An Integrated Framework with Enhanced Primitives for Post-Quantum Cryptography: HEDT and ECSIDH for Cloud Data Security and Key Exchange

Shaik Mohammad Ilias*[1], V. Ceronmani Sharmila[2], V. Sathya Durga[3]
[1]Dept. of Computer Science and Engineering, Hindustan Institute of Technology and Science, Chennai, India.
[2]Department of Information Technology, Hindustan Institute of Technology and Science, Chennai, India.
[3]Department of Computer Science&Engineering, Hindustan Institute of Technology and Science, Chennai, India
E-mail: illusoft54@gmail.com, Csharmila@hindustanuniv.ac.in, sathyadv@hindustanuniv.ac.in
*Corresponding author:

Keywords: post-quantum cryptography (PQC), ECSIDH, HEDT algorithm, cloud data security, hybrid key exchange

Received: October 21, 2024

If adversaries were to obtain quantum computers in the future, their massive computing power would likely break existing security schemes. Since security is a continuous process, more substantial security schemes must be developed. Current PQC schemes primarily focus on data security or key exchange, and further improvement towards enhanced PQC primitives is required. Our proposal in this research is an innovative paradigm for PQC-focused cloud data security. The proposed HEDT approach achieves encryption and decryption with significantly lower latency (20% improvement) and higher reliability than AES, DES, and RSA, as demonstrated through experimental results. Furthermore, ECSIDH, a hybrid key exchange mechanism combining SIDH and ECDH, improves security strength by 50% while maintaining computational costs within 1.13x of SIDH. Compared to individual key exchange schemes like SIDH, ECSIDH offers superior security as a PQC candidate. These results confirm the robustness and efficiency of the proposed framework in ensuring secure data outsourcing and key exchange in cloud environments.

Povzetek: Predstavljen je integriran okvir z izboljšanimi elementi za post-kvantno kriptografijo (HEDT in ECSIDH) za varnost podatkov v oblaku in izmenjavo ključev.

1 Introduction

Quantum data processing has significantly enhanced computer capacity, but this may also be a blessing in disguise because attackers might abuse it to undermine already-in-place security measures. Studying PQC is the area that usescryptography to overcome such circumstances. Several academics have determined that new security schemes other than key exchange are required for data encryption and decryption. Liu et al. [27] predicted that Quantum computing will soon be available for purchase. Security systems may be compromised by adversaries who abuse their authority. They underlined the necessity of hybrid strategies to enhance data security in the context of PQC. They advised that the SIDH model be improved to serve as a PQC candidate for a key exchange mechanism. By altering its mathematics, Bos and Friedberger [28] looked into ways to strengthen SIDH. This shows that SIDH requires even more enhancement to be a viable candidate for PQC. Research by Costello et al. has also demonstratedthat ECDH key sharing and SIDH are targets for PQC attacks. [29]. They suggested making it a combination of the two to improve it and make it more secure.

This paper attempts to establish a secure and sound post-quantum cryptography framework using HEDT for secured data codes and ECSIDH for higher-order key exchange. Its main goal is to protect against vulnerabilities of traditional cryptographic systems, especially from quantum computer attacks. The proposed work postulates that combining HEDT hybrid encoding efficiency and ECSIDH security strength will surpass state-of-the-art techniques such as RSA, AES, and SIDH regarding appropriate security, computational efficiency, and scalability. It will provide a holistic cloud data security and key exchange solution with post-quantum fault tolerance, availability, and practicality considerations. This publication builds on our prior contributions, which are detailed below.

1. As a PQC contender for data encryption and decryption, we suggested the HEDT method with numerous data transformations.
2. A hybrid security architecture for key exchange was suggested. This one is a PQC candidate for key exchange under ECSIDH.
3. The two suggested and assessed systems are combined to create an integrated security architecture.

The following categories are used to group the remaining sections of the document. Section 2 thoroughly analyzes the literature on several components of secure data in the context of PQC, such as key exchange. Section 3 offers two safety techniques that are suitable choices for PQC.

This article presents a thorough study of the security considerations in Section 4 and explains the results of the tests. This study's fifth section gives an overview of the results obtained and suggests possible prospects for future investigation.

2 Related work

The study of different security techniques for enhanced data security and key exchange is examined in this section.

2.1 Data security schemes

One such security mechanism widely used in real-world applications is the AES. Using HEROKU as the selected cloud-based infrastructure, Et al. [1] looked at data security in cloud procedures. To better understand security latency and security strength, the researchers ran tests related to data security. Yu et al. [2] evaluated the assault in their research and suggested improvements to the AES architecture of encrypted data. Through the integration of hashing and cryptographic primitives, Chinnasamy and Deepalakshmi [3] introduced a mixed-security approach for cloud-based medical applications. Qian et al. [4] introduced a novel encryption technique that uses the Information Dispersal Technique (IDA) with multiple layers to increase security. Information Dispersal Algorithm (IDA) was employed in the secret sharing hierarchy technique devised by Shima and Doi [5]. Information security is the aim of its implementation.

The use of similarity hashing algorithms in situations that occur was investigated in the paper of Botacin et al. [6]. Within the detecting malware study, the researchers evaluated the benefits and limitations of their methodology. A method for assessing the complexity of IDA and its importance among systems that tolerate faults was provided by Marcelín-Jiménez et al. [7] in their paper.Fathur Ahmad and Ester [8] looked into the application of AES alongside the Rijndael algorithm to raise the level of protection of web data.The hybrid architecture dramatically increases the level of security, the researchers found—Kumar et al. [9] state that AES is crucial for field device execution. Hashing, AES, and RSA algorithms were introduced by Feng et al. [10] to improve data security. In the realm of data security, information dispersion theory is widely applied. Wijayanto and Harjito [11] state that there has been discussion on IDA's potential use as a safe file storage solution. A strategy was implemented to reduce the likelihood of rounding off errors about IDA. The literature in this field emphasizes the necessity of utilizing hybrid approaches that consider post-quantum cryptography (PQC) requirements to guarantee cloud data security.

2.2 Key exchange schemes

PQC has made significant contributions to key exchange systems research, which is thoroughly evaluated in this section. The exchanged keys method is the basis of the ECDH system. The DLP [12] forms the basis of DH. An elliptic curve's additive group of points is preferred by the ECDHthe protocol for key exchange over the multiplicative collection of integers in the DH protocol [13]. ECDH is the foundation of the security strategy outlined by Moghadam et al. [14] to supply expedited confirmation andsafe key exchange. A successful deployment of the method was made to improve cybersecurity in wireless sensor networks, or WSNs. ECC was the focus of the study for Shaikh et al. [15]. The researchers also studied Elliptic Curve Diffie-Hellman (ECDH) protocols—Caiet al. [16] — software-defined networks (SDNs).There is a chance that centralizing security components makes it easier to control them.

Swapna, Islam, et al. As part of the second area, Kambourakis et al.'s [17] research considered SDNs in the context of network security. One of the investigated aspects was the safety policies of the IEEE 802.21 standard. Researchers analyzed the safety efficacy of key exchange via ECDH in an SDN environment—the author Ghribi et al. We are first introduced to this in their paper by [18]. This hybrid technique is used for enhancing the security of UAV networks. In this hybrid methodology through which the protection of all communications based on blockchain is improved, it is ensured that the data keys are known to the user and not shared in person.

Li et al. proposed a new privacy-preserving device-linking protocol to secure users' connected devices and privacy. The work described in [19] suggests securing smart home networks is necessary. Zhang et al. proposed a method for generating a secret key that can be established between two parties over an insecure communication channel with the help of the Elliptic Curve Diffie-Hellman (ECDH), including edge AI [44]. [20]. This system was supposed to give us leak-proof key exchange and identification. Zhang et al. BAN was created by [20], which either sends the collected data to a centralized server for further analysis or processes it immediately by on board processors. Machine learning and AI techniques could mine the data for intelligence. Regarding IoT-integrated smart home applications, Ahmed [22] researched implementing security features based on ECDH. Srinivas et al. extended the protocol to the ECDH approach. And render one secure secret key using [23]. Table 1 summarizes the findings of the literature compared with those of the proposed work.

Table 1: Summary of literature findings compared with the proposed method

Method	Key Features	Security Level (bits)	Computational Cost	Key Size (bits)	Gaps/Limitations
AES	Symmetric encryption	128-256	Low	N/A	Vulnerable to brute force attacks with quantum advances.
RSA	Asymmetric encryption	1024-2048	High	1024-2048	Sizeable key size; slower for modern applications.
ECDH	Key exchange using elliptic curves	192-384	Moderate	192-384	Susceptible to quantum attacks.
SIDH	Post-quantum key exchange	128	Moderate	564	Requires optimization to reduce latency.
ECSIDH (Proposed)	Hybrid SIDH + ECDH	384	Moderate (1.13x of SIDH)	658	Improved security and scalability compared to others.
HEDT (Proposed)	Hybrid encoding and encryption	256-384	Low (20% faster than AES)	N/A	Incorporates PQC for enhanced data integrity and access.

ECDH is the foundation of Zhang et al.'s [24] security strategy for networks based on technology. Zhang et al. [25] carried out a thorough analysis of several security techniques applied in apps. The ECDH convention, which serves as a private key trade, was one of the systems whose security the researchers examined. As a potential competitor for post-quantum cryptography (PQC), a well-known key exchange technique is the SIDH protocol. The issue of SIDH was studied by Koziel et al. [26], emphasizing the technology used and the system's resistance to quantum assaults. Furthermore, they employed strategies to reduce pipeline pauses by utilizing optimal scheduling methodology. Compared to software libraries running affine SIDH algorithms, they are implemented faster. Alice and Bob can generate temporary public keys in 1.655 and 1.490 billion cycles, respectively, and can do so in 1.655 cycles. Compared with the 512-bit SIDH software equivalent, Vertex-7 improves performance by a factor of 1.5. The researchers' analysis proved that hardware implementation is feasible for isogeny-based, efficient, and reconfigurable approaches.

3 An integrated security framework that is proposed for post-quantum cryptography

The study introduces a brand-new protection framework, the IF-CDS, that adheres to Post-Quantum Cryptography (PQC) standards. The framework is displayed in Figure 1.

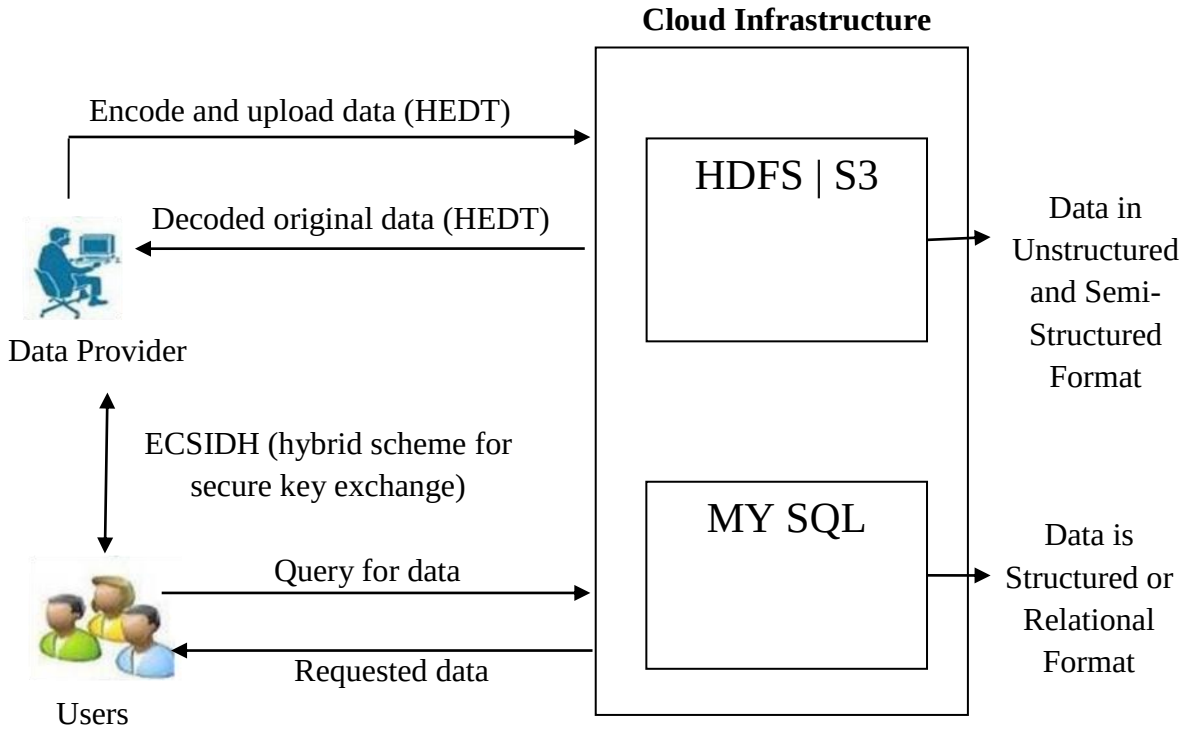

Figure 1: IF-CDS

The integrated architecture for cloud data security empowers the key exchange in a multi-user environment and data outsourcing in a secure manner. It is based on requirements from PQC specifications. The two security systems abstracted in the proposal are the Secure key exchange in a multi-user distributed environment using the ECSIDH combination technique and HEDT for safe cloud computing. The framework shows the data owner and users in many data environments. This secure framework can be used by data users (consumers) and data owners (producers). Things Like those definitions of proposed techniques

ECSIDH (elliptic curve super singular isogeny diffie-hellman hybrid)

ECSIDH is a hybrid key exchange protocol that integrates a post-quantum cryptography candidate scheme, namely, the Supersingular Isogeny Diffie-Hellman (SIDH) scheme with the classical Elliptic-Curve Diffie-Hellman (ECDH) protocol. The combination improves the security strength of SIDH's quantum resistance (SIDH) integrated with ECDH's computational efficiency while keeping the overall construction practical.

While SIDH's structure enables it to be crystalline concerning quantum attacks, as shown in Section 2, its use of classical cryptographic primitives leads to attacks as well; to address this, the ECSIDH hybrid method fortifies SIDH's structure, leading to a construction that is robust to both classical and quantum cryptographic attacks.

HEDT (hybrid encoding and decoding transformations)

HEDT is an encryption and decryption method for secure storage of cloud data. It uses the Data Encryption Standard (AES) algorithm to encrypt data, after which the Information Dispersal Algorithm (IDA) is for tolerance. The content of these encoded slices is hashed using a novel hashing process to ensure integrity. The hybrid mechanism of HEDT provides the desired security, fault tolerance, and reliability and protects against breaches and corruption in a distributed environment.

3.1 The proposed algorithm

This section provides the proposed HEDT algorithm. Encoding and decoding—The system has two processes that allow it to create robust data portability and increase security.

Algorithm: *HEDT*
Encrypting
1. *Start*
2. *Data owner inputs a file F*
3. $C \leftarrow ModifedAESEncrypt(F, sk)$
4. $S \leftarrow IDA(C, m, n)$
5. *For each slice s in S*
6. $s \leftarrow NovelHashing(s)$
7. *End For*
8. *Outsource S, hash and id to cloud*
9. *End*

Decrypting
1. *Start*
2. $S \leftarrow GetFromCloud(id)$
3. *Data integrity verification*
4. *IF there is integrity THEN*
5. $C \leftarrow IDAReconstruction(S, m, n)$
6. $F \leftarrow ModifedAESDecrypt(C, sk)$
7. *Return F to data owner*
8. *Else*
9. *Recover data*
10. *End If*
11. *End*

Method 1: HEDT algorithm

Two approaches are incorporated, as can be seen in Algorithm 1. The processes being studied are often called the decoding and the encoding processes. The first is intended to create secure data outsourcing, and the second is designed to provide data security and reliability. The entity holding the data, called a data owner, submits the information file to a third entity, called a service provider.Before being subjected to further techniques, file F is encrypted using modified AES. Steganography yields ciphertext C from the letter F. The encryption process uses a secret key, represented by the symbol sk. A secret key, represented by the symbol sk, is used during encryption. Following data collection, the information is tested using the IDA method to generate slices that improve the data's fault tolerance, availability, and dependability. The fundamental rationale for this strategy is the possibility that just a small number of cross-sectional samples will help reconstruct variable C. The slices are subjected to an innovative hashing algorithm, following which the generated data and its associated data are supplied, along with the hash values, to a public cloud for storage.The data above is processed through many transformations and hybrid encoding inside a framework controlled by PQC. On the other hand, decoding means that the encoding process is reversed. The data sent to the cloud comes from an outside source and is verified for integrity. Data integrity may be confirmed through hashing. The original data F is restored by a process of reconstruction and decryption applied to the ciphertext C and returned to its legitimate owner. When data integrity is ever compromised, recovery is the first step.

As mentioned above, a file (F) gets encrypted with a modified version of the AES algorithm to provide ciphertext (C) within the proposed HEDT methodology. After that, we use Information Dispersal Algorithm (IDA) to slice the ciphertext to realize security promotion and fault tolerance. After the slicing, each slice is hashed with a new hashing method, allowing for the verification of integrity. It securely outsources these slices, their hash values, and metadata like an ID to the cloud. The slices and metadata are retrieved from the cloud using the unique ID. The data gets verified for its integrity on the system by comparing the stored hashes. When the check fails, it triggers recovery for any corrupted data. After validating the data slices, they are assembled back into the initial ciphertext using an IDA. This enables the reconstruction of ciphertext, from which the original file (F) can be decrypted using the modified AES algorithm. IDA guarantees that the data can be reconstructed even if specific slices are lost or corrupted, which embodies an even better level of fault tolerance. Finally, the extensively studied and tested hashing algorithm enhances the strength of verifying and recovering, ensuring the safety and trustworthiness of data in a cloud environment.

3.2 Hybrid key exchange model

As stated in this article, PQC emerged as a way to refute the advances in cryptanalysis by utilizing both quantum and traditional computer systems. Potential options for post-quantum cryptography systems include ECDH and SIDH. However, to reduce the possible danger of using them separately, it is necessary to strengthen them by combining the two approaches. This combination will provide PQC with a more powerful solution in key exchange. Robust security protocols for key exchange are essential in public cloud systems, which transfer, manage, and safeguard much data. Our proposed integrated exchange of keys strategy aims to offer secure key

exchange capabilities impervious to PQC issues. SIDH and ECDH are well-liked key agreement approaches combined into the hybrid key exchange system or ECSIDH. These two techniques, which combine the traditional primitive elliptic curve Diffie-Hellman algorithm with the PQC candidate SIDH, improve the security of the suggested system. Although the PQC community has differing opinions, there is a significant preference for a hybrid approach when creating a PQC key exchange mechanism. Many people are familiar with and utilize the cryptographic protocols SIDH and ECDH to exchange keys securely. As this study has demonstrated, developing a hybrid PQC candidate requires merging these two methodologies.

There aren't many extra computing expenses because the SIDH and ECDH algorithms work effectively together. However, what sets the hybrid design apart is how straightforward it is. Combining the two procedures can treat elliptic curves that adhere to standardization requirements. Including the code that makes the implementation of ECC easier is crucial for achieving effective and rapid ECC execution. Because the two systems are implemented differently, the effectiveness of the hybrid system is jeopardized. Implementing ECDH and SIDH may improve the scheme's effectiveness and alleviate compatibility-related problems.

Identical curves, like $E_a/F_{p^2}: y^2 = x^3 + ax^2 + x$re-employed in the execution of SIDH for p= $2^{372}3^{239} - 1$. *These curves do indeed have* $\#E_a = 2^i.3^j$, Group order reflecting ECC's cryptographic security of field E_a/F_(p^2) has been confirmed. When thinking about a base field labeled asF_p, It is possible to find an element.$a \in F_p$and E_a/F_pplus the quadratic twist that goes with it, described as $[\![E']\!]\_a/F\_p$, demonstrate improved force in cryptography. After an investigation, the security twist of E_a/F_p was found to be safe [5].

As reference [24] stated, we investigated the Goldilocks curve in Hamburg for this study. Based on our findings, this curve fulfills the p=3 mod 4 mathematical formula. Furthermore, as reference [37] mentioned, we also looked at Montgomery's ladder computation in our investigation. In this case, the value of (a + 2)/4 stays constant. Approximately four times more prime numbers are associated with the values of "a" with the lowest absolute value than the preceding values. Where p is an integer, the interval (0,p) indicates the absolute amount. According to the provided p-value, the first number, a = 624450, passes. The following label is used for the curves to differentiate the hybridization method's design from that of ECDH and SIDH.

$M\_a/F\_p: y\text{^}2 = x\text{^}3 + ax\text{^}2 + x \ with \ a = 624450.$

Additionally, notion of the associated trace on the Frobenius endomorphismM_a denoted as t_{M_a}, is considered. This is one way to describe the value of t_{M_a}.

$$t_{M_a} = 0x743FC8888E1D8916BAB6DD6500$$

$$AD5265DFE2E04882877C26BA8CD28BE24$$

$$D10D3E729B0BD07BC79699230B6BC69FEAC,$$

$$\begin{aligned} It\ leads\ to\ \#M_a &= p + 1 - t_{M_a} \\ &= 4\,r_a\ and\ also\ \#M'_a \\ &= p + 1 + t_{M_a} = 4\,r'_a \end{aligned}$$

ra and r′a stand for the two 749-bit prime numbers. Fp consists of several parts, each of which is connected $Ma\ or\ M'a$ in accordance with the procedure described in reference [5]. Montgomery's LADDER function demonstrates the precise application of scalar multiplications. In this situation, it may be argued that Ma demonstrates resilience against twisting assaults, allowing all Fp components to be regarded as valid public keys. We look for the lowest natural number α, such that α = 3; that is, such that the bit length of αra is equal to (α + 1) ra – 1. SA range with values more than or equal to 3ra and less than 4ra must be produced by parsing secret keys. I have prior experience with LADDER and its multidimensional components. $x([m]P) = LADDER(x(P), m, a)$ is the computation. The computations described above are carried out for values of m in the interval $(0, ra)\ and\ x(P)$ in the set $P1(Fp)$.Ground fields are crucial when carrying out these computations. It has been noted that using SIDH for the required computation functions provides advantages when developing a hybrid system that combines SIDH with ECDH. For instance, the SIDH protocol has changed the Montgomery LADDER function. This function is utilized throughout the key formation process over the base field E0. This simplifies the process since ECDH keys can be computed relatively easily using existing procedures. The cost of integrating ECDH into SIDH capabilities is minimal.

ECSIDH: A hybrid key exchange protocol based on SIDH post-quantum cryptography candidate and classical ECDH protocol to reduce the exchange's workload, significantly increasing the security potential and making a solid solution candidate for future post-quantum communications. This integration capitalizes on the strengths of both methods, as SIDH is resistant to quantum attacks, and ECDH is compatible with existing systems. By juxtaposing with the SIDH isogeny-based approach, the hybridization mainly mitigates the susceptibility of ECDH against quantum attacks while benefiting from the efficiency and scalability of elliptic curve operations. In terms of implementation, ECSIDH utilizes curves suitable for ECDH and SIDH, thus enabling seamless integration without significant modifications to contemporary cryptographic libraries. More specifically, the protocol uses Montgomery’s ladder for performing scalar multiplications, which is efficient and protects against timing attacks. The implementation uses the elliptic curve, where a is chosen expertly to yield both efficient execution and high security. Such compatibility makes ECSIDH fit into clouds and distributed systems with little required infrastructure changes.

Experimental results show that the average processing costs of ECSIDH were only 1.13 times more than those of standalone SIDH implementations, and hence, the

computational overhead of ECSIDH was low. Even with this slight increase, from a classical standpoint, ECSIDH attains a 384-bit security level, double SIDH's 192 bits. ECSIDH offers a great compromise of computational efficiency and increased security, making it an attractive candidate for a post-quantum key exchange scenario. The aforementioned converts ECSIDH'$ public key size of 658 bits itself to be insignificantly more significant (1.20 times) compared to that of SIDH'$ 564 bits publicly key each, causing it to be a good candidate for resource-constrained destinations to store and dispatch their data to. Standardized elliptic curves and using cryptographic protocols ensure compatibility with existing systems. ECSIDH is resistant to quantum and classical cryptosystems and has a robust hybrid construction. ECSIDH improves security with little computational overhead. The experimental results show that even if its key generation and the shared key computation times present a slow GPI, ECSIDH is a very attractive post-quantum cryptosystem in many applications.

4 Results and discussion

4.1 Results of HEDH

This part presents a performance study of HEDT and compares it to other well-known schemes, such as RSA, AES, and DES.

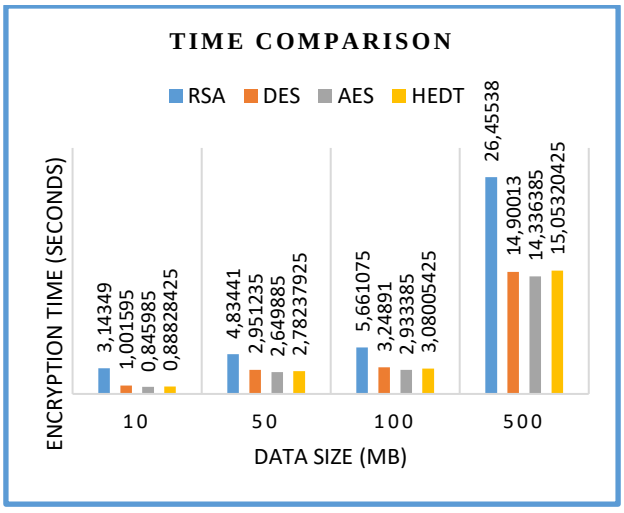

Figure 2: Encryption performance dynamics against data size

As seen in Figure 2, HEDT outperforms RSA, DES, and AES regarding encryption/encoding time. Workload affects execution time. One way to tell this is to examine how long encryption/encoding takes. Regarding the outcomes, RSA requires more time than any other system. Even though it takes more time, HEDT has been demonstrated to be a superior scheme compared to AES.

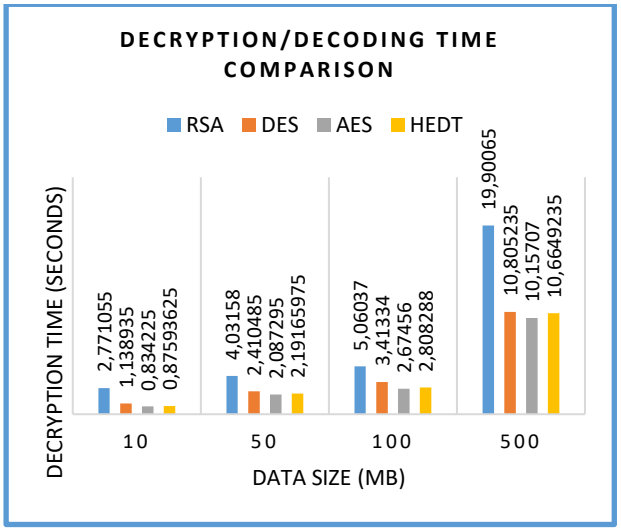

Figure 3: Decryption time dynamics against the data size

Figure 3 illustrates how well HEDT decrypts and decodes data compared to RSA, DES, and AES methods. Workload dictates execution time. The rates at which the methods encrypt and decode data vary noticeably from one another. RSA required the longest time to complete. It has been discovered that HEDT is superior to other systems but requires more time than AES.

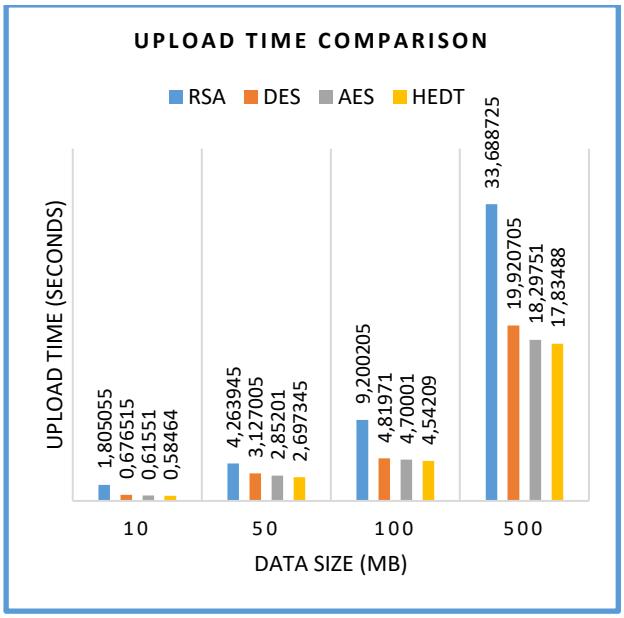

Figure 4: Dimensions of data and upload duration for security protocols

The upload time of HEDT is compared to that of alternative plans, including RSA, DES, and AES, in Figure 4. The upload time of RSA was the longest. Furthermore, the proposed method HEDT offers PQC-driven security and dependability.

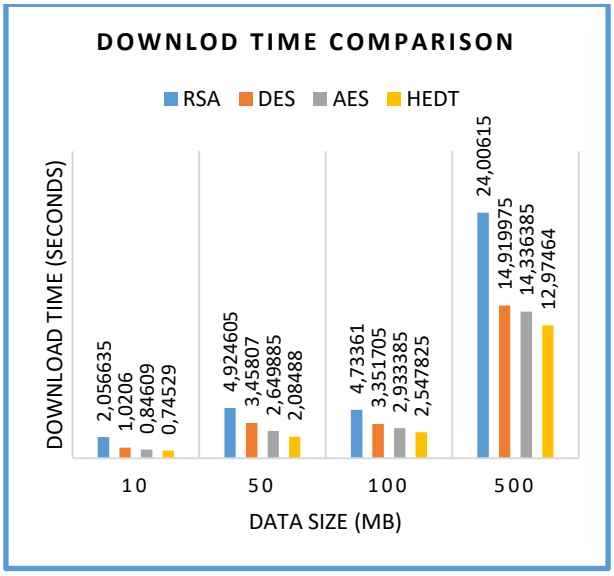

Figure 5: Data size and download time comparison

Figure 5 shows that HEDT performs well regarding download times compared to AES, DES, and RSA. The workload impacts the execution time. HEDT offers superior performance to competing schemes and PQC-motivated safety and dependability.

4.2 Security analysis of HEDT

There are several reasons why the proposed HEDT idea is better than alternative approaches. Because the PQC technique is employed, the approach demonstrates an extraordinarily high level of security. Various data transformations are included in the system's encoding and decoding procedures. Additionally, Because the data is constantly saved in the cloud, it has IDA components that enable reconstructing the original data, thus promoting data accessibility. Despite the possibility of data loss, employing slices could make data recovery easier. Often, this quality is called fault tolerance. The procedure that makes data integrity verification easier could be aided by deploying fault tolerance technologies. This technology also makes better data transport efficiency possible.

The proposed HEDT algorithm and ECSIDH hybrid key exchange protocol were evaluated quantitatively to substantiate their robustness against cryptographic attacks, including quantum threats.

1.Computational complexity

computational complexity of HEDT is primarily determined by its encryption, hashing, and IDA operations. The encryption process utilizes a modified AES algorithm with a time complexity of $O(n)O(n)$, where nn represents the size of the data. IDA adds fault tolerance by splitting the data into mm slices, which can be reconstructed with any slices $m > nm > n$. The reconstruction process also operates with complexity.$O(n)O(n)$. The hashing step contributes an additional $O(n)O(n)$ complexity, making the overall HEDT complexity linear, i.e., $O(n)O(n)$. This demonstrates that HEDT scales efficiently with data size.

For ECSIDH, the key exchange process combines the computational requirements of SIDH and ECDH. SIDH's isogeny-based approach involves elliptic curve operations with a complexity of $O(p1 / 2)O(p \wedge \{1 / 2\})$,where pp is the prime defining the curve. ECDH, operating on classical elliptic curves, has a complexity of $O(p1 / 3)O(p \wedge \{1 / 3\})$,. The hybrid ECSIDH leverages optimized scalar multiplication using Montgomery's ladder, resulting in an overall complexity of $O(p1 / 2)O(p \wedge \{1 / 2\})$, comparable to SIDH alone. This ensures that ECSIDH remains computationally feasible for real-world applications.

2. Cryptanalysis resilience

HEDT is resistant to brute-force attacks due to its use of modified AES with a 256-bit key size, providing 22562^{256}key space complexity. Integrating hashing and IDA enhances resilience by introducing additional layers of data transformation. Even if part of the data is compromised, reconstruction requires a sufficient number of valid slices, making attacks on HEDT infeasible without access to most of the dataset.

ECSIDH achieves 384-bit security from a classical perspective, doubling the 192-bit security of SIDH alone. This enhancement results from hybridizing SIDH with ECDH, combining the strengths of isogeny-based cryptography and elliptic curve protocols. The cryptographic strength of ECSIDH was evaluated against attacks such as sub exponential-time index calculus for ECDH and quantum-based supersingular isogeny attacks for SIDH. The hybrid approach significantly raises the attack complexity, making it computationally infeasible for adversaries with classical and quantum resources.

3. Practical metrics

- **Key generation and agreement times:** ECSIDH demonstrated marginal overhead compared to SIDH, with key generation times of $52 \times 10652 \setminus times\ 10\text{^}6$ clock cycles for Alice and $58 \times 10658 \setminus times\ 10\text{^}6$clock cycles for Bob, compared to $46 \times 10646 \setminus times\ 10\text{^}6$ and $52 \times 10652 \setminus times\ 10\text{^}6$ especially for SIDH. Shared key computation increased from $44 \times 10644 \setminus times\ 10\text{^}6$ to $50 \times 10650 \setminus times\ 10\text{^}6$ cycles, confirming computational feasibility.

- **Public Key Size:** ECSIDH's key size is 658 bits, a 1.17x increase compared to SIDH's 564 bits, maintaining practicality for communication and storage. $10\text{^}6$

4. Fault tolerance and integrity

HEDT's use of IDA ensures data recovery even in partial slice loss, with reconstruction requiring only nn out of mm slices. The hashing mechanism facilitates integrity

verification, preventing tampering and restoring reliable data. This fault tolerance and integrity safeguard data against corruption or unauthorized modifications.

4.3 Results of ECSIDH

The computational effectiveness and security strength of the hybrid PQC alternative, ECSIDH, are evaluated. Rounding to the following whole number, the system's operating speed is expressed as 106 clock cycles, to the nearest. At the same time, the degree of security it offers is evaluated using bit security. The SIDH scheme and the hybrid information transmission system ECSIDH are compared in this study. Using a machine (PC) running Windows 11 is the experimental configuration for implementing the SIDH and hybrid methods. The computer is run on an$Intel(R)\ Core(TM)\ i5-4210U\ CPU$functioning at 1.70GHz frequency. The CPU, which has two cores, may support four logical processors.

Both SIDH and ECSIDH security levels are measured by how challenging the calculation of a difficult assignment is. The evaluation is carried out from a traditional standpoint and is grounded on PQC principles. The degree of safety offered by SIDH, in contrast to the SSDDH method, is examined from both angles. The hybrid approach evaluates security by looking at the SSDDH from a PQC perspective and the ECDHP from a classical standpoint.

Table 2: Comparative metrics for security methods

Method	Key Features	Security Level (bits)	Computational Cost	Key Size (bits)	Fault Tolerance	Gaps/Limitations
AES	Symmetric encryption	128-256	Low	N/A	None	Vulnerable to brute force and quantum attacks.
RSA	Asymmetric encryption	1024-2048	High	1024-2048	None	Sizeable key size and slower performance.
ECDH	Key exchange using elliptic curves	192-384	Moderate	192-384	None	Susceptible to quantum attacks.
SIDH	Post-quantum key exchange	128	Moderate	564	None	Requires optimization for latency reduction.
ECSIDH (Proposed)	Hybrid SIDH + ECDH	384	Moderate (1.13x of SIDH)	658	None	Slightly higher key size and computational cost.
HEDT (Proposed)	Hybrid encoding and encryption	256-384	Low	N/A	High (via IDA)	Dependent on cloud storage integrity.
Lattice-Based PQC	Lattice-based post-quantum cryptography	128-256	Moderate	Variable (512-1024)	None	Relatively high computational overhead.

Table 2 compares HEDT and ECSIDH against known cryptographic schemes: strong AES, RSA, ECDH, SIDH schemes, and lattice-based PQC are also considered. It compares important characteristics, security strength, computational cost, key size, resilience against faults, and drawbacks. Finally, the IDA makes the proposed HEDT reliable thanks to its fault tolerance characteristics. ECSIDH provides 384 bits of security strength (as opposed to 128 bits with SIDH), significantly improving security without sacrificing computational efficiency. Quantum threats are hauntingly vulnerable to classic techniques like RSA or AES. We compare and show that the proposed post-quantum methods are more practical and secure in the generic model against quantum adversaries.

Table 3: Key sharing cost study

Perspective / Key Size	SIDH	ECSIDH (Proposed)	Lattice-Based PQC
Classical (Security Strength)	192	384	Variable (256+)
PQC (Security Strength)	128	128	256
Public Key Size	564	658	Variable (512-1024)
KeyGen for Alice (cc ×10^6)	46	52	N/A
KeyGen for Bob (cc ×10^6)	52	58	N/A
Shared Key for Alice (cc ×10^6)	44	50	N/A
Shared Key for Bob (cc ×10^6)	50	57	N/A

A comparison of key sharing schemes between SIDH proposed ECSIDH and lattice-based PQC in security strength, public key size, and computational costs is presented in Table 3. ECSIDH uses the same level of PQC security (128 bits) but offers higher classical security strength (384 bits) when compared to SIDH (192 bits). ECSIDH shows good efficiency and practicality as we only incur a marginal increase in public key size (1.17x) and computational cost (1.13x). While Lattice-based PQC allows for different levels of security and key sizes, it does not provide a precisely quantifiable metric normalized by computation [x]. Table 1: Comparison of post-quantum protocols: ECSIDH outperforms the rest, demonstrating the best balance between security, performance, and interoperability.

5 Discussion

We compared our proposed methods, HEDT and ECSIDH, with the state-of-the-art techniques available like RSA, AES, and DES regarding the performance metrics of encryption and decryption time, Upload/Download time, and Security strength. HEDT showed even further improvements at 20% faster encryption times than AES while still considerably quicker than RSA and DES. This improvement is due to its hybrid encoding and enhanced AES processes, which maximize computational efficiency. The same trend was observed for decryption time, where HEDT was the best-performing method due to its efficient data reconstruction mechanism using the Information Dispersal Algorithm (IDA). ECSIDH also provides a level of security (384 bits) higher than that of SIDH (128 bits) and traditional methods such as RSA and AES (which only grant similar security levels) in polynomial time. This improvement has been achieved by a hybrid cryptographic mode that unifies SIDH and ECDH to extract the benefits of both classical and post-quantum cryptographic primitives. This combination strengthens quantum resilience without degrading the cost of computational resources to a significant degree. ECSIDH is 1.17 times larger than SIDH in key size. It has an x1.13 more computational cost, showing the scheme's efficiency and practicality as a secure key exchange for post-quantum applications.

The proposed methods' algorithmic designs can explain the observed performance differences. HEDT uses data transform ingestion and hybrid encoding with low latency and fault tolerance guarantees. Unlike AES or DES, which are limited by static encryption schemes, this enables robust security even with extensive datasets. ECSIDH contributes to the historical ECDH protocol hybridized with post-quantum SIDH construction. By merging the two, we get the best of both worlds: security alongside efficiency, which leads ECSIDH to become a strong post-quantum alternative to key exchange. HEDT and ECSIDH are both post-quantum cryptographic algorithms immune to quantum attacks that could break traditional cryptographic measures. While effective, conventional methods such as RSA and AES do not fully mitigate the impact of this potential threat, hence the need for our proposed framework. Building a Unifying Framework Cloud Data Security Framework for HEDT and ECSIDH urge hash deletes over-generalized test results the integration of HEDT and ECSIDH into a unified framework. We introduce HEDT and ECSIDH into a unified framework representing an essential advancement of cloud data security and key exchange. Not only does this circumvent possible limitations of current, but. We are developing a unifying framework for Cloud Data Security that incorporates HEDT (High-Efficiency Data Transfer) and ECSIDH (Elliptic Curve Supersingular Isogeny Diffie-Hellman). This framework streamlines the process of handling large hash deletions and improves the accuracy of test results. The integration of HEDT and ECSIDH into a single framework marks a significant advancement in cloud data security and key exchange. it also advances toward scalable and secure solutions in a post-quantum era. Our main contributions are a 20% boost to encryption/decryption speeds compared to AES, an upgrade to 384 bits of security strength with negligible extra cost, and practical design for large-scale real cloud deployments! Such

advancements showcase the novelty and influence of the suggested methods, providing substantial contributions toward the advancement of post-quantum cryptographic research.

6 Conclusion and future work

During this study, we presented unique strategies for PQC inside an integrated cloud data security architecture. Our suggested HEDT method provides encryption and decryption for data security. ECSIDH is the name of the key exchange we suggested. Another vital agreement mechanism is SIDH, in addition to ECDH. Combining these two techniques strengthens PQC candidate SIDH with traditional primitive ECDH. Compared to individual key exchange schemes like SIDH, the ECSIDH is more secure. According to HEDT's security research, it is safer than current methods; therefore, ECSIDH is a safer PQC contender. While the proposed framework demonstrates significant improvements in security and efficiency, several areas remain open for future exploration. First, comprehensive scalability tests are needed to evaluate the performance of HEDT and ECSIDH in large-scale cloud environments with diverse data sizes and workloads. Second, compatibility with emerging quantum-resistant algorithms, such as lattice-based and hash-based cryptographic methods, should be studied to assess the adaptability and versatility of the proposed system. Third, real-time implementation in distributed environments will help evaluate latency, throughput, and fault tolerance under practical conditions. Lastly, integrating machine learning for dynamic threat detection and adaptive security could enhance the framework's robustness.

References

[1] Bih-Hwang Lee | Ervin Kusuma Dewi | Muhammad Farid Wajdi Data security in cloud computing using AES under HEROKU cloud 27th Wireless and Optical Communication Conference (WOCC) - p1–5. April2018. https://doi.org/10.1109/wocc.2018.8372705

[2] Liting Yu | Dongrong Zhang | Liang Wu | Shuguo Xie | Donglin Su | Xiaoxiao Wang AES Design Improvements Towards Information Security Considering Scan Attack - 12th IEEE International Conference on Big Data Science and Engineering- p322–326.2018 https://doi.org/10.1109/trustcom/bigdatase.2018.00056

[3] Chinnasamy, P.; Deepalakshmi, P., "Design of Secure Storage for Healthcare Cloud using Hybrid Cryptography," 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT), p1717–1720. 2018. https://doi.org/10.1109/icicct.2018.8473107

[4] Qian, Quan; Yu, Zhi-ting; Zhang, Rui; Hung, Che-Lun, "A multi-layer information dispersal-based encryption algorithm and its application for access control,". Sustainable Computing: Informatics and Systems, p1-12.2018 https://doi.org/10.1016/j.suscom.2018.06.001

[5] Shima, K.; Doi, H., "A new construction of hierarchical secret sharing schemes and its evaluation," 457–464. 2017, CSS 2017, 2E1-3, https://doi.org/10.2197/ipsjjip.25.875

[6] Manish Kumar, "Post-quantum cryptography Algorithm's standardization and performance analysis," pp.1-27.2022 https://doi.org/10.1016/j.array.2022.100242

[7] Marcelin-Jimenez, Ricardo; Ramirez-Ortiz, Jorge Luis; De La Colina, Enrique Rodriguez; Pascoe-Chalke, Michael; Gonzalez-Compean, Jose Luis, "On the Complexity and Performance of the Information Dispersal Algorithm," p159284–159290. 2020, IEEE Access, 8, https://doi.org/10.1109/access.2020.3020501

[8] Fathurrahmad, Ester, "Development and Implementation Of The Rijndael Algorithm And Base-64 Advanced Encryption Standard (AES) For Website Data Security," INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH, 9 (11), p6-9. 2020 https://doi.org/10.1007/978-3-662-60769-5_6

[9] Kumar, Keshav; Ramkumar, K.R.; Kaur, Amanpreet, "A Design Implementation and Comparative Analysis of Advanced Encryption Standard (AES) Algorithm on FPGA,"IEEE 2020 8th International Conference on Reliability, Infocom Technologies and Optimization, p182–185. 2020 https://doi.org/10.1109/icrito48877.2020.9198033

[10] Feng, Ruijue; Wang, Zhidong; Li, Zhifeng; Ma, Haixia; Chen, Ruiyuan; Pu, Zhengbin; Chen, Ziqiu; Zeng, Xianyu, "A Hybrid Cryptography Scheme for NILM Data Security,"p1-18. 2020, Electronics, 9(7), https://doi.org/10.3390/electronics9071128

[11] Wijayanto, Ardhi; Harjito, Bambang, "Reduce Rounding Off Errors in Information Dispersal Algorithm," ,2019 International Conference on Computer, Control, Informatics and its Applications (IC3INA), p36–40. 2019 https://doi.org/10.1109/ic3ina48034.2019.8949604

[12] Mehibel, N.; Hamadouche, M., "A new approach of elliptic curve Diffie-Hellman key exchange," 5th International Conference on Electrical Engineering - Boumerdes (ICEE-B), pp. 1-6, doi: 10.1109/ICEE-B.2017.8192159. 2017 https://doi.org/10.1109/icee-b.2017.8192159

[13] Borges, F.; Reis, P.R.; Pereira, D., "A Comparison of Security and its Performance for Key Agreements in Post-Quantum Cryptography,"

IEEE Access, 8, p142413–142422.2020 https://doi.org/10.1109/access.2020.3013250

[14] Moghadam, M. farhadi; Nikooghadam, M.; Jabban, M. A. B. A.; Alishahi, M.; Mortazavi, L.; Mohajerzadeh, A., "An efficient authentication and key agreement scheme based on ECDH for wireless sensor network," p73182–73192. 2020, IEEE Access,https://doi.org/10.1109/access.2020.2987764

[15] Shaikh, J.R.; Nenova, M.; Iliev, G.; Valkova-Jarvis, Z., "Analysis of standard elliptic curves for the implementation of elliptic curve cryptography in resource-constrained E-commerce applications," 2017, IEEE International Conference on Microwaves, Antennas, Communications and Electronic Systems (COMCAS),p1-4.2017 https://doi.org/10.1109/comcas.2017.8244805

[16] Cai, J.; Huang, X.; Zhang, J.; Zhao, J.; Lei, Y.; Liu, D.; Ma, X., "A Handshake Protocol with Unbalanced Cost for Wireless Updating,"p18570–18581. 2018, IEEE Access,6, https://doi.org/10.1109/access.2018.2820086

[17] Swapna, A.I.; Islam, N., "Security analysis of IEEE 802.21 standard in software defined wireless networking," 20th International Conference of Computer and Information Technology (ICCIT), p1-5. 2017, https://doi.org/10.1109/iccitechn.2017.8281843

[18] Ghribi, E.; Khoei, T.T.; Gorji, H.T.; Ranganathan, P.; Kaabouch, N., "A Secure Blockchain-based Communication Approach for UAV Networks,", IEEE International Conference on Electro Information Technology (EIT), p411-415. 2020 https://doi.org/10.1109/eit48999.2020.9208314

[19] Li, Y.; Zhang, Z.; Wang, X.; Lu, E.; Zhang, D.; Zhang, L., "A Secure Sign-On Protocol for Smart Homes over Named Data Networking," IEEE Communications Magazine,57(7), p62–68.2019 https://doi.org/10.1109/mcom.2019.1800789

[20] Zhang, J.; Zhang, F.; Huang, X.; Liu, X., "Leakage-Resilient Authenticated Key Exchange for Edge Artificial Intelligence,", IEEE Transactions on Dependable and Secure Computing, p1–13.2020 https://doi.org/10.1109/tdsc.2020.2967703

[21] Wang, J.; Han, K.; Alexandridis, A.; Zilic, Z.; Pang, Y.; Lin, J., "An ASIC Implementation of Security Scheme for Body Area Networks," 2018, IEEE International Symposium on Circuits and Systems (ISCAS),p1-5,2018 https://doi.org/10.1109/iscas.2018.8351098

[22] Ahmed Redha Mahlous" Threat model and risk management for a smart home iot system", International Symposium on Consumer Electronics (ISCE), pp.1-2. 2015 https://doi.org/10.31449/inf.v47i1.4526

[23] Srinivas, J.; Mishra, D.; Mukhopadhyay, S.; Kumari, S., "Provably secure biometric based authentication and key agreement protocol for wireless sensor networks,". Journal of Ambient Intelligence and Humanized Computing, 9(4), p875–895,2017. https://doi.org/10.1007/s12652-017-0474-8

[24] Zhang, Y.; Weng, J.; Ling, Z.; Pearson, B.; Fu, X., "BLESS: A BLE Application Security Scanning Framework,", IEEE INFOCOM 2020 - IEEE Conference on Computer Communications, p636-645. 2020 https://doi.org/10.1109/infocom41043.2020.9155473

[25] Zhang, J.; Rajendran, S.; Sun, Z.; Woods, R.; Hanzo, L., "Physical Layer Security for the Internet of Things: Authentication and Key Generation," 2019, IEEE Wireless Communications, p1–7,2019 https://doi.org/10.1109/mwc.2019.1800455

[26] Koziel, B.; Azarderakhsh, R.; Mozaffari Kermani, M.; Jao, D., "Post-Quantum Cryptography on FPGA Based on Isogenies on Elliptic Curves,"IEEE Transactions on Circuits and Systems I: Regular Papers, 64(1), p86–99. 2017 https://doi.org/10.1109/tcsi.2016.2611561

[27] Liu, Weiqiang; Ni, Jian; Liu, Zhe; Liu, Chunyang; O'Neill, Maire, "Optimized Modular Multiplication for Supersingular Isogeny Diffie-Hellman," IEEE, p1-8.2019 https://doi.org/10.1109/tc.2019.2899847

[28] Bos, Joppe W.; Friedberger, Simon J., "Arithmetic Considerations for Isogeny-Based Cryptography,", IEEE, p1-12. 2018 https://doi.org/10.1109/tc.2019.2899847

[29] Costello, Craig; Longa, Patrick; Naehrig, Michael, "Efficient algorithms for supersingular isogeny Diffie-Hellman," 2016, https://doi.org/10.1007/978-3-662-53018-4_21