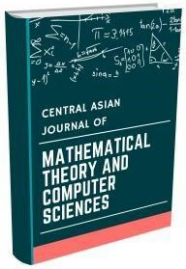

CENTRAL ASIAN JOURNAL OF MATHEMATICAL THEORY AND COMPUTER SCIENCES
https://cajmtcs.centralasianstudies.org/index.php/CAJMTCS
Volume: 07 Issue: 01 | January 2026 ISSN: 2660-5309

Article

Optimized Lattice-Based Digital Signatures for Secure IoT Communication

Zaid Mohammed Mortada[1], Abrar Ali Hasan Al-Ameri[2]

1. Department of Postgraduate Studies, University of Kufa, Najaf, Iraq
2. Faculty of Computer Science and Mathematics, University of Kufa, Najaf, Iraq

* Correspondence: zaidm.alhusaini@uokufa.edu.iq

Abstract: A lightweight, robust, and efficient security mechanism is necessary to combat quantum-generation threats across multiple domains, including healthcare, transportation, and industrial automation, in the Internet of Things (IoT). Post-quantum cryptography has emerged in response to the increasing vulnerability of traditional cryptographic methods, such as RSA and ECC, to quantum attacks. Taking advantage of the hardness of Short Integer Solutions (SIS) and Learning with Errors (LWE), we propose a lattice-based signature scheme for IoT applications. A computationally efficient IoT device model that maintains authenticated, integrity, and anonymity is proposed. The scheme has the advantage of being faster and more efficient than existing key size schemes such as IBS, CLS, and FALCON, according to a detailed security assessment. The proposed scheme maintains practical deployment ability while reducing post-quantum security in IoT ecosystems.

Received: 10th Nov 2025
Revised: 11th Dec 2025
Accepted: 24th Dec 2025
Published: January 26, 2026

Keywords: Lattice-Based Cryptography, Internet of Things (IoT) Security, Post-Quantum Cryptography, Digital Signature Scheme, Short Integer Solution (SIS) Problem.

1. Introduction

A robust, scalable, and quantum-resistant security solution is essential for Internet of Things (IoT) devices such as healthcare and smart grids. While traditional cryptographic schemes are effective against classical attacks, quantum attacks pose significant threats to data integrity, authentication, and device trustworthiness in IoT environments. The Short Integer Solution and Learning with Errors algorithms, which guarantee strong security based on mathematical problems, have been increasingly popular in recent years. The efficiency and parallelism of these schemes make them suitable for constrained environments, not only because they are resistant to quantum adversaries. The Internet of Things (IoT) influences every aspect of people's lives and daily activities. In daily life, we travel, consume, produce, and undergo medical treatment. Smart IoT devices are everywhere today, and the world is becoming increasingly digital and intelligent. There are many security threats associated with Internet of Things devices, which provide

convenience but also pose a threat to people's lives and property. With the development of IoT networks, IoT network security is becoming increasingly important [1].

Public networks require high security for data sharing between IoT devices. A greater emphasis should be placed on data security and user identity privacy when it comes to IoT network applications such as the Internet of Things (IoT) [2], the Home Internet of Things (Home IoT) [3], and the Industrial Internet of Things (IIoT)[3]. Developing drugs, predicting diseases, and creating medical devices all depend on medical data in IoMT systems. For data value to be realized, medical data security and user privacy must be ensured. A home IoT device collects data on how the user lives. This data puts the lives and property of users at risk. Vehicles connected to the Internet of Things collect traffic data, real-time road data, and logistics data in real-time. National security requires information about infrastructure, such as geography and transportation. Using sensors, software, and networks, the Internet of Things consists of a physical network of connected devices. A smart device, also known as a connected device, can be anything from home appliances to wearables to industrial machinery[4]. IoT allows devices to be connected to the Internet for data collection, analysis, and remote control.

Figure 1: The security of IoT networks.

It is a cryptographic technique in which several signers, each possessing their own private-public key pair, sign the same message simultaneously. Security is improved, unauthorized actions are prevented, distributed control is ensured, and accountability is assured by using multi-signature applications. IoT systems are more secure and reliable when they use multiple trusted signatures. A literature review indicates that you can combine traditional public-key cryptographic systems with multi-signature schemes, such as modular exponentiation (RSA), discrete logarithm problem (DLP), and bilinear pairing. Quantum cryptosystems are expected to grow exponentially in the near future, posing major threats to existing public-key cryptosystems. Lattice cryptography techniques have become popular as a means of defending against these threats. Real-world IoT problems can be solved with multi-signature schemes based on lattices [5], and [6]. LBC (Lattice-Based Cryptography) has proven promising since its introduction in recent years as an alternative to public-key cryptosystems. A notable feature of the LBC implementations is that they can perform integer-based linear algebra on matrices and vectors [7]. Their limited resources make them an attractive choice for devices with limited resources, like the Internet of Things. Using a lattice-based secure scheme, [12] envisioned a future smart city with smart healthcare. A lightweight key exchange mechanism was used as well as an authentication mechanism.

2. Related Work

Since lattice-based cryptographic primitives are post-quantum resilient and computationally efficient, their integration into IoT security frameworks has gained considerable attention. The feasibility of lattice-based digital signatures in resource-constrained environments has been explored in several studies, with the goal of balancing security, speed, and memory consumption. The literature presents many mechanisms for authentication, encryption, and signatures. However, these mechanisms are vu Quantum attacks, however, are capable of compromising these mechanisms. Using a lattice-based SIS hard problem, [8] built the first lattice-based algorithm in 1996. Lattice-based signature mechanisms called TESLA have been proposed as an alternative to LWE problems. With the SIS problem in mind, the author proposes an ElGamal-based lattice-based encryption and signature scheme [9]. According to the author [10] We propose an embedded system-specific lattice-based signature framework. Radio Frequency Identification (RFID) authentication protocol relying on NTRU lattices for security. For customer-side networks of the smart grid, an abelian lattice is proposed that preserves privacy. Their design contributes to reducing communication burden and protecting the privacy of users in smart grid environments. Lattices that rely on signatures operate similarly.

Using hard lattice problems as a basis for designing stable cryptographic algorithms, author[11] demonstrated how to design such algorithms. Lattices were adopted for public-key encryption, but Oded Regev wasn't able to propose a scheme that was sufficiently robust and stable until 2005. Using lattices and generalizing parity learning, this method is used. Many fields use lattices, which are n-dimensional vector spaces with periodic point arrangements. Cryptographic algorithms based on lattices are mainly divided into two types: problems with the nearest vector (CVP) and problems with the shortest vector (SVP). Cryptographic builders used in lattice-based algorithms are time-efficient, simple, and provide security proofs even under worst-case conditions [12]. Because these algorithms do not solve complicated problems, they also solve a number of simple quantum resistant problems [13]. There is a high degree of hope for lattice-based cryptography among the post-quantum algorithms. Systems based on blockchain that support the Internet of Things, such as ECDSA [14]. Due to integer factorization and discrete logarithms' simplicity, these algorithms cannot withstand quantum attacks. Several IoT and blockchain-based systems use PQC due to its resistance to quantum attacks. A low-resource IoT environment has high memory and overhead requirements during PQC signatures and verifications. Due to its high performance and wide range of applications, lattice-based cryptography is especially suitable for low-power IoT environments [15]. The use of lattice cryptography to secure and strengthen blockchain transactions has been proposed by a wide range of cryptographic schemes [16]. However, its computational complexity has strained network resources because of its high overhead [17]. Since LBBS schemes are resistant to quantum attacks, they have become a cornerstone of privacy protection for post-quantum blockchains [18]. The complexity of key pairs and signature sizes does not benefit IoT systems with limited resources, even if they provide protection against quantum attacks. To prevent quantum attacks, post-quantum blockchains must be developed secure and efficient. This article presents an overview of lattice-based blind signatures as well as a comparison with LBBS. IoT devices with resource constraints require a post-quantum threat model-resilient architecture to ensure privacy-preserving authentication and anonymized data sharing [19]. A blind signature based on LWE/SIS cannot be used by low-power devices due to the larger keys and the associated arithmetic calculations. Blind-signature architectures overcome these limitations by reducing the burden on the device chain and providing post-quantum security.

3. Proposed Methodology

Suppose n is a major number, and $x = 2nloga, a = poly(n)$, and $H : \{0,1\}^* \rightarrow \{0,1\}^k$. are positive and negative integers, respectively.is a negative integer .Ensures the security of hashes. The Gaussian parameter $s = L\tilde{}\omega(\sqrt{logn})$. is used here along with $L\tilde{} \geq O(\sqrt{nlogq})$,.

1. Setup: n and q, the SIS parameters, are input when the security parameter (SIS parameter) is entered.

The $A_0 \in Z_q^{n\times m}$ matrix follows Lemma 1 because it is a uniformly random $n \times m$ matrix with $||\widetilde{T_{A_0}}|| \leq O(\sqrt{nlogq})$ as its basis. Using the root lattice basis $(,A_0, T_{A_0}]$ you can generate subpublics and privates. $(A_{0,}T_{A_0})$ can be used as a root lattice basis for generating subpublic and private keys.

2. Signatures: In addition to ExtBasis and RandBasis, the following algorithms can be used to generate secret keys:

$$T_{A_i'} \leftarrow RandBasic\left(ExtBasis\left(T_{A_0}, A_i' = A_0\middle|A_i, s\right), s\right) \quad (1)$$

In P-QBN, public-private key pairs $\{(A_i', T_{A_i'}), \ldots, (A_n', T_{A_n'})\}$ are used for signing and verifying transactions, while public-private key pairs are$(Tx.)$ used for transferring funds. By using the public key pair PK, the transaction address $(Tx.)$ can be generated, and by using $\{(A_i', T_{A_i'}), \ldots, (A_n', T_{A_n'})\}$, the transaction can be signed and verified. A user's identity can only be protected if both public and private keys $(T_{A_i'}A_i')$ are used at the same time.

- You should choose Bj if you are $m[j] = 1$; otherwise, do nothing if you are $m[j] = 0$,. Hamming weight $l*$ for message m should be set at.

$$B_m = \left(A_i \middle|\middle|B_{j1}\middle|\middle| \ldots ||B_{j1*}\right)$$

- For the transaction message m, SampleD and Lemma 4 are combined to form the signature $v \in Z_q^{(l^*+1)m}$.

$$v \leftarrow SampleD\left(ExtBasis\left(T_{A_i'}, B_m, s\right), s\right) \quad (2)$$

3. Confirm: and v, are the input transaction message and signature, respectively.

$$B_m v = 0(modq), \left||v|\right| \leq s\sqrt{(l^*+1)m} \quad (3)$$

If the hold is accepted, it is accepted; otherwise, it is refused.

3.1 Correctness

This plan is obviously correct, there is no doubt about it. Assume that n is the security parameter and that lemma 1 and lemma 4 generate the other system parameters. It is also possible to correctly execute ExtBasis, Rand Basis, and SampleD algorithms. Using ExtBasis, one can extend the lattice $A\frac{1}{q}(A')$ basis to a lattice $A\frac{1}{q}(A')$ basis of a larger dimension. With this algorithm, however, there is no guarantee that S and S' are independent. ExtBasis output can be randomized using RandBasis to improve the security of a subsecret key. Using the algorithms SampleD and ExtBasis to generate the signature v will increase its probability of being accepted by the verification algorithm. Consequently, the proposal for a signature scheme is correct.

3.2 Security Proof

Detailed security proofs for the proposed signature scheme are provided in this part.

Theorem 1: With the exception of the probability $\frac{\varepsilon}{l_{q2}}$., P-QBN autograph arrangements are highly unforgeable under adaptively chosen message attacks.

Proof: It is only if Theorem 2 holds that the proposed signature scheme will be safe against such forgeries.

Theorem 2: In the event that adversary A is able to break the proposed scheme through an adaptively selected message attack using q_2 times sign queries, challenger C will be able to solve a SIS example with probability$\frac{\varepsilon}{l_{q2}}$ (l is the length of the transaction message).

Proof: Consider the case where challenger A provides an instance of SIS to challenger C.

$$SIS_{n,}(l+2)m, q, 2s\sqrt{(l+1)m} = (\bar{B}, n, m, l, q, s) \quad (4)$$

Here you will find two $\bar{P} = (\bar{P}_0, \ldots, P)$ and two $\bar{P}_i \in Z_q^{(l^*+1)m}$. Following this, he aims to generate a short vector that satisfies his requirements, v

$$\bar{P}v = 0(modq), ||v|| \leq s\sqrt{(l+1)m} \quad (5)$$

Setup: Message $m^{(1)}, \ldots, m^{(q2)}$. is obtained by challenger C by executing Message A. In cases where $B = \{b|b \in \{0,1\}^{\leq k}\}$, is not the prefix for all $m^{(i)}$, set P is computed.

In [27], p at most l_{q2} is sufficient to compute this type of set in polynomial time. $b \in B$, is randomly selected, and t and $|b|$ are set, respectively, for the hammering weight and the length of the hammer. A public key is generated by C by following the steps below.

$A\frac{1}{q}(C_j)$ and $T_j \in Z_q^{m\times n}$ *here* $C_j \in Z_q^{m\times n}$ *and* $j = t_j, i = 1, 2, \ldots, t.$ *Let* $P = \bar{P}.$ are randomly selected as $|b| - t$ trapdoor lattice and trapdoor basis

$0 < t_1, t_2, \ldots, t_t < |p|$ *and* $p_t = 1$. if $i < |p|$, lets equal here. will appear. Other subscripts are as follows: $A_j\ P_j$. When the $i > |p|$, *let* $P_i = \bar{P}_i$ begins.

In the next step, $(P_i, C_1, \ldots, C_k)$. is used to generate public keys. The game begins when challenger C sends adversary (n, m, q, s, k) parameters and public keys. A list L is maintained by C to store the answers to Sign questions.

In a sign query, the adversary A assumes that the attacker gets the true hash value of $q_{2m^{(1)},\ldots,m^{(q2)}}$. The list L is checked by C to ensure it's fresh; otherwise, the same outcome is returned. A new message's signature can be generated by C. The hash value p can satisfy pseudo-randomness even though it is not the prefix of $m^{(i)}$. Former $|p|$ locations still have a possibility of 1 at $t_1, t_2, \ldots, t_t$.A location of type t' corresponds to a public matrix of type $P_{t'} = C_{t'}$. The lattice $A\frac{1}{q}(P_{t'})$ can therefore be obtained by C. The signature v_i for message $m^{(i)}$ can be generated by C using lattice $A\frac{1}{q}(C_{t'})$ trapdoors. In the end, C sends v_i back to adversary A, and stores $(v_i\ m^{(i)})$ in L.

Based on a simple calculation, there is no probability that location t' will be $1 - (\frac{3}{4})^{|p|}$, or $(\frac{3}{4})^{|b|}$. Assuming p is a short bit string of B, $b||0$ and $b||1$ are not prefixes of $m^{(i)}$. In the case of bit strings p', a prefix m(i0) does not have a prefix b'. Because p is the shortest 2 bit string, and there are only lq 2 bit strings, $log_2 2^{l-|p|}$ *and* $|p| \geq log_2(lgs)$. is the shortest 2 bit string available.There is no shorter 2 bit string than this. Therefore, B contains only bit strings that satisfy $|b| \geq log_2(lgs)$. $(\frac{3}{4})^{|b|}$ has a negligible probability compared to $(\frac{3}{4})^{|b|} \leq (\frac{3}{4})^{log_2(lgs)}$. If p is randomly selected with the prefix of message M, it has a probability of being $\frac{1}{lq_2}$. SIS can be solved by C with a high probability $\frac{1}{lq_2(1-(\frac{3}{4})^{log_2(lgs)}} \approx \frac{1}{lq_2}$. Probability is high.

3.3 Efficiency Comparison

Comparing the efficiency of parameters in this paper with those in similar literature is recommended. Based on equations (2) and (5) in the sign phase, the proposed scheme's signature size is not 2mlogq+l, which should be mlogq. Combining double signatures with SampleD and SamplePre results in an inefficient and complex signature. Public and private keys of the proposed signature scheme are significantly smaller than those of bonsai tree signatures [20]. It is also possible to enhance key generation efficiency by using this method as well as eliminate redundancy in wallets by using this method. Signature schemes based on lattices are both secure and easy to implement in P-QBNs.

3.4 Signature Schemes Based on Lattices

The following subset summarizes what we studied in this paper: signature schemes. TESLA and BLISS are described in the GLP scheme[21].

The problem is formalized in Appendix A2 and consists of three types of signature schemes: Learning rings with errors, ring short integers, and decisional compact knapsacks.

1. GLP: Public keys are tuples of $a \leftarrow \$\, R_q$ and $b = as + e\,(mod\ q)$., with coefficients in $\{-1, 0, 1\}$;, whereas secret keys are polynomials $s, e \leftarrow \$\, R_q$, [1] with ternary coefficients. Input μ is sampled first using $y_1, y_2 \leftarrow \$\, R_q, [k]$. by the sign algorithm. After that, we havehed together the most significant bits in $y_1 + y_2$ with μ.A signature polynomial z_1 is computed along with a signature polynomial z_1. z_2 is compressed to z_1 in order to conceal the secret.Consequently, only some signatures will be returned (see [21] for more information). z_1 and z_2 are checked during verification for size, as well as $H\big([az_1 + z_2^* - bc]_{d,q}, \mu\big)$. and c for equality. According to Güneysu et al.[21] GLP-Set-I for 512 and 8383489 parameters is used. There is a minimum hardness of 80 bits in this instance of the DCK [22].
2. Ring-TESLA: An$a_1, a_2 \leftarrow \$\, R_q, b_1 = a_1 s + e_1\,(mod\ q), and\ b_2 = a_2 s + e_2\,(mod\ q)$. Polynomial. Public key $\boldsymbol{vk}$ contains three polynomials with large coefficients, while secret key sk contains three polynomials with small coefficients. Randomly sampling $\leftarrow \$\, R_q$,[B] during message signing. By comparing $a_1 y$ and $a_2 y$ most significant bits, $c \in \mathbb{B}n, \omega$. encodes the polynomial. To verify the signature, we check $H\big([a_1 z - b_1 c]_{d,q}, [a_2 z - b_2 c]_{d,q}, \mu\big)$ against c', which encodes the polynomial of (c', z),.
3. The parameters n = 512 and q = 39960577 were used in Akleylek et al. [28] to achieve 128-bit hardness. Ring-TESLA is not the only TESLA scheme that has a great deal of influence; standard-lattice-based TESLA also has a great deal of influence.
4. BLISS: An NTRU-like key pair $vk = (a_1,\ a_2) = \Big(2\frac{2g+1}{f}(mod\ q), q - 2,\Big) where\ f, g \leftarrow \$\, F_{d1,d2} = \{\sum_{i=1}^{n-1} h_i, x^i\,|h_i \in \{-2, -1, 0, 1, 2\}, |\{h_i = \pm 1\}| = d_1, |\{h_i = \pm 2\}| = d_2\}$ and f are invertible modulo Q, is chosen. $= (s_1, s_2)^T = (f, 2g + 1)^T$ a secret key s_k begins with this element. Furthermore, $(a_1,\ a_2)(s_1, s_2)^T$ is chosen so that it is a mod 2q vector, and $\xi \in Z$ is a mod 2q vector. A message is signed by sampling random vectors y_1 and y_1 using Gaussian distribution.Randomness, public key, message, and public key are combined to compute hash value c. By applying rejection sampling to z_2, $z_1 = y_1 + (-1)^b s_1 c\ and\ z_2 = y_2 + (-1)^b s_2 c$ is computed, and $Z_2 Y_2$ is compressed into Z_P.

It should also be noted that is zero in BLISS-I and BLISS-II .Therefore, the following is true

$$:s_{j,i} \in \begin{cases} \{-1,0,1\} & if\ j = 1 \\ \{-1,1,3\} & if\ j = 2, i = 0, \\ \{-2,0,2\} & if\ j = 2, i \in \{1, \dots, n, -1\}, \end{cases}$$

In which $s_1 = \sum_{i=0}^{n} s_{1,i} x^i and\ s_2 = \sum_{i=0}^{n} s_{2,i} x^i$. Occurs.

4. Result and Discussion

IoT signature schemes are compared in Figure 2 based on their running times (in microseconds). A lattice-based signature scheme outperforms the other models with a running time of just 400 seconds, significantly faster than IBS (1200 seconds), CLS (900 seconds), and CL-DVAAS (770 seconds). In comparison with efficient post-quantum schemes like FALCON (600 s) and BSDH (650 s), the proposed model shows marked improvements, highlighting its suitability for environments with limited resources and time.

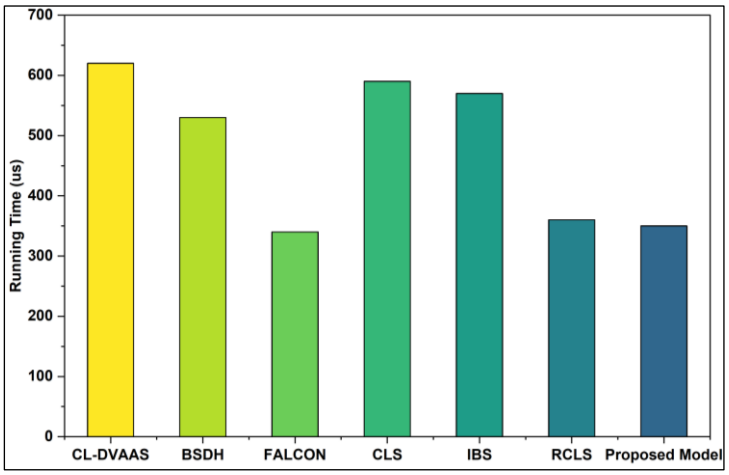

Figure 2: Comparison of IoT Application Running Time (s) Across Signature Schemes.

In Figure 3, the running times for various signature schemes are compared in microseconds (s), illustrating their computational efficiency. FALCON is the fastest of the listed models, with 340 s, followed by 350 s for the Proposed Model, and 360 s for RCLS. In contrast, traditional schemes such as CL-DVAAS (620 s), CLS (590 s), and IBS (570 s) have a higher latency. Based on these findings, IoT environments that are resource-constrained and time-sensitive can benefit from the Proposed Model.

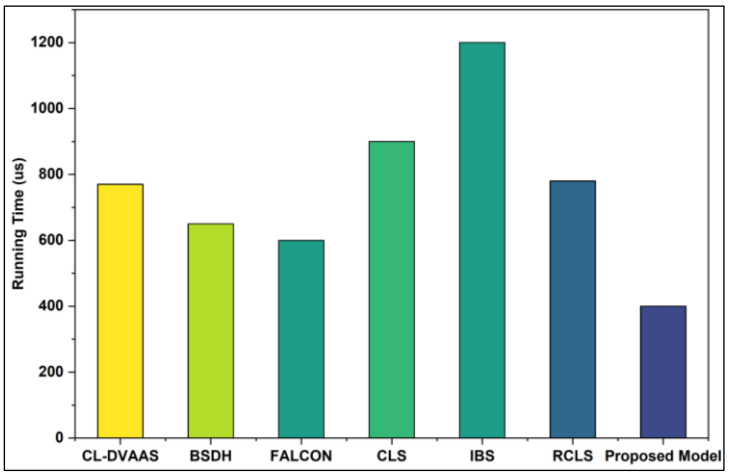

Figure 3: Comparison of running times for IoT signature schemes.

As shown in Figure 4, the size of the message is positively correlated with the time it takes to process the message in microseconds (s). A message size of 0 bits requires 0.19 seconds to process, whereas a message size of 1000 bits requires 0.68 seconds to process. In IoT environments, it is critical to evaluate the scalability and responsiveness of signature schemes. There is a clear trend toward higher latency for larger messages.

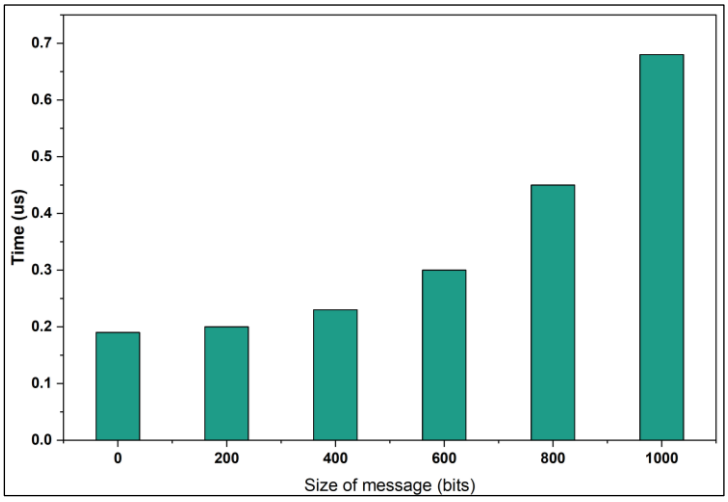

Figure 4: An IoT Signature Scheme that compares message size with processing time (s).

An illustration of the relationship between message size and processing time in microseconds (s) is shown in figure 5. The 400-bit message displays a noticeable spike at 0.5 s, deviating from the otherwise consistent trend of increasing message size with message size. There may be a potential inefficiency or overhead at that specific size, warranting further investigation for performance optimization in IoT signature schemes.

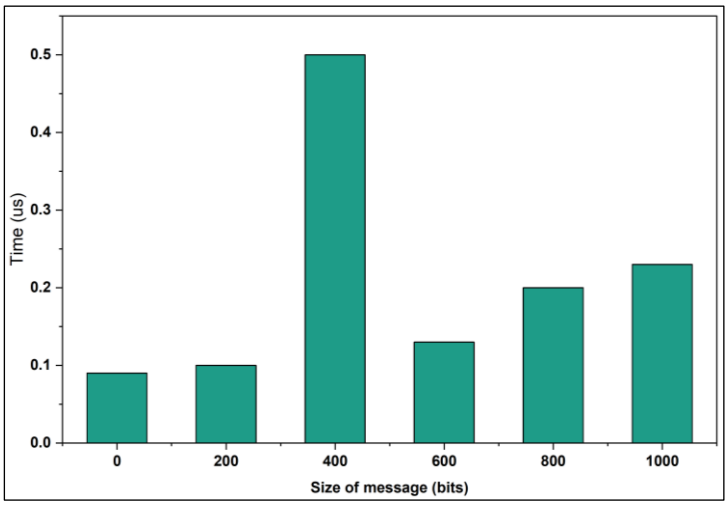

Figure 5: In IoT Signature Schemes (s), processing time varies with message size.

Various signature schemes are compared in figure 6 according to their communication cost in bits, relevant to IoT applications. CLS and IBS have the lowest costs among the models, with 1310 bits and 1350 bits, respectively. BSDH (1530 bits) and FALCON (1460 bits) are closely followed by the Proposed Model at 1400 bits. In IoT environments with bandwidth constraints, the proposed model achieves a favorable balance between security and communication efficiency.

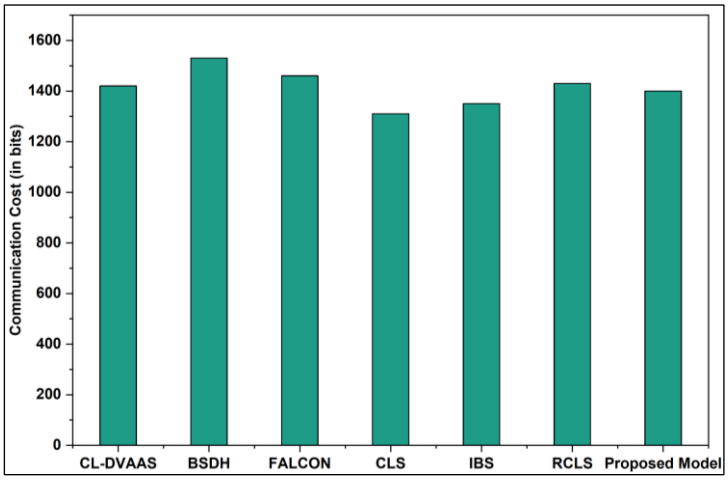

Figure 6: A comparison of the communication costs associated with IoT signature schemes (bits).

5. Conclusion

Using a lattice-based signature scheme, we address the growing concern about quantum vulnerabilities in traditional cryptography in this paper. In the case of adaptive chosen-message attacks, the scheme makes use of the mathematical hardness of lattice problems to ensure high unforgeability. Compared with existing lattice-based and classical signature mechanisms, the proposed method is faster and more efficient at generating keys. We propose a scheme that reduces signature size, improves speed, and provides strong resistance to quantum attacks in IoT- and blockchain-integrated environments in the future.

REFERENCES

1. A. E. Omolara *et al.*, "The internet of things security: A survey encompassing unexplored areas and new insights," *Computers & Security*, vol. 112, p. 102494, Jan. 2022, doi: 10.1016/j.cose.2021.102494.
2. A. Ghubaish, T. Salman, M. Zolanvari, D. Unal, A. Al-Ali, and R. Jain, "Recent Advances in the Internet-of-Medical-Things (IoMT) Systems Security," *IEEE Internet Things J.*, vol. 8, no. 11, pp. 8707–8718, Jun. 2021, doi: 10.1109/JIOT.2020.3045653.
3. P. Rani, J. Kumar, S. Singh, P. Dey, and L. H. Jasim, "Decoding the Aspects of Intelligent Traffic Management," in *Artificial Intelligence Technologies for Smart and Sustainable Urban Transportation*, 1st ed., P. Raj, S. Yadav, M. K. Mishra, S. P. Yadav, and V. H. C. Albuquerque, Eds., Wiley, 2025, pp. 287–300. doi: 10.1002/9781394346776.ch17.
4. P. Rani, R. Kumar, A. Singh, J. Jagtap, and M. Almusawi, "Testifying the Criticality of the Internet of Things (IoT), 5G and AI: A Perfect Combination for Battery Management," in *Artificial Intelligence Technologies for Smart and Sustainable Urban Transportation*, 1st ed., P. Raj, S. Yadav, M. K. Mishra, S. P. Yadav, and V. H. C. Albuquerque, Eds., Wiley, 2025, pp. 71–87. doi: 10.1002/9781394346776.ch5.
5. C. Ma and M. Jiang, "Practical Lattice-Based Multisignature Schemes for Blockchains," *IEEE Access*, vol. 7, pp. 179765–179778, 2019, doi: 10.1109/ACCESS.2019.2958816.
6. M. Kansal, A. K. Singh, and R. Dutta, "Efficient Multi-Signature Scheme Using Lattice," *The Computer Journal*, vol. 65, no. 9, pp. 2421–2429, Sep. 2022, doi: 10.1093/comjnl/bxab077.
7. V. Chamola, A. Jolfaei, V. Chanana, P. Parashari, and V. Hassija, "Information security in the post quantum era for 5G and beyond networks: Threats to existing cryptography, and post-quantum cryptography," *Computer Communications*, vol. 176, pp. 99–118, Aug. 2021, doi: 10.1016/j.comcom.2021.05.019.

8. A. Shamir, “Identity-Based Cryptosystems and Signature Schemes,” in *Advances in Cryptology*, vol. 196, G. R. Blakley and D. Chaum, Eds., in Lecture Notes in Computer Science, vol. 196. , Berlin, Heidelberg: Springer Berlin Heidelberg, 1985, pp. 47–53. doi: 10.1007/3-540-39568-7_5.
9. D. S. Gupta and G. P. Biswas, “Design of lattice-based ElGamal encryption and signature schemes using SIS problem,” *Trans Emerging Tel Tech*, vol. 29, no. 6, p. e3255, Jun. 2018, doi: 10.1002/ett.3255.
10. T. Güneysu, V. Lyubashevsky, and T. Pöppelmann, “Practical Lattice-Based Cryptography: A Signature Scheme for Embedded Systems,” in *Cryptographic Hardware and Embedded Systems – CHES 2012*, vol. 7428, E. Prouff and P. Schaumont, Eds., in Lecture Notes in Computer Science, vol. 7428. , Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 530–547. doi: 10.1007/978-3-642-33027-8_31.
11. M. Ajtai, “Generating hard instances of lattice problems (extended abstract),” in *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing - STOC ’96*, Philadelphia, Pennsylvania, United States: ACM Press, 1996, pp. 99–108. doi: 10.1145/237814.237838.
12. C. Peikert, “A Decade of Lattice Cryptography,” *FNT in Theoretical Computer Science*, vol. 10, no. 4, pp. 283–424, 2016, doi: 10.1561/0400000074.
13. P. W. Shor, “Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer,” *SIAM Rev.*, vol. 41, no. 2, pp. 303–332, Jan. 1999, doi: 10.1137/S0036144598347011.
14. D. Johnson, A. Menezes, and S. Vanstone, “The Elliptic Curve Digital Signature Algorithm (ECDSA),” *IJIS*, vol. 1, no. 1, pp. 36–63, Aug. 2001, doi: 10.1007/s102070100002.
15. P. Rani, U. C. Garjola, and H. Abbas, “A Predictive IoT and Cloud Framework for Smart Healthcare Monitoring Using Integrated Deep Learning Model,” *NJF Intelligent Engineering Journal*, vol. 1, no. 1, pp. 53–65, Dec. 2024, doi: 10.64179/3080-7549.1004.
16. W. Yin, Q. Wen, W. Li, H. Zhang, and Z. Jin, “An Anti-Quantum Transaction Authentication Approach in Blockchain,” *IEEE Access*, vol. 6, pp. 5393–5401, 2018, doi: 10.1109/ACCESS.2017.2788411.
17. P. Bagchi, B. Bera, A. K. Das, S. Shetty, P. Vijayakumar, and M. Karuppiah, “Post quantum lattice-based secure framework using aggregate signature for ambient intelligence assisted blockchain-based IoT applications,” *IEEE Internet of Things Magazine*, vol. 6, no. 1, pp. 52–58, 2023.
18. A. Singh *et al.*, “Blockchain-Based Lightweight Authentication Protocol for Next-Generation Trustworthy Internet of Vehicles Communication,” *IEEE Trans. Consumer Electron.*, vol. 70, no. 2, pp. 4898–4907, May 2024, doi: 10.1109/TCE.2024.3351221.
19. P. Rani, S. Verma, S. P. Yadav, B. K. Rai, M. S. Naruka, and D. Kumar, “Simulation of the Lightweight Blockchain Technique Based on Privacy and Security for Healthcare Data for the Cloud System:,” *International Journal of E-Health and Medical Communications*, vol. 13, no. 4, pp. 1–15, Sep. 2022, doi: 10.4018/IJEHMC.309436.
20. D. Cash, D. Hofheinz, E. Kiltz, and C. Peikert, “Bonsai Trees, or How to Delegate a Lattice Basis,” *J Cryptol*, vol. 25, no. 4, pp. 601–639, Oct. 2012, doi: 10.1007/s00145-011-9105-2.
21. V. Lyubashevsky, “Lattice Signatures without Trapdoors,” in *Advances in Cryptology – EUROCRYPT 2012*, vol. 7237, D. Pointcheval and T. Johansson, Eds., in Lecture Notes in Computer Science, vol. 7237. , Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 738–755. doi: 10.1007/978-3-642-29011-4_43.
22. L. Ducas, A. Durmus, T. Lepoint, and V. Lyubashevsky, “Lattice Signatures and Bimodal Gaussians,” in *Advances in Cryptology – CRYPTO 2013*, vol. 8042, R. Canetti and J. A. Garay, Eds., in Lecture Notes in Computer Science, vol. 8042. , Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 40–56. doi: 10.1007/978-3-642-40041-4_3.