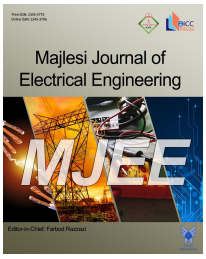

Volume 19, Issue 1, 192516 (1-9)

Majlesi Journal of Electrical Engineering (MJEE)

https://doi.org/10.57647/j.mjee.2025.1901.16

Ranking of post-quantum cryptography digital signature schemes using evaluation based on distance from average solutions

Anitha Kumari Kumarasamy*, Jaishriram Pichaikutty Muthu, Shakthi Sathiswaran, Darshan Kirthic Muthusamy Sadhasivam, Pranavv Aaditya Mohanraj

Department of IT, PSG College of Technology, TN, India.

***Corresponding author:** kak.it@psgtech.ac.in

Original Research

Received:
30 September 2024
Revised:
22 November 2024
Accepted:
6 December 2024
Published online:
1 March 2025

Abstract:

With the development of quantum computing technology, the current cryptographic systems face significant threats. Quantum algorithms, such as Shor's algorithm, have demonstrated the capability to efficiently solve mathematical problems upon which traditional cryptographic protocols rely for security. This emphasizes the critical need for Post-Quantum Cryptography (PQC) as a preemptive measure against the potential vulnerabilities posed by quantum computers. There are diverse signature schemes available, each exhibiting unique performance characteristics. The selection of an optimal scheme tailored to specific applications is necessary for ensuring both efficiency and security. To address this, a novel approach based on Evaluating Distance from Average Solution (EDAS) can be employed to rank the PQC algorithms based on the compromise score computed within the algorithm. In the pursuit of evaluating various schemes, signatures are generated using SPHINCS+-Haraka-128s-simple, SPHINCS+-Haraka-256f-simple, Supersingular Isogeny Key Encapsulation (SIKE), Falcon-1024 and Dilithium5. These schemes represent a spectrum of post quantum cryptographic techniques, each with its strengths and weaknesses. The performance metrics are systematically measured to provide a quantitative basis for comparison. Key aspects, including the efficiency of generating keys, signing processes, and verification procedures, are scrutinized to capture the schemes' overall capabilities. The EDAS is then calculated for each metric using the weight computed by Eigenvector or Real Time Aggregation strategies, offering a nuanced perspective by accounting for the distance of each scheme's performance from the average solution. By considering these findings, stakeholders can make informed decisions about which scheme aligns best with their particular security and efficiency requirements, thus contributing to a more robust and tailored digital signature implementation.

Keywords: Digital signature schemes; Eigenvector; Evaluation based on distance from average solution; Post-quantum cryptography; Ranking; Real-time aggregation

1. Introduction

With rapidly developing quantum computing technology, the safety of ordinary cryptographic systems is threatened. Quantum algorithms, such as Shor's algorithm, have shown extraordinary efficiency in solving mathematical problems underlying classical cryptographic protocols. Thus, the urgency of adopting Post-Quantum Cryptography (PQC) as a preemptive defense against potential threats from quantum computers is emphasized. Among various cryptographic techniques, it is essential to choose an appropriate signature scheme according to specific applications to ensure both efficiency and security. Cryptographic weaknesses enhance the decision-making process by systematically evaluating and ranking alternative post-quantum cryptographic algorithms based on criteria such as security strength, performance, and scalability. This capability positions EDAS as a valuable tool in identifying and selecting robust cryptographic solutions that are resistant to quantum threats.

This paper presents a new approach based on Evaluating Distance from Average Solution (EDAS) to rank the PQC algorithms using the score obtained. The algorithms considered include SPHINCS+-Haraka-256f-simple, SPHINCS+-Haraka-128s-simple, Supersingular Isogeny Key Encapsulation (SIKE-p751) based DSA, Falcon-1024 and Dilithium5

among others which are evaluated through EDAS. Each of these schemes is representative of post-quantum cryptography methods with different strengths and weaknesses. The ranking uses a quantitative approach that involves the systematic measurement of performance metrics including key generation efficiency, signing processes and verification procedures for comparison purposes. Eventually, the metric of Distance from Average Solution (DAS) is computed for each metric, which gives insight into how well schemes perform relative to the average.

As a part of the EDAS algorithm, weights are computed for each parameter based on which these algorithms are ranked. Two approaches are implemented for this. The eigenvector approach involves calculating the weights based on the main eigenvector of the pairwise comparison matrix. In this way, the algorithm will identify major factors that contribute most to its overall performance among all other algorithms. The technique uses eigenvalues and corresponding eigenvectors to assign weighting to each parameter in an evaluation process. A higher eigenvector value indicates a stronger influence on ranking of signature schemes, so such parameters are assigned greater weights. However, real-time aggregation strategy takes into consideration dynamic computations for weightings. With this method, it adjusts weights using real time performance data thus incorporating the current information in the valuation process. Continuously updating/re-adjusting weights as per changing conditions or priorities guarantees that assessment remains relevant and up to date with latest performance dynamics. This flexibility accommodates changes and updates making evaluation more adaptable. By employing either one of these strategies i.e., eigenvector or real-time aggregation; a comprehensive and flexible approach towards weight computation is achieved by the EDAS algorithm.

This approach enables a comprehensive ranking of signature schemes that matches varying application-specific priorities. It further outlines practical implications associated with EDAS in nine diverse application areas such as agriculture, business management, construction management, energy and natural resources, healthcare management, Information Technology (IT), manufacturing and supply chain management and transportation management.

With that integration, stakeholders can make informed decisions on signing up for the systems that best meet their security efficiency needs. Therefore this paper provides inputs to the development of a secure and efficient implementation framework of digital signatures customized for the quantum computing era.

The objective of this research is to enhance the evaluation and selection process of cryptographic algorithms, particularly in the context of post-quantum digital signatures. Traditional comparison methods often lack optimization and face several limitations, reducing their effectiveness. To address this, the research aims to introduce Evaluation based on Distance from Average Solution as a ranking algorithm to provide a systematic and objective approach for evaluating the performance of the cryptographic algorithms. Within EDAS, the weights are computed using either the eigenvector strategy or real-time aggregation strategy which quantifies the importance of each parameter used for comparing the algorithms, thereby enhancing the reliability of the cryptographic algorithm evaluations.

2. Literature survey

Evaluation based on Distance from Average Solution has seen increased usage in multiple Multi-Criteria Decision-Making (MCDM) applications. EDAS is a powerful tool that assesses alternatives based on their distance from an average solution, allowing for more informed decision-making. Known for its robustness against weight variations, EDAS is applicable across various domains.

A. Literature review on EDAS applications in different fields

Ali Ebadi Torkayesh et al. conducted a comprehensive literature review on EDAS as an Multi-Criteria Decision Making (MCDM) technique, highlighting its application across real-world sectors such as agriculture, business, construction, IT, manufacturing, supply chain, and transportation [1]. Phuong Thanh Phan et al. suggested the utility of EDAS in scenarios with increased evaluation parameters, specifically in selecting construction managers within civil engineering [2]. In multi-criteria inventory classification (MCIC), Mehdi Keshavarz-Ghorabaee et al. implemented EDAS to evaluate alternatives using positive and negative distances [3].

B. Sustainable and industrial applications of EDAS

Mohamed Abdel-Basset et al. applied EDAS to the sustainable selection of offshore wind power plant locations, emphasizing its stability across various weights, transparency, and dependability [4]. In the defense industry, Güneri et al. demonstrated the practical relevance of EDAS by evaluating supplier companies [5]. Shankar Chakraborty et al. combined EDAS with the TOPSIS method to enhance MCDM processes [6].

C. Advances in EDAS: integration with linguistic numbers and MCDM techniques

Siqi Zhang et al. examined Picture 2-Tuple Linguistic Numbers (P2TLNs) and their integration with EDAS, allowing for multi-criteria group decision-making while highlighting the advantages of this novel approach over traditional EDAS [7]. Torkayesh et al. reviewed EDAS in multiple fields and explored its integration with machine learning and advanced decision-making models, further extending its real-world applications [8]. Chen et al. introduced improvements to EDAS that incorporate aggressive and conservative estimates, enhancing complex C-IF information measurement and enabling robust ranking in MCDA problems, such as post-quantum cryptographic algorithms [9].

D. Recent innovations in EDAS applications and enhancements

EDAS has been applied across various domains with evolving enhancements. For instance, Büyüktaş et al. (2022) used EDAS for green supplier selection, showcasing its effectiveness in sustainability assessments and its ability to

accommodate various criteria for aligning suppliers with organizational sustainability goals [10]. Jiang et al. (2023) introduced fuzzy decision-making with EDAS, creating a reliable framework for uncertain environments [11]. In smart city planning, Zhang et al. (2024) demonstrated EDAS's adaptability to urban challenges, supporting multi-criteria assessments for urban development projects [12].

E. Application of EDAS for post-quantum cryptographic algorithm selection

This paper utilizes EDAS to rank post-quantum cryptography digital signature algorithms, including SPHINCS+-Haraka-128s-simple, SPHINCS+-Haraka-256f-simple, SIKE-p751, Dilithium5, and Falcon-1024. Daniel J. Bernstein et al. underscore the importance of PQC in the quantum computing era, aiming for secure yet flexible cryptographic solutions [13]. Shagun Sharma et al. provide a technical overview of PQC algorithms, examining methods for securing classical cryptographic algorithms [14].

F. Performance evaluation of PQC algorithms

Kanad Basu et al. proposed a High-Level Synthesis (HLS) hardware design approach to assess the hardware performance of PQC algorithms [15, 16]. Daniel J. Bernstein et al. also introduced a Sphincs+ signature framework utilizing a FORS scheme and customizable hash functions for digital signatures, simplifying security analysis [17]. Deepraj Soni et al. reviewed variants of Sphincs+ and Falcon algorithms, focusing on trade-offs in power, area, speed, and security parameters for key and signature generation [18–20].

G. Comparisons and trade-offs in PQC algorithms

Léo Ducas et al. proposed the Dilithium lattice-based signature algorithm, which features a reduced public key size for faster processing speeds [21]. James Howe et al. analyzed the Dilithium and Falcon algorithms on the ARM Cortex M7, providing insights into performance on constrained devices [22, 23]. Tako Boris Fouotsa et al. introduced a countermeasure for SIKE post-quantum cryptography that avoids traditional key disclosure requirements [24]. Fábio Borges et al. compared PQC security, focusing on key agreement protocols that address challenges like the Discrete Logarithm Problem and Integer Factorization Problem [25]. Manish Kumar et al. compared NIST-selected PQC algorithms by evaluating metrics like NIST level, key sizes, and performance [10, 26]. Teik Guan Tan et al. provided a feasibility matrix that matches PQC algorithms to application requirements, facilitating the replacement of classical digital signing algorithms with PQC alternatives [11]. Manohar Raavi et al. evaluated NIST finalist PQC signature schemes, analyzing implementation costs, communication overheads, and processing times [12]. Marin Vidaković et al. offered insights into PQC algorithm integration, comparing key metrics like security level, speed, and efficiency within constrained environments [27].Conventional post-quantum digital signature comparisons exhibit several shortcomings. Firstly, the absence of standardized algorithms for ranking post-quantum cryptography schemes across diverse domains restricts informed decision-making in cryptographic solution selection. Secondly, the lack of established methodologies for computing weights assigned to different parameters undermines the reliability and objectivity of cryptographic algorithm assessments. Lastly, insufficient clarity in the reasoning for weight assignment within existing EDAS-based ranking methodologies leads to ambiguity in cryptographic algorithm evaluations.

3. Proposed methodology

In recent years, decision-making processes have increasingly recognized the significance of uncertainty and imprecision in evaluating alternatives across various domains. The Evaluation based on Distance from Average Solution (EDAS), introduced in 2015, is a widely recognized method that is commonly used in various decision-making situations. It provides a list of alternatives ranked by their cumulative distance scores. Due to its flexibility and effectiveness, EDAS has become one of the most reliable solutions for complex decision-making problems. Its wide acceptance proves it is a choice for many decision-makers. Originally developed as a ranking tool to prioritize among alternatives in complex landscapes of multiple criteria decisions, EDAS had remarkable features through its normalization process. In contrast to traditional methods like Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) and VIKOR, which stands for Viekriterijumsko Kompromisno Rangiranje, a Serbian term for "multi-criteria optimization and compromise solution", which use ideal and nonideal solutions, EDAS differs by utilizing normalization techniques built on the concept of average solution. This shift comes from the understanding that realistic decision contexts often require subtlety; hence moving closer or farther from the ideal setting does not guarantee the right alternative.

Within EDAS, two different weight computation strategies are employed to quantify the priority of parameters, which in turn influence the ranking of algorithms. These strategies, namely the eigenvector strategy and the real-time aggregation strategy, offer distinct approaches to assessing the importance of parameters. The eigenvector strategy utilizes mathematical principles to determine weights, considering the importance of each parameter. In contrast, the real-time aggregation strategy allows for dynamic adjustments of weights based on the latest data values, providing adaptability to changing circumstances. By employing these complementary strategies within the EDAS framework, decision-makers can obtain a comprehensive and nuanced understanding of algorithm performance, enabling informed decision-making across various domains.

The Evaluation based on Distance from Average Solution method heavily relies on its weighting techniques to assess and rank alternatives effectively. However, previous methods like Opinion Weight Criteria Method (OWCM) and the Full Consistency Method (FUCOM), which can be utilized within the EDAS framework, have inherent drawbacks that can affect decision-making outcomes. OWCM, while beneficial for incorporating expert opinions, often suffers from subjectivity, leading to potential inconsistencies in rankings when different experts provide conflicting assessments. Fur-

thermore, its dependence on qualitative judgments can limit its effectiveness in scenarios where objective data is crucial. Similarly, FUCOM aims to ensure consistency through structured pairwise comparisons, yet it remains labor-intensive and may introduce human error as the complexity of the decision matrix increases. The necessity for multiple evaluations can become cumbersome, particularly in large-scale assessments.

Both methods also lack the adaptability needed in dynamic environments, where criteria priorities may shift rapidly, as they do not facilitate automatic recalibration based on real-time data inputs. These limitations highlight the necessity for an enhanced weighting approach within EDAS that minimizes subjectivity and maximizes consistency and adaptability in multi-criteria decision-making.

3.1 Eigenvector method

The eigenvector method involves assessing the importance or priority of the parameters by constructing a pairwise comparison matrix based on the given ranking. The obtained matrix is used to compute the respective eigenvector and eigenvalues using which the weights are computed by normalizing the principal eigenvector i.e., the eigenvector with the maximum eigenvalue. This approach provides a systematic method to quantify the importance of the parameters.

3.1.1 Matrix generation function

Step 1: Input processing: The function utilizes the "rank" parameter which carries a ranked list of factors.

Step 2: Matrix initialization: To store importance weights for influential factors, initially, a matrix filled up with zeros by the function.

Step 3: Diagonal Initialization: Each factor will have equal priority to itself and hence all diagonal elements are set as 1.

Step 4: Importance Assignment: Starting from the first rank, an increase in value is assigned to each element in the matrix. The higher ranks correspond to more important values.

Step 5: Incremental Importance: This involves moving through the rank list from lowest to highest and increasing the importance or priority values along the way up so that there is a gradual increase among them.

Step 6: Dynamic Scaling: In addition, to maintain consistency in the matrix and ensure relevant factor weights, this function dynamically scales the importance values in proportion to each other.

Output: Finally, when complete, this generates a matrix that reflects how important every factor is according to the ranking given. This matrix is referred to as the priority matrix.

Following the creation of the priority matrix, the algorithm proceeds to calculate the factors' weights using the Eigenvector strategy.

3.1.2 Calculating the parameter weights

Step 1: Eigenvector Computation: The algorithm applies NumPy linear algebra functions to determine the eigenvalues and eigenvectors of the priority matrix. The biggest eigenvalue's eigenvector is denoted as v_i. It will represent the principal vector of determining all factor weights.

$$Av_i = \lambda\, j\, \max v_i \tag{1}$$

where A is the pairwise comparison matrix, v is the eigenvector, λ is the eigenvalue, i represents the eigenvectors and j is the eigenvalue in i^{th} eigenvector.

Step 2: Weight Calculation: After computing eigenvalues and eigenvectors, it moves on to calculate the weightings of factors by normalizing the primary eigenvector. This step standardizes all the weights so that they can sum up to 1, which allows for effective comparisons among these factors.

$$w_i = \frac{v_i}{\sum_{j=1}^{n} v_j} \tag{2}$$

where w_i is the weight assigned to factor i, v_i is the i^{th} eigenvector.

This algorithm uses a rank-based way of identifying factors with the parameters ranked from least important to most important depending on assigned scores. These scores are then transformed into importance or priority levels within the priority matrix.

The model's versatility allows researchers to apply it across multiple domains where factorization plays a vital role in determining respective weights. Typically, programming code is utilized to simulate real-world problems, enabling the testing of various scenarios to gain deeper insights into the effects of different factors on the outcome. This iterative process aids in developing a clearer understanding of how various parameters influence the final results.

3.2 Weight calculation by real-time aggregation

Step 1: Reciprocal Calculation and Summation: Initially, the function called calculate_weights divides each element of the input array by one (calculates the reciprocal). These reciprocals are then added to obtain the total reciprocal sum.

The input array consists of real-time parametric values obtained from [28].

Input array = [[98.8, 60.57, 56.52, 500, 434, 378],

[320, 10520, 29132, 300, 2528, 1312],

[3305.33, 130.95, 1841.3, 500, 64, 32],

[1635, 38.42, 1592.1, 500, 128, 64],

[40.23, 1446.52, 9782.67, 300, 1281, 897]]

Step 2: Standardization: After getting the sum of the reciprocal values, normalize each reciprocal by dividing with the total sum. This is done to ensure that the weights sum up to 1 which facilitates their straightforward interpretation and comparison.

$$W(e_i) = \frac{1/e_i}{\sum_{j=1}^{n} 1/e_i} \tag{3}$$

where e_i is the i^{th} parameter's real-time value.

Once the weight calculation function is established, it is applied to each algorithm's performance metrics or parameters, generating weights for each parameter across all algorithms.

This step allowed us to quantitatively assess the relative importance of each parameter in the context of different cryptographic algorithms. By aggregating the weights for each parameter, we obtained insights into their significance and impact on algorithm selection.

3.2.1 Evaluation based on distance from average solution (EDAS) ranking

The Eigenvector and the Real-time Aggregation strategy quantify the importance of the parameters for comparing the PQC algorithms. These computed weights are incorporated within the EDAS algorithm and ranks are generated based on the compromise score.

EDAS uses two measures, Positive Distance from Average Value (PDA) and Negative Distance from Average Value (NDA), to compare different choices and establish their relative priority levels. These measures are crucial for generating final orderings.

Step 1: Create the initial decision matrix based on real-world data. For the real-time values, we utilize real-time values obtained from [28].

Input array = [[98.8, 60.57, 56.52, 500, 434, 378]

[320, 10520, 29132, 300, 2528, 1312]

[3305.33, 130.95, 1841.3, 500, 64, 32]

[1635, 38.42, 1592.1, 500, 128, 64]

[40.23, 1446.52, 9782.67, 300, 1281,897]]

This matrix outlines the alternatives or the algorithms including SIKE-p751 based DSA, Falcon-1024, Dilithium5, SPHINCS+-Haraka-128s-simple and SPHINCS+-Haraka-256f-simple (indexed as $m = 1, 2, \cdots, i$) across various criteria or parameters including NIST security level, Computation time, signing time, verifying time, public key size and private key size (indexed as n where $n = 1, 2, \cdots, j$).

Step 2: Determine the average solution by considering all the parameters. Calculate the average solution for each parameter.

$$\text{Average of parameter } (AV_j) = \frac{\sum_{i=1}^{n} x_{ij}}{n} \tag{4}$$

where,

i = algorithm

j = parameter

x_{ij} = real-time time values of i^{th} algorithm and j^{th} parameter

Step 3: Calculate two critical measures of EDAS, namely PDA (Positive Distance from Average) and NDA (Negative Distance from Average) based on the nature of conflicting parameters. For the beneficial parameter NIST security level, compute PDA and NDA values using the designated equations, while for non-beneficial parameters which include signing time, verification time, public key size, private key size and computation time, utilize separate equations as shown below.

$$\begin{aligned}
\text{PDA_B}_{ij} &= \frac{\max(0, x_{ij} - AV_j)}{AV_j} \\
\text{NDA_B}_{ij} &= \frac{\max(0, AV_j - x_{ij})}{AV_j} \\
\text{PDA_NB}_{ij} &= \frac{\max(0, AV_j - x_{ij})}{AV_j} \\
\text{NDA_NB}_{ij} &= \frac{\max(0, x_{ij} - AV_j)}{AV_j}
\end{aligned} \tag{5}$$

where,

PDA_B_{ij} is the positive distance from the average solution for the beneficial parameter, NDA_B_{ij} is the negative distance from the average solution for the beneficial parameter, PDA_NB_{ij} is the positive distance from the average solution for non-beneficial parameters, NDA_NB_{ij} is the negative distance from the average solution for non-beneficial parameters, and,

i = algorithm

j = parameter

x_{ij} = real-time time values of i^{th} algorithm and j^{th} parameter

AV_j = Average of parameter j

Step 4: Utilize weight coefficients assigned to each parameter obtained from the real-time aggregation method or eigenvector method. These coefficients are applied to determine the weighted sum of PDA and NDA values.

$$\begin{aligned}
SP_i &= \sum_{j}^{n} w_\text{B}_j \text{PDA_B}_{ij} + \sum_{j}^{n} w_\text{NB}_j \text{PDA_NB}_{ij} \\
SN_i &= \sum_{j}^{n} w_\text{B}_j \text{NDA_B}_{ij} + \sum_{j}^{n} w_\text{NB}_j \text{NDA_NB}_{ij}
\end{aligned} \tag{6}$$

where SP_i is the sum of the positive distance of the i^{th} algorithm, SN_i is the sum of the negative distance of the i^{th} algorithm, w_B_j is the weight of the i^{th} beneficial parameter, w_NB_j is the weight of the j^{th} non-beneficial parameter.

Step 5: Normalize the weighted sum values of PDA and NDA using the specific normalization equation.

$$\text{NSP}_i = \frac{SP_i}{\max(SP_i)} \quad \text{NSN}_i = 1 - \frac{SN_i}{\max(SN_i)} \tag{7}$$

where NSP_i is the normalized sum of the positive distance of the i^{th} algorithm, NSN_i is the normalized sum of the negative distance of the i^{th} algorithm.

Step 6: Finally, ascertain the compromise score (AS_i) for each algorithm. Rank the algorithm based on their compromise scores, with higher scores indicating algorithms that are better suited for the given application.

$$AS_i = \frac{1}{2}(\text{NSP}_i + \text{NSN}_i) \tag{8}$$

Following the introduction of EDAS, numerous studies aimed to strengthen its reliability and adaptability by incorporating various uncertainty sets to effectively address complex real-world problems.

4. Result analysis

The result analysis provides a comprehensive comparison of PQC algorithms with their real-time values of NIST level, Public and Private key sizes and Signing, Verification and Computation time. Following the real-time values comparison, the weights computed using the eigenvector and real-time aggregation strategy are analyzed through graphical representation. This comparison highlights the variations in weights assigned to different parameters by each strategy. Furthermore, the compromise scores provided by the Evaluation based on Distance from the Average Solution of the PQC algorithms are compared based on their compromise score to obtain which algorithm is most suitable for the given application.

4.1 Comparative analysis of the post quantum cryptography algorithms based on their real-time values

In figure 1, it's evident that the PQC algorithms SPHINCS+-Haraka-256f-simple, SIKE-p751, Falcon-1024, ml_dsa_87 and Dilithium5 have the highest NIST level of 5. Conversely, SPHINCS+Haraka-128s-simple, ml_dsa_44, ml_dsa_65 exhibits a comparatively lower NIST level of 1, 2, 3 respectively indicating lower security measures.

From figure 2, it is inferred that SPHINCS+-Haraka-128s-simple has the smallest public and private key sizes (32 and 64 bytes respectively), while Falcon-1024 and ml_dsa_87 have the largest public key size (2592 bytes) and ml_dsa_65 has the largest private key size (4896 bytes). SPHINCS+-Haraka-128s-simple offers the most compact option, but potentially with lower security. Conversely, Falcon-1024 and ml_dsa_87 have large public keys and ml_dsa_65's large private key translates to larger data transfers, storage needs, and potentially slower processing, although they might provide stronger security.

In figure 3, it is observed that SPHINCS+-Haraka-128s-simple appears to have the fastest signing time (around 6.88 milliseconds), followed by SPHINCS+-Haraka-256f-simple (around 38.42 milliseconds) while Dilithum5 seems to have the slowest signing time (around 5279.67 milliseconds). For the Verification time, ml_dsa_44 seems to have the fastest verification time (around 14 milliseconds), followed by ml_dsa_65 (around 23 milliseconds). Dilithum5 again seems to have the slowest verification time (around 10341 milliseconds). In the case of Computation time, ml_dsa_44 also has the fastest computation time (around 17 milliseconds), followed by ml_dsa_65 (around 33 milliseconds). Dilithuim5 again seems to have the slowest computation time (around 10341.1 milliseconds). From this, we can infer that Dilithium5 consistently takes the most time, indicating that it is the most time-consuming cryptographic algorithm.

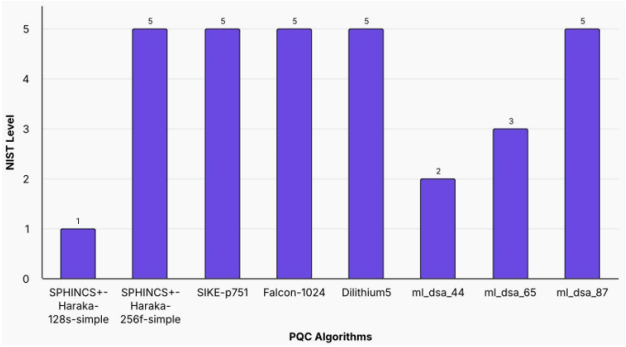

Figure 1. NIST level vs PQC algorithms.

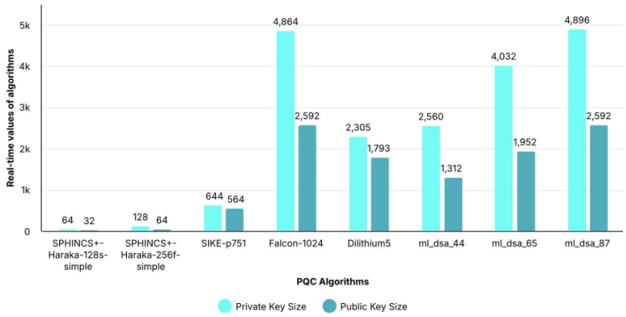

Figure 2. Public and private key sizes vs PQC algorithms.

4.2 Weight comparison using eigenvector and real-time aggregation

In figure 4, the eigenvector strategy prioritizes ranking for weight allocation, potentially resulting in significant differences in algorithmic weights. This strategy typically depends on predetermined criteria or past data for assigning weights to parameters, often leading to marked divergences among algorithms. Nonetheless, such methods might overlook real-time fluctuations in performance metrics, introducing possible inaccuracies in weight distribution. Conversely, a real-time aggregation strategy dynamically adjusts weights based on current values, offering finer control and adaptability in dynamic contexts. By integrating the latest performance data, this approach accommodates nuanced variations in algorithmic weights, reflecting their current performance status.

4.3 Rank comparison using eigenvector and real-time aggregation with EDAS

Table 2 represents the compromise score and the rank for each of the PQC algorithms by Eigenvector strategy. SIKE-p751 has the highest ranking making it most suitable for the specific application.

Table 3 represents the compromise score and the rank for each of the PQC algorithms by Real-time aggregation strat-

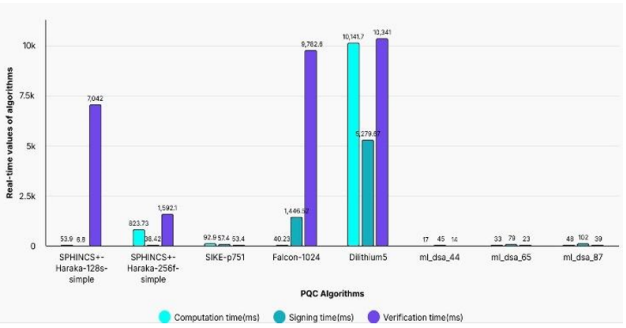

Figure 3. Signing time, verification time and computation time vs PQC algorithms.

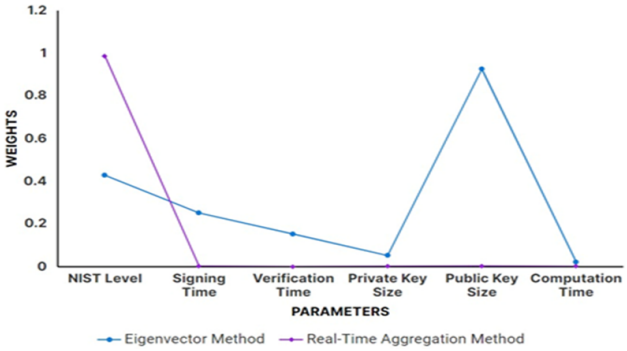

Figure 4. Eigenvector vs real-time aggregation for each parameter.

egy. SIKE-p751 has the highest ranking making it most suitable for the specific application.

4.4 Rank comparison with OCPM and FUCOM methods

Table 4 clearly demonstrates that the Eigenvector method is the superior approach for ranking post-quantum cryptographic algorithms, as evidenced by its consistent performance across various metrics. With SIKE-p751 achieving the highest score of 0.4823 and securing the top rank in all three methods, it highlights the method's effectiveness in integrating multiple criteria such as security and efficiency into a coherent evaluation framework. The second position of SPHINCS+-Haraka-256f-simple further illustrates the Eigenvector method's ability to balance performance and security parameters effectively. In contrast, the OWCM and FUCOM methods exhibit more variability in their rankings, particularly with SPHINCS+-Haraka-128s-simple, which is ranked lower in the Eigenvector method due to its efficiency shortcomings. This inconsistency suggests that while OWCM focuses on security, and FUCOM emphasizes efficiency, they lack the comprehensive adaptability offered by the Eigenvector method. Overall, the results underscore the Eigenvector method's robustness and reliability, making it the preferred choice for complex decision-making scenarios in post-quantum cryptography.

Remarks

Based on the analysis presented in figure 5, it is evident that the eigenvector weight computation strategy emerges as the preferred method over the real-time aggregation weight computation strategy, despite its increased time complexity. This preference arises from the eigenvector strategy's capacity to generate compromise scores with a wider distribution, facilitating reliable ranking of algorithms according to application-specific priorities. While the real-time aggregation strategy enables the manipulation of weights based on the latest data, the eigenvector strategy offers more accurate results by capturing the inherent importance of each parameter. By leveraging mathematical principles to determine weights, the eigenvector strategy offers a robust and objective approach to decision-making in cryptographic algorithm evaluation. Despite its computational complexity, the eigenvector strategy's ability to generate compromise scores enables decision-makers to prioritize algorithms effectively, considering various application-specific considerations.

In contrast, while the real-time aggregation strategy offers the advantage of adaptability to dynamic data changes, its effectiveness may be compromised by the lack of a clear framework for determining parameter weights. Without a systematic approach to weight computation, the real-time aggregation strategy may lead to inconsistencies or biases in the evaluation process, limiting its utility for precise algorithm ranking. Thus, while both strategies have their merits, the eigenvector strategy stands out as the preferred choice for its ability to provide accurate and reliable results in cryptographic algorithm evaluations.

5. Discussion

The proposed approach of using the Evaluating Distance from Average Solution (EDAS) method for ranking post-quantum cryptography algorithms, such

Table 1. Calculated weights for each parameter by using the eigenvector method and real-time aggregation method.

Parameters	Eigenvector Method	Real-Time Aggregation Method
NIST Level	0.4284	0.9877
Signing Time	0.2523	0.0030
Verification Time	0.1530	0.0007
Private Key Size	0.0529	0.0026
Public Key Size	0.9256	0.0041
Computation Time	0.0241	0.0019

Table 2. EDAS based ranking of algorithms using eigenvector method.

Algorithms	Eigenvector Method	Rank Obtained
SPHINCS+-Haraka-256f-simple	0.4344	2
SPHINCS+-Haraka-128s-simple	0.0525	7
SIKE-p751	0.4969	1
Dilithium5	0.0827	5
Falcon-1024	0.1196	4
ml_dsa_44	0.0545	6
ml_dsa_65	0.0521	8
ml_dsa_87	0.4160	3

Table 3. EDAS based ranking of algorithms using Real-time Aggregation method.

Algorithms	Real-time Aggregation Method	Rank Obtained
SPHINCS+-Haraka-256f-simple	0.4986	2
SPHINCS+-Haraka-128s-simple	0.0007	6
SIKE-p751	0.5	1
Dilithium5	0.4654	5
Falcon-1024	0.4743	4
ml_dsa_44	0.00035	7
ml_dsa_65	0.00033	8
ml_dsa_87	0.4901	3

as SPHINCS+-Haraka-128s-simple, SPHINCS+-Haraka-256f-simple, SIKE-p751, Dilithium5, and Falcon-1024, offers a systematic framework. When applying EDAS to rank post-quantum cryptographic (PQC) algorithms, security concerns like data integrity attacks and process manipulation must be addressed. Tampering with input data or ranking criteria may skew results, potentially leading to the selection of weaker algorithms. Additionally, side-channel attacks could expose sensitive information about the algorithms. Securing the EDAS framework is essential to ensure that the ranking process remains resistant to manipulation and is reliable for critical cryptographic applications.

Fault detection is another crucial factor when evaluating PQC algorithms with EDAS. Faults, whether due to hardware failures or malicious attacks, can expose vulnerabilities in cryptographic systems. Integrating fault detection similar to schemes used for AES, such as concurrent structure-independent fault detection schemes for the Advanced Encryption Standard, or FPGA-based PQC implementations using isogenies on elliptic curves enhances the robustness of the ranking process.

6. Future work

In the future, the proposed method of ranking the post-quantum cryptographic signatures using Evaluation based on Distance from Average Solutions (EDAS) can be refined through the following approaches:

• Including integration of an FPGA-based ranking process, that significantly enhances the speed and efficiency of the ranking framework.

• Using machine learning models for dynamic adjustments based on new performance data, enabling real-time updates. This approach will help the ranking framework stay relevant and adaptable.

• Combining EDAS with other decision-making techniques for a better analysis of algorithm performance. This integration can yield deeper insights, facilitating more informed decisions when selecting post-quantum cryptographic algorithms for specific applications.

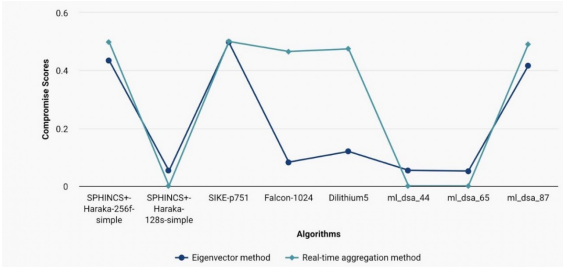

Figure 5. Ranking scores using eigenvector and real-time aggregation.

• Addressing potential security attacks on the EDAS ranking process, ensuring robustness against data manipulation, side-channel attacks, and fault injection attacks, which could compromise the evaluation and lead to biased rankings.

7. Conclusion

In conclusion, the research has highlighted the limitations of traditional methods, such as the Elliptic Curve Digital Signature Algorithm (ECDSA), in accurately assessing cryptographic algorithms, particularly in the context of emerging quantum computing technologies. We introduced the Evaluation based on Distance from Average Solution (EDAS) methodology alongside two weight computation strategies, namely the eigenvector strategy and real-time aggregation strategy, to enhance cryptographic algorithm ranking. Through analysis, we find that while both the real-time aggregation and eigenvector strategies offer valuable insights, the eigenvector strategy emerges as the more efficient choice. Despite its increased time complexity, the eigenvector strategy provides more accurate and reliable results by considering the inherent importance of each parameter. This methodical approach enables informed decision-making in cryptographic algorithm selection, contributing to advancements in cryptographic research and development.

Table 4. Ranking of OWCM, FUCOM, and Eigenvector methods.

Algorithms	Eigenvector Method	OCPM	FUCOM
SPHINCS+-Haraka-256f-simple	0.4594	0.3725	0.3406
SPHINCS+-Haraka-128s-simple	0.0796	0.3192	0.3918
SIKE-p751	0.4823	0.4506	0.4895
Dilithium5	0.0532	0.0120	0.0025
Falcon-1024	0.0891	0.1462	0.1641

Authors contributions
Authors have contributed equally in preparing and writing the manuscript.

Availability of data and materials
The data that support the findings of this study are available from the corresponding author upon reasonable request.

Conflict of interests
The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] A. Ebadi Torkayesh, M. Deveci, S. Karagoz, and J. Antucheviciene. "**A state-of-the-art survey of evaluation based on distance from average solution (EDAS): Developments and applications**.". *Expert Systems with Applications*, 221(119724), 2023.
DOI: https://doi.org/10.1016/j.eswa.2023.119724.

[2] P. T. Phan and P. T. Nguyen. "**Evaluation based on the distance from the average solution approach: A derivative model for evaluating and selecting a construction manager**.". *Technologies*, 10(5):107, 2022.
DOI: https://doi.org/10.3390/technologies10050107.

[3] M. Keshavarz-Ghorabaee, E. Zavadskas, L. Olfat, and Z. Turskis. "**Multi-criteria inventory classification using a new method of evaluation based on distance from average solution (EDAS)**.". *Informatica*, 26:435–451, 2015.
DOI: https://doi.org/10.15388/Informatica.2015.57.

[4] M. Abdel-Basset, A. Gamal, M. Elhoseny, M. A. Hossain, et al. "**Assessing the sustainable aspects of location selection for offshore wind power plant**.". *Elsevier*, pages 87–109, 2024.
DOI: https://doi.org/10.1016/b978-0-443-13378-7.00005-4.

[5] B. Güneri and M. Deveci. "**Evaluation of supplier selection in the defense industry using q-rung orthopair fuzzy set based EDAS approach**.". *Expert Systems with Applications*, 222(119846), 2023.
DOI: https://doi.org/10.1016/j.eswa.2023.119846.

[6] S. Chakraborty, P. Chatterjee, and P. P. Das. "**Evaluation based on distance from average solution (EDAS) method**.". *Apple Academic Press*, pages 183–189, 2024.
DOI: https://doi.org/10.1201/9781003377030-16.

[7] S. Zhang et al. "**EDAS method for multiple criteria group decision making under picture 2-tuple linguistic environment**.". *Mathematics*, 7(3), 2019.
DOI: https://doi.org/10.3390/math7030243.

[8] A. E. Torkayesh et al. "**A state-of-the-art survey of evaluation based on distance from average solution (EDAS): Developments and applications**.". *Expert Systems with Applications*, 221(119724), 2023.
DOI: https://doi.org/10.1016/j.eswa.2023.119724.

[9] T. Y. Chen. "**A circular intuitionistic fuzzy evaluation method based on distances from the average solution**.". *Engineering Applications of Artificial Intelligence*, 117(105499), 2023.
DOI: https://doi.org/10.1016/j.engappai.2022.105499.

[10] M. Kumar. "**Post-quantum cryptography algorithm standardization and performance analysis**.". *Array*, 15(100242), 2022.
DOI: https://doi.org/10.1016/j.array.2022.100242.

[11] T. G. Tan, P. Szalachowski, and J. Zhou. "**Challenges of post-quantum digital signing in real-world applications: A survey**.". *Cryptology ePrint Archive*, 2019. URL https://eprint.iacr.org/2019/1374.

[12] M. Raavi et al. "**Security comparisons and performance analyses of post-quantum signature algorithms**.". *Applied Cryptography and Network Security: 19th International Conference, ACNS*, pages 424–447, 2021.
DOI: https://doi.org/10.1007/978-3-030-78375-4-17.

[13] D. J. Bernstein and T. Lange. "**Post-quantum cryptography**.". *Nature*, 549(7671):188–194, 2017.
DOI: https://doi.org/10.1038/nature23461.

[14] S. Sharma et al. "**Post-quantum cryptography: A solution to the challenges of classical encryption algorithms**.". *Modern Electronics Devices and Communication Systems: Select Proceedings of MEDCOM 2021*, 2023.
DOI: https://doi.org/10.1007/978-981-19-6383-4-3.

[15] K. Basu et al. "**NIST post-quantum cryptography-a hardware evaluation study**.". *Cryptology ePrint Archive*, 2019. URL https://ia.cr/2019/047.

[16] C. A. Roma et al. "**Energy efficiency analysis of post-quantum cryptographic algorithms**.". *IEEE Access*, 9:71295–71317, 2021.
DOI: https://doi.org/10.1109/access.2021.3077843.

[17] D. J. Bernstein et al. "**The SPHINCSv+ signature framework**.". *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, pages 2129–2146, 2019.
DOI: https://doi.org/10.1145/3319535.3363229.

[18] D. Soni et al. "**SPHINCS+**.". *Hardware Architectures for Post-Quantum Digital Signature Schemes*, pages 141–162, 2021.
DOI: https://doi.org/10.1007/978-3-030-57682-0-9.

[19] H. Seo, M. Anastasova, A. Jalali, and R. Azarderakhsh. "**Supersingular isogeny key encapsulation (SIKE) round 2 on ARM Cortex-M4**.". *IEEE Transactions on Computers*, 70(10):1705–1718, 2020.
DOI: https://doi.org/10.1109/TC.2020.3023045.

[20] D. Soni et al. "**Falcon**.". *Hardware Architectures for Post-Quantum Digital Signature Schemes*, pages 31–41, 2021.
DOI: https://doi.org/10.1007/978-3-030-57682-0-3.

[21] L. Ducas et al. "**Crystals-dilithium: A lattice-based digital signature scheme**.". *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2018(3):238–268, 2018.
DOI: https://doi.org/10.46586/tches.v2018.i1.238-268.

[22] J. Howe and B. Westerbaan. "**Benchmarking and analysing the NIST PQC finalist lattice-based signature schemes on the ARM Cortex M7**.". *IACR Cryptology ePrint Archive*, 405, 2022.
DOI: https://doi.org/10.1007/978-3-031-37679-5-19.

[23] V. Lyubashevsky. "**Lattice-based digital signatures**.". *National Science Review*, 8(9), 2021.
DOI: https://doi.org/10.1093/nsr/nwab077.

[24] T. B. Fouotsa and C. Petit. "**SHealS and HealS: Isogeny-based PKEs from a key validation method for SIDH**.". *Advances in Cryptology–ASIACRYPT 2021: 27th International Conference on the Theory and Application of Cryptology and Information Security*, pages 279–307, 2021.
DOI: https://doi.org/10.1007/978-3-030-92068-5-10.

[25] F. Borges, P. R. Reis, and D. Pereira. "**A comparison of security and its performance for key agreements in post-quantum cryptography**.". *IEEE Access*, 8:142413–142422, 2020.
DOI: https://doi.org/10.1109/access.2020.3013250.

[26] M. Kumar. "**Post-quantum cryptography algorithm's standardization and performance analysis**.". *Array*, 15(100242), 2022.
DOI: https://doi.org/10.1016/j.array.2022.100242.

[27] M. Vidaković and K. Miličević. "**Performance and applicability of post-quantum digital signature algorithms in resource-constrained environments**.". *Algorithms*, 16(11), 2023.
DOI: https://doi.org/10.3390/a16110518.

[28] M. Kumar. "**Post-quantum cryptography algorithm's standardization and performance analysis**.". *Array*, 15(100242), 2022.
DOI: https://doi.org/10.1016/j.array.2022.100242.