Post-Quantum Digital Signatures over Finite Fields with Hidden Generators

Tuan Nguyen Kim
Phenikaa School of Computing, Phenikaa University, Ha Dong, Hanoi, Vietnam
tuan.nguyenkim@phenikaa-uni.edu.vn

Luu Hong Dung
Le Quy Don Technical University, Northern Tu Liem, Hanoi, Vietnam
luuhongdung@lqdtu.edu.vn

Hoang Duc Tho
Vietnam Academy of Cryptography Techniques, Thanh Tri, Hanoi, Vietnam
thohd@actvn.edu.vn

Ha Nguyen Hoang
University of Sciences, Hue University, Hue, Vietnam
nguyenhoangha@hueuni.edu.vn (corresponding author)

Received: 9 July 2025 | Revised: 4 August 2025 | Accepted: 22 August 2025

Licensed under a CC-BY 4.0 license | Copyright (c) by the authors | DOI: https://doi.org/10.48084/etasr.13269

ABSTRACT

The advent of quantum computers poses a direct threat to the security of traditional digital signature schemes, which are based on the Rivest–Shamir–Adleman (RSA) and Elliptic Curve Cryptography (ECC) cryptosystems. Shor's algorithm allows solving the Discrete Logarithm Problem (DLP) in polynomial time, whereas Grover's algorithm significantly reduces the effort required for brute-force attacks on symmetric hash functions and ciphers. Although many post-quantum solutions have been proposed, such as lattice-based schemes (e.g., CRYSTALS-Dilithium, Falcon) or hash-based schemes (e.g., SPHINCS+), they still have some limitations to overcome, such as large public keys, bulky signatures, high computational costs, and difficulties in integrating into existing Public Key Infrastructures (PKIs). In this paper, we propose a new type of hard problem, defined over a finite prime field, in which the generator is kept secret to prevent any direct Shor attack and is only subject to a limited influence from Grover. Based on this newly proposed hard problem, we construct a post-quantum digital signature scheme that is both Shor-resistant and Grover-resistant, secure against classical attacks, and fully compatible with current PKI infrastructures. Compared with existing post-quantum digital signature schemes, our solution significantly optimizes the size of public keys and signatures while increasing the speed of signing and verification. The newly proposed hard problem cannot be solved by known classical or quantum algorithms, thus ensuring long-term security. Performance evaluation results show that the scheme provides an optimal balance between performance and security, opening up a cost-effective implementation path for the post-quantum cryptography era.

Keywords-post-quantum digital signature; new hard problem; Shor's algorithm; Grover's algorithm; Public Key Infrastructure (PKI)

I. INTRODUCTION

The advent and continued development of quantum computers offer tremendous computational potential, yet they also pose serious challenges to current cryptographic security. The two core algorithms of quantum cryptography, Shor's algorithm [1] and Grover's algorithm [2], have demonstrated the ability to break most classical cryptographic tools. Specifically, Shor solves the Discrete Logarithm Problem (DLP) and Integer Factorization Problem (IFP) in polynomial time, fundamentally weakening Rivest–Shamir–Adleman (RSA), Elliptic Curve Cryptography (ECC), and cyclic group-based schemes; whereas Grover reduces the complexity of brute-force attacks on hash functions and symmetric ciphers from $O(2^n)$ to $O(2^{n/2})$. As a result, both traditional digital signatures and many symmetric encryption mechanisms face the risk of security breakthroughs when large-scale quantum computing becomes a reality.

To address the "quantum shock," the cryptography community has proposed a series of Post Quantum Cryptography (PQC) solutions, including: lattice-based schemes (e.g. CRYSTALS-Dilithium [3], Falcon [4]), based on the Shortest Vector Problem (SVP) or Learning with Errors (LWE); hash based signatures (e.g., SPHINCS+ [5]), taking advantage of the one-way nature of hash functions; and code-based and multivariate schemes based on the problems of correcting code errors or solving systems of polynomial equations.

Despite being standardized and evaluated, these PQC schemes often face practical problems: public keys can be tens of kilobytes in size, signatures are cumbersome, computational costs are high, and sometimes extensive changes to the existing Public Key Infrastructure (PKI) are required. This is a major obstacle to rapid deployment in real-world applications, from digital authentication and the Internet of Things (IoT) to e-banking services, where resources are limited and backward compatibility with legacy systems is necessary.

Table I compares the public key and signature sizes of traditional signature schemes (RSA, Elliptic Curve Digital Signature Algorithm (ECDSA)) with those of post-quantum signature schemes at NIST Level 1 equivalent security (~128 bits).

TABLE I. SECURITY LEVEL, PUBLIC KEY SIZE, AND SIGNATURE SIZE FOR SELECTED DIGITAL SIGNATURE SCHEMES

Scheme	Security level	Public key size (bytes)	Signature size (bytes)
RSA 2048	≈112 bit	256	256
ECDSA 256	≈128 bit	64	64
CRYSTALS-Dilithium2	NIST Level 1 (≈128 bit)	1312	2420
Falcon-512	NIST Level 1 (≈128 bit)	897	752
SPHINCS+SHA2-128	NIST Level 1 (≈128 bit)	32	7856

The data from Table I show that RSA 2048 uses a modulus of 2048 bits, so the public key and signature each occupy 256 bytes. ECDSA-256 represents the public key as two coordinates, X and Y, each 32 bytes, totaling 64 bytes. The signature is also 64 bytes long. Post-quantum NIST Level 1 schemes choose different trade-offs: CRYSTALS-Dilithium2 [6] uses a 1.3 KB key and a 2.4 KB signature; Falcon 512 requires only a 0.9 KB key and a 0.75 KB signature; SPHINCS+ [5] keeps the key as small as 32 bytes but the signature is up to 7.8 KB.

In this context, the research task is to construct a post-quantum digital signature scheme that is resistant to both Shor and Grover, while maintaining advantages in key size, computational efficiency, and compatibility with existing PKIs. We address this requirement by proposing a new type of hard problem, defined over a finite prime field F_p. The key point of the design is to keep the group generator secret, thereby preventing any direct attack using Shor's algorithm and only being marginally affected by Grover attacks.

Based on the newly proposed problem, we design a post-quantum digital signature scheme with the following properties:

- Simultaneous Shor and Grover resistance: protection against both quantum algorithm attacks and brute force attacks.
- Optimal keys and signatures: the public key and signature sizes are significantly smaller than those of standard PQCs.
- High performance: competitive signing and verification speeds, suitable for real-time applications.
- Existing PKI compatibility: no changes to the deployed digital certificate structure are required, enabling easy migration to existing infrastructures.

In summary, the advent of quantum computing has undermined the security foundation of traditional digital signature schemes, forcing the research community to develop entirely new cryptographic approaches. Although many post-quantum solutions have made significant progress, they still face obstacles such as large key sizes, low performance, and difficulty in integrating into existing PKI infrastructures. Therefore, it is necessary to explore alternative approaches, built on new mathematical problems, to create digital signatures that are both resistant to quantum attacks and meet practical operational requirements. Before introducing our digital signature scheme, the next section clarifies the threat posed by the two quantum algorithms, Shor and Grover, to schemes based on IFP and DLP.

II. QUANTUM THREATS AND RELATED WORKS

In this section, we analyze in detail the two quantum algorithms, Shor's algorithm and Grover's algorithm, whose breakthroughs undermine IFP and DLP, and we review related work that has sought to mitigate their impact on digital signature schemes.

A. *Threats Posed by Shor's Algorithm*

Shor's algorithm [1], published in 1994, marked a watershed in quantum cryptography by solving two foundational classical problems, the IFP and DLP, in polynomial time. At its core, Shor's method reduces these arithmetic challenges to a period-finding problem on a quantum computer and then employs the Quantum Fourier Transform (QFT) to efficiently determine that period.

In terms of computational complexity, the IFP with modulus N can be solved on a classical computer in $L_N[1/3]$ time (sub-exponential), whereas Shor reduces it to polynomial time $O((logN)^3)$. Similarly, Shor solves the DLP in cyclic groups also in polynomial time in the input length.

With RSA, security relies on the impossibility of factoring $N = p \times q$ when p and q are large enough. Shor breaks this assumption by finding p and q directly. With ECC, security relies on the difficulty of the DLP on elliptic curves; Shor also solves this problem in polynomial time. As a result, all RSA, ECC, and other signature schemes based on these problems lose their security once an adversary has a quantum computer with enough qubits and stability.

Therefore, there is an urgent need to develop new signature schemes that Shor's algorithm cannot exploit, namely, hard problems that cannot be reduced to an appropriate period-finding instance for the QFT. This motivates our proposal of an entirely new foundational problem over prime finite fields, in which the generator is kept secret, thereby preventing the periodic mapping step required by Shor.

B. Threats Posed by Grover's Algorithm

Grover's algorithm [2], published in 1996, is an unstructured search algorithm on quantum computers that reduces the complexity of a brute-force attack from $O(N)$ to $O(\sqrt{N})$ with a high probability of success. The most direct application in cryptography is for symmetric key systems and hash functions: instead of having to try 2^n keys, Grover only needs about $2^{n/2}$ steps, which is equivalent to halving the key length. As a result, a cipher like AES 128, which is secure against a classical attack with 2^{128} possibilities, becomes only about 2^{64} difficult on a quantum computer.

Similarly, the security of an n-bit hash function (e.g., SHA-256) degrades to $2^{n/2}$ against pre-image and collision attacks. Although Grover does not break the underlying mathematical structure as Shor does, the halving of the "bit security" still represents a serious threat: to maintain 128 bits of security, the symmetric key must be increased to at least 256 bits.

Therefore, any post-quantum signature scheme must not only resist Shor's algorithm against its public key component but also withstand Grover's impact on hash functions and symmetric elements. Our design achieves this by only slightly increasing parameter lengths to offset Grover's advantage, while keeping the overall system compact and efficient.

C. Related Works

To address the threat posed by quantum computers, many studies have focused on developing post-quantum digital signatures. The most common approach relies on established post-quantum algorithms such as lattice-based, hash-based, and code-based schemes [7]. Other research takes a different path, avoiding direct use of traditional post-quantum algorithms and instead leveraging new mathematical problems to build signature schemes that are both quantum-resistant and compatible with existing PKIs. Three representative studies are summarized below:

- The study by authors in [8] introduces a signature scheme based on the DLP hidden within a two-dimensional cyclic group. This approach offers small public keys and signatures, facilitating deployment, while leveraging the concealed group structure to increase mathematical hardness against quantum attacks. However, further evaluation of practical performance and testing against specific quantum-attack scenarios are needed to confirm its security.
- The study by authors in [9] proposes a signature scheme based on non-abelian groups, leveraging the complexity of non-commutative algebraic problems to enhance quantum resistance compared to schemes over abelian groups. This approach delivers high security and opens a new direction for post-quantum signatures, but its complex mathematical structure may pose deployment challenges and requires further analysis of performance and resilience against specific quantum attacks.
- Authors in [10] introduced a new class of post-quantum signature schemes based on group actions. This approach differs significantly from earlier group-based signatures and applies a cryptographic framework built on group actions, offering an alternative to traditional signature schemes.

Post-quantum signature schemes, despite extensive study, still suffer from large key sizes and challenging PKI integration. Conversely, "classical" approaches that avoid quantum algorithms offer better compatibility but lack thorough security and performance evaluation. This underscores the need for a new digital signature solution that is both quantum-resistant and easily deployable on existing infrastructures.

III. PROPOSED NEW HARD PROBLEM

In this section, we introduce a new hard problem designed as the foundation for post-quantum digital signature schemes. This problem can be viewed as a variant of the DLP [11], whether over finite fields or elliptic curves (Elliptic Curve Discrete Logarithm Problem (ECDLP)) [12], in which a critical parameter (the generator g in DLP or the base point G in ECDLP) is kept secret. Hiding this parameter disrupts conventional solution methods, making the problem significantly harder than the traditional DLP/ECDLP [13, 14]. We will formally define the problem, analyze its mathematical hardness, and prove its resistance against both classical and quantum attacks, including Shor's and Grover's algorithms.

A. Proposed New Hard Problem over Prime Finite Fields

Based on the DLP over the prime finite field F_p, we propose the following two new hard-problem variants. If the parameter g (the generator of the multiplicative group F_p^*, with p prime) is kept secret, the problem becomes infeasible to solve. In the simplest case, the generator g is replaced with a secret key x. The new hard problem over the finite field is then stated as follows:

- Form 1: Given a prime number p, and for each positive integer y in F_p, find an integer x that satisfies the equation: $y = x^x \; mod \; p$.
- Form 2: Given a prime number p, and for each pair of integers (a, b) in F_p, find an integer x that satisfies the equation: $a^x \equiv x^b \; mod \; p$.

It is clear that, apart from brute-force search, the standard algorithms for solving the DLP over finite fields, such as Baby-Step Giant-Step, Pollard's Rho for DLP, Index Calculus, all fail to solve this newly proposed hard problem, for the following reasons:

- Form 1: The function x^x is not linear in x, nor is it a fixed-power function, so: Pollard Rho cannot be used because it relies on the linearity of exponentiation; Baby-Step Giant-Step cannot be used because this algorithm does not have a way to generate a pre-table for the function x^x; the function cannot be decomposed into its base elements as in Index Calculus. In addition, computing the inverse of the function $x^x \bmod p$ is extremely difficult mathematically, with no obvious group structure to exploit.

- Form 2: This is the intersection equation between two exponential functions, where on the left-hand side a^x is the traditional discrete logarithm form, whereas on the right-hand side x^b is the polynomial form. In this equation, x is in both the exponent and the base, so it is not possible to isolate x on only one side as in the traditional DLP problem. Thus, the known DLP algorithms cannot be applied. In addition, since both sides of this problem depend on x in different and nonlinear ways, there is no way to convert to simple additive and multiplicative groups. That is, it has an unclear group structure, leading to the inability to apply the DLP problem in the cyclic group, because the DLP algorithms strongly depend on the group structure.

In summary, both variants of the new hard problem over finite fields are highly nonlinear, lack any explicit group structure, and cannot be reduced to the classical DLP. Consequently, no existing DLP-solving algorithm applies effectively. This novel hardness property makes the proposed problem an ideal foundation for constructing digital signature schemes with strong security guarantees, including quantum-resistant schemes.

B. Quantum Resistance of the Proposed New Hard Problem

We evaluate the quantum resistance of the proposed new hard problem based on its immunity to two prominent quantum algorithms: Shor's algorithm and Grover's algorithm.

- Resistance to Shor's algorithm for Form 1 ($y = x^x \bmod p$): Shor's algorithm can only solve problems where the unknown appears in an exponent with a fixed base, i.e., $g^x \equiv y$. In Form 1, both the base and the exponent are x, making the function $f(x) = x^x$ lack any group structure or exploitable periodicity for the QFT, rendering Shor ineffective.
- Resistance to Shor's algorithm for Form 2 ($a^x \equiv x^b \bmod p$): This nonlinear "exponential-polynomial" equation cannot be reduced to the form g^x. Since there is no quantum transformation that can extract a hidden period in such expressions, Shor's algorithm is not applicable to this hard problem either.
- Resistance to Grover's Algorithm for Forms 1 and 2: Grover's algorithm can speed up brute-force search over the range $x \in [1, p-1]$ by reducing the complexity from $O(p)$ to $O(\sqrt{p})$. However, this still represents exponential complexity. Therefore, if p is chosen to be sufficiently large (e.g., ≥ 256 bits), the proposed hard problems remain secure against Grover's attack. For instance, when $p \approx 2^{256}$, Grover's algorithm would require about 2^{128} steps, still infeasible for any practical quantum attack.

In summary, the proposed new hard problem not only inherits the complexity of the DLP and ECDLP but also enhances it by hiding a critical parameter, rendering existing algorithms, both classical and quantum, inapplicable. With its resistance to Shor's and Grover's algorithms, as well as brute-force attacks, this problem serves as a promising foundation for secure and practical post-quantum digital signature schemes. The next section presents how this problem is applied in the design of such a signature scheme.

IV. PROPOSED POST-QUANTUM DIGITAL SIGNATURE SCHEME

In this section, we employ the proposed hard problem over a prime finite field to construct a high-security digital signature scheme. The quantum resistance of the proposed scheme is also demonstrated.

A. Post-Quantum Signature Scheme over a Prime Finite Field

1) Key Generation and Parameter Setup

Algorithm 1 describes the process executed by the signer, who is responsible for generating the digital signature on message M: (i) generation of the key pair (private and public) $(x_1, x_2), (y_1, y_2)$; and (ii) generation of the other required domain parameters, p, q, with $q|(p-1)$. Domain parameters are selected according to standards such as ISO/IEC 14888-3, FIPS 186-4, or GOST R34.10-94.

```
Algorithm 1: Key Generation and Parameter Setup
Input: $L_q, L_p$
Output: $p, q, x_1, x_2, y_1, y_2$
[1] Generate $p, q$ such that $len(p) = L_p, len(q) = L_q$, and $q|(p-1)$
[2] Select $a_1$ such that $1 < a_1 < p$
[3] Compute $x_1 \leftarrow (a_1)^{\frac{p-1}{q}} \bmod p$; if $x_1 = 1$, then go to [2]
[4] Select $a_2$ such that $1 < a_2 < p$
[5] Compute $x_2 \leftarrow (a_2)^{\frac{p-1}{q}} \bmod p$; if $x_2 = 1$ then go to [4]
[6] Compute $y_1 \leftarrow (x_1)^{x_2} \bmod p$; if $y_1 = 1$ then go to [2]
[7] Compute $y_2 \leftarrow (x_2)^{-x_1} \bmod p$; if $y_2 = 1$ then go to [2]
[8] Return $p, q, x_1, x_2, y_1, y_2$
```

Here, $len(.)$ is the function that returns the bit length of an integer; L_q, L_p are the bit lengths of primes p and q; p, q are the domain parameters; and x_1, x_2, y_1, y_2 are the private and public key components, respectively.

2) Signature Generation Procedure on Message M

The signer uses Algorithm 2 to generate the signature (r, s) on the message M.

```
Algorithm 2: Signature Generation
Input: $p, q, x_1, x_2, M$
Output: $(r, s)$
[1] Generate $k$: $1 < k < q$
[2] Compute $h \leftarrow H(M)$
```

```
[3] Compute $r \leftarrow \left((x_1)^{x_2+k\times(x_1)^{-k}} \times (x_2)^{(x_1)^{-(k-1)}\times h}\right) mod\, p$
[4] Compute $n \leftarrow p \times q$
[5] Compute $s \leftarrow r \times (x_1)^k mod\, n$
[6] Return $(r, s)$
```

Here, M is a signed message with $M \in \{0,1\}^\infty$; $H(.)$ is a hash function $H: \{0,1\}^* \mapsto Z_h$ with $q < h < p$; $h = H(M)$ is the representative value (hash value) of the message M to be signed; and k is a randomly chosen value in the range $(1, q)$.

3) Signature Verification Procedure on Message M

The recipient of the signature, the verifier, uses Algorithm 3 to verify the validity of the signature on the message M. The verification expression is as follows:

$$(y_1)^{(s \bmod q)} \times (s \bmod p)^r mod\, p = (y_2)^{r\times h} \times (r)^{(s \bmod q)+r} mod\, p \qquad (1)$$

If M and the signature (r, s) satisfy (1) then the signature is considered valid, and the message is verified for origin and integrity. Otherwise, the signature is considered forged, and the message is rejected.

```
Algorithm 3: Signature Verification
Input: $p, q, y_1, y_2, M, (r, s)$
Output: True / False
[1] Compute $h \leftarrow H(M)$
[2] Compute $a \leftarrow (y_1)^{(s \bmod q)} \times (s \bmod p)^r mod\, p$
[3] Compute $b \leftarrow (y_2)^{r\times h} \times (r)^{(s \bmod q)+r} mod\, p$
[4] If $a = b$ then return True; else return
    False
```

Here, M and (r, s) are the message and its signature to be verified. If the result is True, then the integrity and origin of M are asserted. Otherwise, if the result is False, then M is denied for origin and integrity.

4) Proof of the Correctness of the Proposed Signature Scheme

We need to prove that: If $a = (y_1)^{(s \bmod q)} \times (s \bmod p)^r mod\, p$ and $b = (y_2)^{r\times h} \times (r)^{(s \bmod q)+r} mod\, p$ then $a = b$.

Indeed, if the signature and the message to be verified have not been tampered with, then:

From: $y_1 = (x_1)^{x_2} mod\, p$, $s = r \times (x_2)^k mod\, n$, and $a = (y_1)^s \times (s)^r mod\, p$, we obtain:

$$a = (y_1)^s \times (s)^r mod\, p$$

$$= (x_1)^{x_2\times r\times(x_2)^k} \times (r \times (x_2)^k)^r mod\, p$$

$$= (x_1)^{r\times(x_2)^{k+1}} \times (x_2)^{k\times r} \times (r)^r mod\, p \qquad (2)$$

From: $y_2 = (x_2)^{-x_1} mod\, p$, $s = r \times (x_2)^k mod\, n$, $r = \left((x_1)^{x_2} \times (x_2)^{(x_2)^{-k}\times(x_1\times h+k)}\right) mod\, n$, and $(y_1)^{s\times h} \times (s)^r mod\, p = (y_2)^r \times (r)^{s+r} mod\, p$, we have:

$$b = (y_2)^{r\times h} \times (r)^{s+r} mod\, p$$

$$= (y_2)^{r\times h} \times (r)^s \times (r)^r mod\, p$$

$$= (x_2)^{-x_1\times r\times h} \times \left((x_1)^{x_2} \times (x_2)^{(x_2)^{-k}\times(x_1\times h+k)}\right)^s \times (r)^r mod\, p$$

$$= (x_2)^{-x_1\times r\times h} \times (x_2)^{x_1\times(x_2)^{-k}\times h\times s} \times (x_1)^{x_2\times s} \times (x_2)^{k\times(x_2)^{-k}\times s} \times (r)^r mod\, p$$

$$= (x_2)^{-x_1\times r\times h} \times (x_2)^{x_1\times(x_2)^{-k}\times h\times r\times(x_2)^k} \times (x_1)^{x_2\times r\times(x_2)^k} \times (x_2)^{k\times(x_2)^{-k}\times r\times(x_2)^k} \times (r)^r mod\, p$$

$$= (x_2)^{-x_1\times r\times h} \times (x_2)^{x_1\times r\times h} \times (x_1)^{r\times(x_2)^{k+1}} \times (x_2)^{k\times r} \times (r)^r mod\, p$$

$$= (x_1)^{r\times(x_2)^{k+1}} \times (x_2)^{k\times r} \times (r)^r mod\, p \qquad (3)$$

From (2) and (3), we conclude that $a = b$. Thus, the correctness of the scheme is proved.

B. Resistance to Classical Attacks of the Proposed Digital Signature Scheme

In this section, we demonstrate the resilience of the proposed finite-field post-quantum digital signature scheme against two common classical attacks: secret-key compromise and signature forgery.

1) Attack on the Secret Key

An attack on the secret key typically targets the key-generation algorithm (Algorithm 1) and the signature-generation algorithm (Algorithm 2). The adversary's goal is to recover the private keys x_1, x_2 from the public keys y_1, y_2, or from a signature that has been generated on message M.

The attacker cannot recover the secret key from the public key, because in Algorithm 1, Lines 2 and 4 select two random numbers $\alpha_1, \alpha_2 \in F_p$; Lines 3 and 5 ensure that the values x_1, x_2 are not set to 1; and Lines 6 and 7 generate the public key using the nonlinear formulas $y_1 = f(x_1) mod\, p$ and $y_2 = g(x_2) mod\, p$, where f, g are nonlinear functions that cannot be reduced to a form solvable by discrete logarithms. Therefore, since no discrete logarithm operation applies, the attacker cannot derive the secret key from the public key.

The attacker also cannot recover the secret key from a signature on a message k, because in Algorithm 2, Line 1, the value k is chosen randomly in the range $(1, q)$ and Lines 3–5 generate the signature (r, s) based on the newly proposed hard problem rather than using conventional multiplication. Since the signature formula relies on this hard problem, the attacker cannot solve the equations to obtain the secret key without solving this problem.

2) Signature Forgery Attack

A signature forgery attack occurs if an adversary can produce a valid signature on a message without knowledge of the private key. Under the proposed scheme, forging a signature requires satisfying the verification condition:

$$(y_1)^{(s \bmod q)} \times (s \bmod p)^r mod\, p = (y_2)^{r\times h} \times (r)^{(s \bmod q)+r} mod\, p$$

This condition corresponds directly to the second form of the newly proposed hard problem. Therefore, an adversary would need to solve this hard problem to generate a valid signature. Since no algorithm other than brute-force is currently known to solve it, signature forgery is computationally infeasible under the proposed scheme.

C. Quantum Resistance of the Proposed Digital Signature Scheme Against Shor and Grover

As analyzed in Section III.B, the new hard problem underlying the proposed scheme is quantum-resistant. In practice, however, the security of a digital signature scheme also depends on how this problem is implemented in each step of the scheme. This section clarifies the resistance of the proposed finite-field signature scheme to Shor's and Grover's algorithms by demonstrating how each algorithmic component actively thwarts quantum attacks.

The proposed digital signature scheme is built upon a newly introduced hard problem in which the generator is kept hidden and never revealed. This design provides strong quantum resistance, particularly against two well-known quantum algorithms, Shor's and Grover's:

- Resistance to Shor's algorithm: To solve the DLP or ECDLP problems, Shor's algorithm requires the construction of a quantum oracle performing the transformation $| r\rangle \mapsto | g^r \, mod p\rangle$ in the case of finite fields, or $| r\rangle \mapsto | r \cdot G\rangle$ for elliptic curves. In the proposed scheme, the finite-field generator g is randomly generated and kept secret as part of the private key, with only $y = g^x \, mod \, p$ publicly available. This prevents an attacker from constructing the oracle $f(r) = g^r$, since g is unknown. Consequently, the scheme fully neutralizes the capabilities of Shor's algorithm, not only in theory but also at each step of the quantum procedure.
- Resistance to Grover's algorithm: Grover's algorithm accelerates brute-force search by reducing the complexity from $O(2^n)$ to $O(2^{n/2})$. The proposed scheme mitigates this threat by enforcing a minimum secret key length of $n \geq 256$, keeping the attack cost at $O(2^{128})$, which remains infeasible for any practical quantum computer. Furthermore, in Algorithm 2, a valid signature is determined not solely by the pair (r, s), but must simultaneously satisfy two independent verification equations involving two distinct keys and two hidden generators. This requires an attacker to solve two instances of the new hard problem concurrently, significantly expanding the search space and further diminishing the effectiveness of Grover's algorithm.

The scheme's resistance to Shor and Grover arises not only from the underlying hard problem, but also from its algorithmic design: the public key hides the generator, the signing and verification processes are distributed across independent parameters, no quantum oracle can be constructed for Shor, and the complex search space reduces Grover's efficiency. As a result, the scheme offers strong quantum resistance while maintaining high performance and seamless integration with existing PKI infrastructures without requiring major architectural changes.

V. DISCUSSION

The proposal in this paper represents a clear advancement in both security and performance compared to existing post-quantum schemes. However, to fully validate its practicality and security, further analysis across several related aspects is still required:

- Comparison with other post-quantum signature schemes: Current post-quantum signature schemes, such as lattice-based (CRYSTALS-Dilithium, Falcon), hash-based (SPHINCS+), and code-based (McEliece), each offer distinct advantages but also face notable limitations. The scheme proposed in this paper introduces a novel direction by relying on a new hard problem that remains secure against both Shor's and Grover's algorithms while preserving compatibility with traditional PKI infrastructures. Its key strengths include avoiding complex structures such as lattices or Merkle trees, maintaining reasonable key and signature sizes, and supporting ease of deployment, thus enabling a smoother transition to the post-quantum era.
- Comparison with ECC-based schemes: Although the two post-quantum signature schemes are built on different mathematical foundations, elliptic curves (ECC) and finite prime fields F_p, they share a common design principle: using a new hard problem with a hidden generator to thwart quantum attacks, particularly those based on Shor's algorithm. Both schemes offer strong quantum resistance, high computational efficiency, and compatibility with existing PKI infrastructures. The main distinction lies in the algebraic structure of the underlying group. The ECC-based scheme benefits from the compactness and efficiency of elliptic curve groups, making it well-suited for resource-constrained environments. In contrast, the F_p-based scheme relies on a simpler group structure, which eases implementation and auditing in conventional systems. Considering both validates the robustness of the hard problem across different platforms and broadens the scope of practical deployment in the post-quantum era.
- Performance and scalability: The proposed scheme offers two key advantages in terms of performance and scalability. First, it achieves high speed by avoiding heavy matrix operations, as in lattice-based schemes, and Merkle tree structures, as in hash-based ones. Instead, all computations rely solely on modular multiplication and exponentiation, which can be efficiently optimized on both general-purpose CPUs and embedded hardware. Second, it enables seamless integration because the public key structure resembles that of RSA/ECC, allowing plug-and-play compatibility with existing PKI infrastructures (e.g., X.509, TLS, PGP, blockchain) without requiring architectural changes. In addition, the compact signature size supports applications in smart contracts, blockchain transactions, IoT devices, and smart cards. Nonetheless, some limitations remain: the scheme has not yet been benchmarked against other PQC algorithms, and further evaluation on FPGA/ASIC

platforms is required to fully assess and optimize its performance.

- Resistance to attacks: The proposed scheme is resilient not only against Shor and Grover but also against all known classical attacks, due to two core mechanisms. First, it replaces the traditional DLP with a new hard problem in which the generator is hidden, preventing both quantum (e.g., Shor) and classical algorithms from exploiting group structure. Second, brute-force attacks require up to 2^{2n} attempts (with $n \geq 256$), making them computationally infeasible. In essence, hiding the generator is the key factor that elevates the problem's hardness and fortifies the scheme against all known attacks. Moreover, the scheme is inherently immune to lattice-specific attacks such as fault analysis on CRYSTALS-Dilithium. However, further study is needed on side-channel vulnerabilities, particularly timing and power analysis attacks when implemented on hardware. Countermeasures such as masking (hiding secret values) and blinding (randomizing inputs) should be considered to prevent leakage of sensitive information.

- Limitations and future directions: While the proposed scheme offers strong resistance against Shor and Grover attacks and retains compatibility with existing PKI systems, several aspects remain to be addressed. It lacks comprehensive experimental evaluation across diverse hardware and software platforms, and its resilience against side-channel attacks has not yet been verified. Moreover, unlike schemes such as CRYSTALS-Dilithium and Falcon, it has not undergone standardization. Future work will focus on algorithm optimization, real-world deployment in PKI, blockchain, and IoT platforms, as well as extending the design to support group and collective signatures [15]. With proper optimization and independent evaluation, this scheme has the potential to become a robust and versatile post-quantum digital signature solution.

VI. CONCLUSION

This paper introduced a new hard problem defined over a prime finite field and, based on it, proposed a post-quantum digital signature scheme resistant to both Shor's and Grover's algorithms. The scheme employs two secret keys and two public keys in the signature generation and verification process, which not only strengthens resistance against key recovery and forgery attacks but also maintains high performance and compatibility with existing Public Key Infrastructure (PKI) systems.

The analysis shows that Shor's algorithm cannot be applied to the proposed scheme, since the problem lacks the discrete logarithm structure that Shor's method requires. Grover's algorithm only shortens the brute-force attack time without breaking the scheme when the chosen parameter is large enough. The proposed scheme is also secure against classical attacks. By using a new hard problem instead of the traditional discrete logarithm, no classical algorithm can solve this problem in a feasible time. Even with the brute-force attack technique, the attacker will have to try 2^{2n} cases to find the secret key, which is almost impossible if $n \geq 256$.

In summary, we have successfully proposed a new hard problem in a finite field, which ensures the necessary security conditions to be used as a foundation to build a digital signature scheme. Therefore, the digital signature scheme built from this hard problem is not only resistant to classical attacks but also resistant to quantum attacks. This is considered a second major contribution of this study. Our study has also opened a new approach to finding quantum-resistant solutions for digital signature schemes without using quantum algorithms.

The next steps are to optimize the computational speed, test the scheme on blockchain and Internet of Things (IoT) platforms, and evaluate side-channel resistance. The results pave the way for a digital signature system that is both quantum-resistant and efficient, suitable for current and future information security infrastructures.

REFERENCES

[1] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proceedings 35th Annual Symposium on Foundations of Computer Science*, Santa Fe, NM, USA, 1994, pp. 124–134, https://doi.org/10.1109/SFCS.1994.365700.

[2] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proceedings of the twenty-eighth annual ACM symposium on Theory of Computing*, Philadelphia, PA, USA, 1996, pp. 212–219, https://doi.org/10.1145/237814.237866.

[3] L. Ducas *et al.*, "CRYSTALS-Dilithium: A Lattice-Based Digital Signature Scheme," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, vol. 2018, no. 1, pp. 238–268, Feb. 2018, https://doi.org/10.13154/tches.v2018.i1.238-268.

[4] P. Fouque *et al.*, "Falcon: Fast-Fourier Lattice-based Compact Signatures over NTRU," *Post-Quantum Cryptography Standard*, Jan. 2020.

[5] D. J. Bernstein, A. Hülsing, S. Kölbl, R. Niederhagen, J. Rijneveld, and P. Schwabe, "The SPHINCS+ Signature Framework," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, London, UK, 2019, pp. 2129–2146, https://doi.org/10.1145/3319535.3363229.

[6] J. Bos *et al.*, "CRYSTALS - Kyber: A CCA-Secure Module-Lattice-Based KEM," in *2018 IEEE European Symposium on Security and Privacy (EuroS&P)*, London, UK, 2018, pp. 353–367, https://doi.org/10.1109/EuroSP.2018.00032.

[7] A. Ali, M. a. H. Farquad, C. Atheeq, and C. Altaf, "A Quantum Encryption Algorithm based on the Rail Fence Mechanism to Provide Data Integrity," *Engineering, Technology & Applied Science Research*, vol. 14, no. 6, pp. 18818–18823, Dec. 2024, https://doi.org/10.48084/etasr.8993.

[8] D. Y. Guryanov, D. N. Moldovyan, and A. A. Moldovyan, "Post-quantum digital signature schemes: setting a hidden group with two-dimensional cyclicity," *Informatization and communication*, vol. 4, pp. 75–82, Nov. 2020, https://doi.org/10.34219/2078-8320-2020-11-4-75-82.

[9] A. A. Moldovyan, N. A. Moldovyan, D. N. Moldovyan, and A. A. Kostina, "A new approach to the development of digital signature algorithms based on the hidden discrete logarithm problem," *Information Security Questions*, no. 4 (135), pp. 45–49, 2021, https://doi.org/10.52190/2073-2600_2021_4_45.

[10] C. Battarbee, D. Kahrobaei, L. Perret, and S. F. Shahandashti, "SPDH-Sign: Towards Efficient, Post-quantum Group-Based Signatures," in *Post-Quantum Cryptography: 14th International Workshop, PQCrypto 2023*, College Park, MD, USA, 2023, pp. 113–138, https://doi.org/10.1007/978-3-031-40003-2_5.

[11] T. Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, vol.

31, no. 4, pp. 469–472, Jul. 1985, https://doi.org/10.1109/TIT.1985.1057074.

[12] I. Blake, G. Seroussi, and N. Smart, *Elliptic Curves in Cryptography*. Cambridge, UK: Cambridge University Press, 1999.

[13] G. Filippone, "On the Discrete Logarithm Problem for elliptic curves over local fields." arXiv, Apr. 27, 2023, https://doi.org/10.48550/arXiv.2304.14150.

[14] A. Abdullah, A. Mahalanobis, and V. M. Mallick, "A new method for solving the elliptic curve discrete logarithm problem," *Journal of Groups, Complexity, Cryptology*, vol. 12, no. 2, Feb. 2021, Art. no. 2, https://doi.org/10.46298/jgcc.2020.12.2.6649.

[15] K. T. Nguyen, H. N. Hoang, and D. H. Ngoc, "A New Security Enhancing Solution when Building Digital Signature Schemes," *Engineering, Technology & Applied Science Research*, vol. 15, no. 3, pp. 23613–23621, Jun. 2025, https://doi.org/10.48084/etasr.10370.