Proceedings of CONF-SEML 2026 Symposium: Computational Analysis and Modeling in Complex Intelligent Systems
DOI: 10.54254/2755-2721/2026.GU34652

An Investigation of Lattice-Based Digital Signatures and Their Aggregate Variants for Post-Quantum Security

Yiming Tong

School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing, China
b23041912@njupt.edu.cn

Abstract. With quantum computing now widely treated as a credible adversary to conventional public-key assumptions—most notably discrete logarithms and integer factorization—post-quantum cryptography has moved from a speculative research topic to an active engineering agenda. Within that broader landscape, lattice-based cryptography is routinely singled out as the leading candidate for next-generation digital signatures, largely because its security can be reduced to well-studied lattice problems believed resistant to quantum attacks. Aggregate signatures compress multiple individual signatures into a single compact object, translating into improved batch-verification throughput in settings such as blockchain and IoT. Against this backdrop, the present investigation offers a detailed analysis of lattice-based aggregate signature constructions. Core lattice notions are reviewed alongside security models, followed by an examination of two aggregation paradigms: unordered and ordered. Representative schemes are analyzed with respect to their construction logic and structural bottlenecks. A cross-scheme comparison is then used to motivate future research directions. By pulling together recent progress while isolating persistent obstacles, this investigation characterizes an ongoing shift from feasibility-oriented prototypes toward deployment-minded designs, offering a focused reference for standardization efforts targeting post-quantum-secure aggregate signatures.

Keywords: Lattice-based cryptography, Aggregate signatures, Post-quantum security, Batch verification, Fiat-Shamir with aborts

1. Introduction

Against the backdrop of credible, near-term progress in quantum hardware, conventional public-key encryption is no longer insulated by the hardness assumptions on which it has historically relied. By exploiting Shor's algorithm, a sufficiently capable quantum computer can solve integer factorization and discrete logarithm instances at speeds that render many classical security margins moot. Under these conditions, widely deployed cryptosystems, most notably Rivest–Shamir–Adleman (RSA) and elliptic-curve-cryptography (ECC) families, are confronted with a nontrivial erosion of their long-run viability. Out of that pressure has come an unmistakable shift in emphasis within the global cryptography community: post-quantum cryptography is being treated less as a purely theoretical exercise and more as an engineering target with deployment constraints that must be met. In this

© 2026 The Authors. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/).

DOI: 10.54254/2755-2721/2026.GU34652

respect, the National Institute of Standards and Technology (NIST) has occupied a central coordinating role in driving standardization forward [1].

Within post-quantum candidates, lattice-based constructions are typically set apart by one particularly consequential attribute: their security arguments can be reduced to well-studied worst-case hard problems on lattices. Two such anchor problems recur throughout this literature—Learning With Errors (LWE) and Short Integer Solutions (SIS)—and both remain resistant to known quantum attacks while also supporting comparatively efficient algorithmic instantiations. At the level of problem statements, LWE centers on distinguishing noisy linear equations from uniformly random data; SIS instead asks for a short non-zero vector lying in the kernel of a random matrix. Among the signature schemes built atop these assumptions are Dilithium and Falcon; both have been selected within NIST's standardization portfolio [1]. Existence-unforgeable (EUF-CMA) under adaptive chosen-message attacks is a fundamental security objective of digital signatures. When facing batch verification, the security model must consider key substitution attacks. In such an attack, an attacker who controls part of the public key may try to fake a valid aggregate signature containing unauthorized messages.

With the rapid development of distributed systems such as blockchain, IoT, and vehicle-to-everything (V2X), the ability to efficiently store and verify large amounts of digital signatures has become crucial. Traditional one-by-one verification methods cannot fulfill the demand for low latency and low bandwidth in such applications, so aggregate signature technology has developed rapidly. These methods significantly lower storage and transmission cost by compressing multiple independent signatures into a compact form. Aggregated signatures have become fundamental for improving system performance in limited resource environments.

In recent years, lattice-based aggregate signatures have made important progress. Boneh and Kim [2] first proposed a logarithmic-sized aggregate signature technique under the assumption of SIS, laying the theoretical basis for sublinear compression. Boudgoust and Roux-Langlois pointed out that there are limitations in the construction when aggregating Fiat-Shamir with Aborts signatures such as Dilithium [3]. Celi et al. introduced a threshold signature scheme correspond with NIST Standard Modular Digital Signature Algorithm (ML-DSA), which is beneficial to promote standardization process [4]. Deng et al. constructed an aggregate signature without certificate in the field of V2X, which can be proved secure in standard security model [5]. There are still several main problems such as the balance between security and efficiency, the inherent algebraic constraints of signature methods and the insufficient support for dynamic groups.

Comprehensively review lattice-based aggregate signature schemes, analyze key challenges facing disordered aggregation and ordered aggregation. This project is significant for promoting the standardization of post-quantum cryptography and building the digital infrastructure of the future. Sections 2 and 3 respectively discuss unordered aggregation signature techniques and ordered aggregation signature techniques. Section 4 compares and analyzes the two techniques and proposes future research directions. Section 5 summarizes the work presented in this paper.

2. Unordered aggregate signature schemes

Fig. 1 illustrates the main process of unordered aggregate signatures. During the signing phase, multiple signers independently generate signatures $\sigma_1,\sigma_2,\ldots,\sigma_n$ and send these signatures to the aggregator. The aggregator can compress multiple individual signatures into a concise aggregate signature σ_{agg} without interacting with the signers. During the verification phase, the verifier only

DOI: 10.54254/2755-2721/2026.GU34652

needs to perform a single batch verification to confirm the legality of all signatures. This method can significantly reduce storage and communication cost.

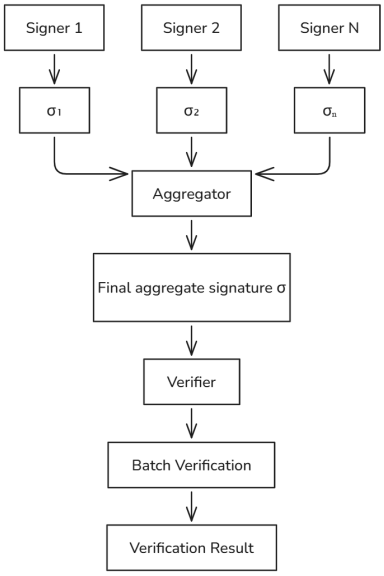


Figure 1. Process of unordered aggregate signatures (picture credit: original)

In unordered aggregate signatures, the aggregator can compress multiple independent signatures into one. The core challenge of this technology is achieving both efficient compression and resistance to key substitution attacks. Early schemes mostly used the linear homomorphic property of lattices, but it was found to have serious security problems later. Achieving a sublinear growth in aggregate signature size with the number of signatures is considered as an important theoretical breakthrough. Boneh and Kim first proposed a logarithmic size aggregation scheme based on the standard SIS assumption, which became an important milestone in the field [2]. Their defined aggregation verification algorithm, AggVerify, receives an aggregation signature σ_{agg}, a group of messages $\mu_{i\,i=1}^{n}$, and the corresponding public key vkii=1^{n}. The algorithm outputs 1 if and only if each individual signature passes verification. Its core verification is the following formula:

$$\mathrm{AggVerify}(\sigma_{agg},\{\mu_i\}_{i=1}^{n},\{vk_i\}_{i=1}^{n})=1\Longleftrightarrow\forall i,\mathrm{Verify}(vk_i,\mu_i,\sigma_i)=1 \quad (1)$$

Based on this achievement, later work continued to explore improvement in multi-message, multi-user scenarios, and developed a practical system compatible with the NIST standard signature algorithm [6, 7].

Recent research indicates that adding aggregation ability to NIST standardized signatures will face significant structural obstacles. Boudgoust and Roux-Langlois found that in signatures like Dilithium, which are based on Fiat–Shamir with abort, the commitment values must be independent and cannot be merged [3]. Direct aggregation cannot compress signatures and also leads to superlinear expansion. This result reveals the fundamental conflict between the underlying paradigm of signature and the need for aggregation. Therefore, researchers are attempting to combine lattice signatures with more advanced cryptographic tools. Tomita and Shikata combined modular lattice signatures with succinct non-interactive arguments of knowledge (SNARKs) and achieved a breakthrough in aggregating massive signatures into a very short proof [6].

DOI: 10.54254/2755-2721/2026.GU34652

Parallel to the more theory-facing literature, work has been moving at the level of deployable engineering prototypes. Using the LaBRADOR proof system, Nevado et al. explored whether Falcon signatures could be batch-aggregated in practice by recasting Falcon's verification equation as an arithmetic circuit [7]. Out of that construction comes a compact artifact: on the order of 74 KB for an aggregation covering thousands of individual signatures. Under their reported benchmarks, validating an aggregate corresponding to 10,000 Falcon-512 signatures required roughly 2.65 seconds. That latency continues to function as a binding constraint on adoption in high-frequency settings.

Alongside these general-purpose aggregation attempts, scenario-specific lattice-based aggregate-signature mechanisms have also advanced. Chen et al., for example, introduced a non-interactive identity-based multi-signature scheme grounded in lattices with the explicit aim of enabling public-key aggregation [8]. Verification is supported directly on aggregated public keys; equally importantly, multi-round interaction among signers is avoided altogether. Security can be established under the SIS assumption, and the resulting design targets constrained environments with limited resources.

In the field of V2X, Deng et al. designed a certificateless aggregate signature mechanism and completed security proofs under the standard model [5]. Compared to existing schemes that have only been proven secure under random oracle models, this technology not only effectively avoids their potential security problems, but also provides more solid theoretical support for batch verification operations.

3. Ordered aggregate signature schemes

Figure 2 illustrates the typical process of ordered aggregate signatures, such as sequential aggregate signatures. Signers participate in aggregation according to a predetermined order. The first signer generates an initial aggregate signature based on their own message. Each subsequent signer first verifies the correctness of the current aggregate signature, then merges their own signature into it to produce a new aggregate signature. After all signers have participated, the final aggregate signature σ_{final} is obtained. The verifier only needs to verify this final signature to confirm the validity of all messages in the entire signature chain. This sequential structure enables constant-size compression of signatures, but requires signers to cooperate in a fixed order.

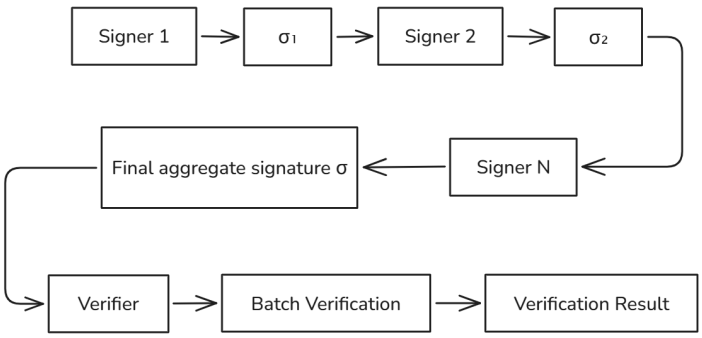


Figure 2. Process of ordered aggregate signatures (picture credit: original)

Ordered aggregate signatures, particularly sequential aggregate signatures, require signers to aggregate signatures one by one in a predetermined sequence, trading sequential constraints for

DOI: 10.54254/2755-2721/2026.GU34652

constant signature size. This process can be formalized as recursive aggregation. Let the initial aggregate signature be $\sigma^{(0)}=\perp$. For i from 1 to n, the i -th signer performs:

$$\sigma^{(i)}=\mathrm{Aggregate}(\sigma^{(i-1)},\mu_i,sk_i,\{vk_j\}_{j=1}^{i}) \tag{2}$$

and the final aggregate signature is $\sigma_{final}=\sigma^{(n)}$. The verifier only needs to verify this final signature to confirm the validity of all messages in the signature chain. Boudgoust and Takahashi constructed the first sequential half-aggregation scheme for the Fiat-Shamir with Aborts paradigm [9]. But due to the scheme's own structure, its compression ratio is very small, only about one percent.

Threshold signatures, as an important branch of ordered aggregation signatures, have made significant progress in recent years. Against the backdrop of NIST's ML-DSA standardization track, Celi et al. were the first to articulate a threshold signature scheme that is explicitly compatible with ML-DSA [4]. Six participants are supported. Per-party communication overhead is capped at no more than 1 MB during interaction. A prototype implementation was also delivered in Go, thereby moving beyond paper design into an executable system; in turn, this engineering effort supplies concrete pathways for multi-device cryptocurrency wallets as well as threshold TLS authentication. Put differently, the contribution functions as a hinge between lattice-problem-based threshold signatures as largely theoretical constructs and their subsequent standardization-facing and deployment-oriented realization.

Lin et al., by contrast, introduced a general construction framework for threshold ring signatures —General Construction of Threshold Ring Signatures (GC-TRS)—and then instantiated it via two lattice-based schemes: lattice-based threshold ring signature (LTRS) and compact threshold ring signature (CTRS) [10]. Within CTRS specifically, the signature size increases only logarithmically with respect to the number of ring members; correspondingly, computational complexity is $O(\log n)$. Rarely do such asymptotic improvements translate so directly into usability at scale; here they do, substantially strengthening both practicality and scalability for threshold ring signatures under growing membership sizes.

Over the past several years, group signatures—often treated as a canonical mechanism for ordered aggregation—have attracted sustained scholarly attention and exhibited clear methodological maturation. Chen et al. [11] introduced a lattice-based group signature construction that permits local revocation by the validator and accommodates user-controllable linkability. Under the random oracle model, complete anonymity was established alongside traceability and non-framing; on top of that cryptographic substrate, a post-quantum-secure medical data-sharing system was then built by leveraging blockchain technology. Using G-trapdoor generation as the enabling technique, Xie et al. [12] put forward an identity-based, lattice-based linked ring signature scheme. Signature generation and verification were accelerated by approximately 50%, thereby supplying an efficiency-oriented privacy-preservation route for deployment contexts such as electronic voting.

Against the backdrop of earlier, comparatively permissive formulations, Anada et al. sought to sharpen the theory's rigor. Within a more exacting security model, a synchronous aggregation signature mechanism was constructed and tight security guarantees were obtained [13]. More recently, Niu et al. introduced a lattice-based aggregation signature scheme exhibiting linear homomorphism; under the standard model, provable security can be achieved, thereby supplying stronger trust assurances for multi-source collaborative computing environments [14].

DOI: 10.54254/2755-2721/2026.GU34652

4. Comparative analysis and future directions

Latticebased aggregate signatures have broad application prospects in scenarios such as blockchain, IoT and electronic voting, but they still face several core challenges. There is still a contradiction between security and efficiency: taking LaBRADOR as an example, although its aggregate signature is compact, its verification delay is high, which may be a bottleneck in high-frequency application environments [7]. The algebraic structure of existing signature schemes brings limitations too. Studies have shown that signatures like Dilithium, based on Fiat-Shamir with Aborts, are difficult to compress during aggregation and may even lead to size expansion [3]. Most current aggregate signature schemes are designed for static groups and lack support for dynamic member changes, which is an indispensable ability in practical systems. Table 1 provides a comparison of representative lattice-based aggregate signature schemes.

Table 1. Comparison of representative lattice-based aggregate signature schemes

Scheme	Type	Core Mechanism	Aggregation Size	Advantage	Limitation
Boneh & Kim [2]	Unordered	Hierarchical authentication tree	Logarithmic	First sublinear compression	Requires multiple rounds
Boudgoust & Roux-Langlois [3]	Unordered	FSwA structure analysis	Potentially superlinear	Reveals fundamental conflict	Non-constructive
Nevado et al. [7]	Unordered	LaBRADOR + Falcon	74 KB per 10,000 signatures	Compatible with NIST standards	High verification latency
Chen et al. [8]	Unordered	Identity-based with public key aggregation	Linear	Non-interactive and certificateless	Requires key escrow
Deng et al. [5]	Unordered	Certificateless aggregation	Compact	Provably secure in standard model	Designed for vehicular networks
Celi et al. [4]	Ordered	Threshold ML-DSA	Up to 1 MB for 6 parties	Compatible with NIST standards	Limited number of participants
Lin et al. [10]	Ordered	GC-TRS framework	O(log n)	Logarithmic ring signature size	Complex construction
Chen et al. [11]	Ordered	Group signature with user-controlled linkability	Acceptable	Suitable for blockchain medical applications	Application specific
Boudgoust & Takahashi [9]	Ordered	Fiat-Shamir half-aggregation	Compression rate approximately 1%	First attempt at sequential aggregation	Extremely low compression ratio

Against the immediate constraint of standards compliance, a threshold signature construction reported as fully compatible with NIST's ML-DSA has been put forward [4], a move that materially lowers the friction associated with real-world integration. On the applied side, resource-aware designs targeting vehicular networks [5] and wireless medical sensor networks [8] indicate that lattice-based aggregation can be made to run in environments where compute, memory, and energy budgets are tight. At the level of theory, attention has pivoted to size and proof strength: logarithmic-size threshold ring signatures [10] compress communication costs at scale, while aggregation signatures proven secure in the standard model [13, 14] tighten formal assurances without leaning on random-oracle idealizations. Taken together, the literature is no longer preoccupied with whether aggregation is possible; instead, it increasingly concentrates on constructions that are efficient

DOI: 10.54254/2755-2721/2026.GU34652

enough to matter operationally while remaining secure enough to withstand rigorous scrutiny and sufficiently deployment-ready to leave prototype status.

Across the comparative literature, three trajectories recur with unusual consistency. One concerns efficiency: attention has drifted from theoretical compression ratios toward practically feasible designs, exemplified by zero-knowledge proof systems like LaBRADOR, which achieve compact signature aggregation compatible with NIST standards yet still face verification delays. A second trajectory extends signature functionality into more complex variants—threshold signatures, identity-based aggregate signatures, and linkable ring signatures—driven by blockchain, IoT, and V2X applications. The third trend shifts research focus from general constructions to aggregation support for standardized algorithms such as Dilithium and Falcon, ensuring post-quantum standards can enable efficient batch verification. Future work must balance security and efficiency by designing aggregation-friendly mechanisms that overcome structural limitations, support dynamic groups and flexible participation models, explore new signature structures for logarithmic aggregation across more scenarios, develop protocols for dynamic member changes, and drive engineering implementation to integrate aggregation into NIST-standardized post-quantum signatures, thereby unlocking the potential of lattice-based aggregation signatures in future digital infrastructure.

5. Conclusion

Against the backdrop of post-quantum threat models, this investigation surveys lattice-based digital signatures together with their aggregate counterparts. Within unordered aggregation, efficient batch verification is often attainable, yet key substitution attacks remain a central concern, and structural constraints emerge under Fiat–Shamir with aborts (FSwA). By contrast, ordered aggregation typically yields tighter signature compaction, but either sequential collaboration among signers becomes necessary, or the design retreats to static group assumptions. Over roughly the past several years, progress has been visible across standardization efforts, application-facing development work, and theory-building. Accordingly, the center of gravity has moved from "can it be done at all?" to "can it be deployed without unacceptable operational friction?", although persistent gaps remain: safety–efficiency trade-offs still resist clean resolution; dynamic participation continues to be difficult to support; and certain algebraic limitations have proven stubborn. To realize the prospective role of lattice-based aggregate signatures in future digital infrastructure, subsequent research should prioritize architectures explicitly designed for aggregation-friendliness alongside engineering-level integration pathways.

References

[1] X. Chen, J. Huang, Q. Huang, An overview of lattice-based signature and its variants supporting aggregation. J. Cryptogr. 10(1), 1-19 (2023)
[2] D. Boneh, S. Kim, One-time and interactive aggregate signatures from lattices, in Advances in Cryptology --- CRYPTO 2020, pp. 680-709 (2020)
[3] K. Boudgoust, A. Roux-Langlois, Overfull: Too Large Aggregate Signatures Based on Lattices. Comput. J. 67, 719-727 (2024)
[4] S. Celi, R. del Pino, T. Espitau, G. Niot, T. Prest, Efficient threshold ML-DSA, in Proceedings of the 35th USENIX Security Symposium, (2026)
[5] L. Deng, J. Wen, Y. Gao, N. Wang, H. Huang, S. Li, Certificateless aggregate signature scheme with security proofs in the standard model suitable for internet of vehicles. IEEE Internet Things J. 11, 28765-28773 (2024)
[6] T. Tomita, J. Shikata, Compact aggregate signature from module-lattices. IACR Cryptol. ePrint Arch. 2023: 471 (2023)

DOI: 10.54254/2755-2721/2026.GU34652

[7] D. Nevado, D. Kim, M. Stopar, Lattice-based signature aggregation: Performance analysis and benchmarks. Ethereum Research Forum (2025)
[8] X. Chen, J. Huang, K. Xiao, H. Li, Q. Huang, A non-interactive identity-based multi-signature scheme on lattices with public key aggregation. IEEE Trans. Dependable Secure Comput. 22, 4189-4199 (2025)
[9] K. Boudgoust, A. Takahashi, Sequential half-aggregation of Fiat-Shamir with aborts signatures, in Computer Security --- ESORICS 2023, LNCS vol. 14345, (Springer, 2024), pp. 270--289
[10] H. Lin, M. Wang, W. Wen, S.F. Sun, K. Liang, Generic construction of threshold ring signatures and lattice-based instantiations. Des. Codes Cryptogr. 93, 3955-4017 (2025)
[11] Y. Chen, D. He, C. Peng, M. Luo, Lattice-based group signature with user-controlled linkability and verifier-local revocation. J. Softw. 36, 4444-4460 (2025)
[12] J. Xie, L. Wang, S. Liu, J. Gao, B. Wang, Identity-based lattice-based linkable ring signature in the random oracle model. J. Front. Comput. Sci. Technol. 18, 2190-2202 (2024)
[13] H. Anada, M. Fukumitsu, S. Hasegawa, Tightly secure lattice-based synchronized aggregate signature in standard model, in Proc. ICISC 2024, LNCS, (Springer, 2024)
[14] K. Niu, M. Shi, C. Peng, et al., Linearly homomorphic aggregate signature scheme with provable security in the standard model. J. Commun. 46, 75--86 (2025)