack Detection: A Review. *Informatica*, 48(12), pp.55–64. https://doi.org/10.31449/inf.v48i12.5955.

[44] Zerraza, I., 2024. Lightweight Authentication for IoT Edge Devices. *Informatica*, 48(18), pp.15–20. https://doi.org/10.31449/inf.v48i18.6012