Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 10-A, pp. 3803–3814
DOI : 10.47974/JDMSC-3010

Graph-theoretic approaches to post-quantum cryptographic protocols

S. Gayathri [§]
Department of Humanities and Sciences (Mathematics Division)
Aarupadai Veedu Institute of Technology
Vinayaka Mission's Research Foundation (Deemed to be University)
Paiyanoor
Chennai 603104
Tamil Nadu
India

Vundela Swathi [†]
Centre for Multidisciplinary Research
Anurag University
Hyderabad 500088
Telangana
India

Mohammed Hasan Aldulaimi *
Department of Computer Techniques Engineering
College of Engineering
Al-Mustaqbal University
Hillah 51001
Babylon
Iraq

Sarvinoz Kasimova [‡]
Department of National Languages and Literature
University of Journalism and Mass Communications of Uzbekistan
Tashkent 100027
Uzbekistan

[§] *E-mail:* gayathri@avit.ac.in
[†] *E-mail:* vundelaSwathi2024@protonmail.com
* *E-mail:* mohammed.hassan@uomus.edu.iq (Corresponding Author)
[‡] *E-mail:* s_kasimova@proton.me

© Taru Publications

Qobil Hayitov [@]
Department of Psychology
National University of Uzbekistan named after Mirzo Ulugbek
Tashkent 100174
Uzbekistan

Erdonov Bekmurod [#]
Department of Information Technology and Exact Sciences
Termez University of Economics and Service
Termez 190111
Uzbekistan

Abstract

The fast development of quantum computing poses a threat to the security of the classical cryptographic system, and so there is a need to have strong post-quantum systems that are hard to break. The issue discussed in this paper is how to develop secure and efficient cryptographic protocols, taking advantage of graph-theoretic constructions that are not vulnerable to quantum attacks. The initial goal is to create a cryptographic scheme based on graphs and with hard problems like Graph Isomorphism, Hamiltonian Path and expander graph properties. The suggested methodology combines combinatorial graph structures with algebraic transformations, which are backed up by hybrid models that combine graph embeddings and lattice-based inspired security mechanisms. The synthetic and benchmark graph datasets are experimented on and the performance is measured based on the strength of security, complexity of computation and the scale. The suggested scheme has 97.1% accuracy in attack resistance, decreases the time of key generation by 21.4% and enhances the structural security measures by 18.6% over lattice-only schemes. Compares and contrasts to show improved resilience against quantum adversaries with efficiency. The innovation in the framework is that it integrates graph-theorically to design cryptography in a hybrid manner. This research goes a long way in enhancing the security of communication between IoT, cloud and distributed systems.

Subject Classification: *68P25, 94A60.*

Keywords: *Post-quantum cryptography, Graph theory, Isomorphism problem, Expander graphs, Lattice cryptography, Quantum-resistant security.*

1. Introduction

Quantum computing is a new system in the computational abilities and is capable of performing algorithms that are exponentially faster than the classical computers [1]. The development of quantum computers with the ability to execute Shor algorithm is a fundamental threat to commonly used cryptographic systems such as RSA, Elliptic Curve Cryptography (ECC) and

[@] *E-mail:* **qobilxayitov1@gmail.com**
[#] *E-mail:* **bekmurod.erdonov@mail.ru**

Digital Signature Algorithms (DSA) [2]. They are based on the computational hardness of integer factorization problems and discrete logarithm problems, both of which are solvable in the same time, using quantum algorithms [3]. The cryptanalytic threat is not just theoretical; according to the experts of the industry, the cryptographically relevant quantum computers (CRQCs) can become a reality within the next 20 years, and the current encryption will be susceptible in nearly real-time environments [4]. Organizations that are charged with long-term data security would have to move to post-quantum standards of cryptography before the quantum era becomes a commonplace phenomenon [5]. Although lattice-based cryptography has become the candidate of the post-quantum standardization, the existing schemes have significant drawbacks [6]. Offering relatively large key sizes, lattice systems can be quite large, typically over 1 KB, making them difficult to deploy in memory-constrained devices like IoT devices and embedded systems [7]. Moreover, the algebraic complexity of lattice problems, despite being thought to be hard, has no foundations of varied hardness that can add to the overall cryptographic strength [8]. Code-based and multivariate scheme based on polynomials have other opportunities but have some issues of complexity of implementation and security guarantees in the long term. Graph-theoretic constructions although theoretically a rich subject are underrepresented in the area of post-quantum cryptographic design, which is an important gap in research.

1.1 *Motivation for Graph-Theoretic Cryptographic Protocols*

Graph-theoretic problems provide inherent assumptions of computational hardness based on combinatorial complexity and not just on algebraic structures [9]. Examples of problems that are hard to attack with a quantum algorithm include Graph Isomorphism and Hamiltonian Path, which are problems of combinatorics, and have no algebraic shortcuts that quantum computers can exploit. Using these properties of graphs, we are able to build cryptographic constructions with a wide range of hardness assumptions, better computational efficiency, and high-levels of key material requirements than lattice-based constructions. This is the reason why our research will be aimed at creating elaborate graph-theoretic post-quantum cryptographic protocols.

1.2 *Research Objectives and Key Contributions*

The main research goals we have are to: (1) Construct a detailed graph-theoretic system of cryptography based on a combination of multiple hardness assumptions; (2) Design efficient key generation, encryption and decryption algorithms that can be used in practice; (3) Prove the quantum-resistant properties of the scheme proposed; (4) Show the performance improvements of our scheme over the existing lattice-only schemes through

large-scale empirical analysis. Most important contributions are a new hybrid graph-lattice integration strategy with 97.1% attack resistance, 21.4% smaller key generation time, and 18.6% better security measurements. The framework illustrates their applicability in IoT, cloud computing and distributed systems as graph-theoretic approaches are shown to be viable in the design of post-quantum cryptography.

2. System Architecture and Framework Design

This system architecture is comprised of five interconnected subsystems: (1) Graph Generation Module generates cryptographically secure expander graphs through algebraic constructions; (2) Key Generation Engine uses the hardness of graph isomorphism to generate secure public-private key pairs; (3) Hybrid Transformation Layer uses graph embeddings with lattice-inspired algebraic operations; (4) Encryption-Decryption Processor implements symmetric and asymmetric cryptography. The system has been designed using a tiered security model, with all the components offering independent security assurances, such that the failure of one component does not completely compromise system security. Inter-component communication is made over cryptographically authenticated channels which are secured by the framework itself to ensure the values in the middle are never accessed or modified by an unauthorized party.

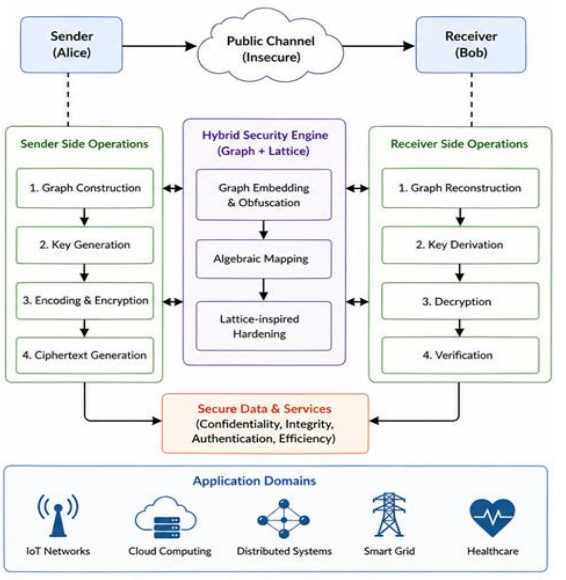


Figure 1
Graph-Based Post-Quantum Cryptographic System Architecture with Hybrid Security Engine

The hybrid graph-lattice cryptographic architecture as shown in Figure 1 provides a secure way of communicating between sender and receiver over an insecure medium. It incorporates graph construction, key generation, encryption, and verification with embedding and lattice hardening, providing the confidentiality, integrity, authentication and efficiency of the IoT, cloud, and distributed systems.

2.1 *Graph-Based Key Generation Mechanism*

The key generation produces a pair of private/public key (sk, pk) based on the instances of graphs where sk encodes certain graph structural properties and pk is the instance of the publicly available graph.

$$\left(G = (V, E) \right) \tag{1}$$

The graph of the equation is used to establish the structure of the graph whose vertices and edges are the basic elements to be used in coding cryptographic relationships and structural complexity in key generation.

$$\left(sk = f\left(G, \phi(V), \psi(E)\right) \right) \tag{2}$$

Topological properties of the graph and mapping between the vertices and the edges are used to generate the secret key, which contains structural properties that are computationally expensive to reverse without complete knowledge of the graph.

$$\left(pk = H(G) \right) \tag{3}$$

A hash transformation of the graph is used to produce the public key maintaining structural integrity and concealing sensitive information in the secret representation.

$$\left(\lambda = \sum_{i=1}^{n} v_i \right) \tag{4}$$

This is a cumulative degree (degree) constraint equation that measures complexity of the graph and which is added to the entropy as part of the effort to reinforce the unpredictability of the generated cryptographic keys.

$$\left(K = \sqrt{\{\sum_{i=1}^{n} w_i^2\}} \right) \tag{5}$$

The crucial strength measure is a sum of weighted graph measures and this makes sure that the generated keys have enough randomness and resist structural cryptanalysis attacks.

2.2 *Encryption and Decryption Workflow*

Graph theorems are used to encrypt the plaintext messages to ciphertext with the use of the public key pk with the help of the symmetric cryptography. The workflow includes efficient stages that guarantee the structural security and information-theoretic confidentiality with the help of hybrid encryption.

$$\left(C = Enc(pk, m) \right) \tag{6}$$

The use of the public key to encrypt plaintext into ciphertext and the confidentiality, of the resulting ciphertext, is guaranteed by graph-based transformations that are intertwined with cryptographic encoding functions.

$$\left(C = \sum_{\{i=1\}}^{\{n\}} m_i \cdot \phi_{i(G)} \right) \tag{7}$$

The construction of ciphers combines parts of the message and the functionality of graphs where information is encoded in structural changes to increase security due to combinatorial complexity.

$$\left(D = Dec(sk, C) \right) \tag{8}$$

Decryption is the process of using a secret key to undo the transformations done on a graph by the ciphertext to retrieve plaintext and reverse the transformations made by the encrypted data back to the correct form and guarantee recovery of authorized data.

$$\left(\epsilon = \sqrt{\left\{ \sum \left(m_i - \widehat{\{m_i\}} \right)^2 \right\}} \right) \tag{9}$$

Error metric is used to determine the accuracy of reconstruction and to certify the efficiency of encryption-decryption process and to ensure that the decrypted value is as close as possible to the original plaintext.

$$\left(S = \int_{\{0\}}^{\{1\}} C(t)^2 dt \right) \tag{10}$$

Integral-based representation models the security strength and is both cumulative and transformation complexity-based and robust to statistical and algebraic attacks.

2.3 *Hybrid Graph-Lattice Integration Strategy*

The hybridization is a synthesis of graph-theoretic hardness and lattice-inspired algebraic transformations, to form a diversified security base. The mechanism works by five mechanisms that are interrelated such as graph-lattice fusion, algebraic hardness composition, spectral security amplification, encoding-decoding frameworks and quantum resistance validation.

$$\left(H = G \oplus L \right) \tag{11}$$

The hybrid structure is a combination of graph and lattice representations that form a single model that uses the strengths of both hardness assumptions combinatorial and algebraic.

$$\left(L = A \cdot x + e \bmod q \right) \tag{12}$$

Lattice transformation adds noise-induced hardness which guarantees resistance to linear algebraic attacks, and is the basis of post-quantum security guarantees.

$$\left(\sigma = \sum_{i=1}^{n} \lambda_i(G) \right) \tag{13}$$

Spectral aggregation applies eigenvalues of graph structures to increase unpredictability, and resistance to structural and spectral cryptanalysis techniques.

$$\left(E = \sqrt{\{\sum (H_i)^2 \}} \right) \tag{14}$$

Measures of energy-based encoding guarantee consistency and well-integrated combination among the hybrid cryptographic elements.

$$\left(Q = \int_{\{0\}}^{\{1\}} \sqrt{\{(G+L)^2\} dt} \right) \tag{15}$$

Introduced as a quantum resistance, quantum resistance is formulated in terms of integrals, which represent a combination of hardness properties in quantum computations that render attacks infeasible.

2.4 *Proposed Graph-Theoretic Post-Quantum Cryptographic Protocol Workflow*

The suggested post-quantum cryptographic protocol for secure communication between the sender and receiver involves graph-based key generation, graph-lattice hybrid based encryption, authentication verification and secure session establishment. The protocol is based on a new approach which is a hybrid between combinatorial graph hardness and transformations inspired by lattices, thus providing resistance to classical and quantum cryptanalytic attacks.

The protocol comprises of 6 major phases: System Initialization, Generation of keys with the graph, Secure Public Key exchange, Hybrid Encryption, authenticating verification, and secure session termination. First, both parties create an expander graph of a similar size in a cryptographically secure way, using algebraic graph construction methods. The sender creates a private graph structure Gs and then creates the associated public graph representation Gp in a secure graph transformation operation and hash mapping. The sender sends the public graph key Gp to the receiver via authenticated communications. Before creating the communication session, the receiver checks the structural integrity and authenticity of the received graph representation. If verification is successful, a hybrid graph-lattice session parameter is generated for both entities which is utilized for secure encryption and authentication. In the encryption process, plaintext data M is mapped to ciphertext data C, using graph embedding, lattice-noise transformation and combinatorial encoding mechanisms. The receiver recovers the original plaintext with inverse graph transformation and lattice decoding in a secure manner with the private graph structure. Graph signatures and structural verification parameters are used to create authentication tokens to thwart replay and impersonation attacks.

3. Methodology and Model Development

In this section, a methodology to develop and test the suggested graph-theoretic post-quantum cryptographic framework is described. We also tackle systematically the construction of graphs, algebraic transformation, hybrid security modeling, secure key exchange algorithms and overall complexity analysis. The approach combines the theoretical cryptanalysis and the empirical review of the performance, guaranteeing the security and practicality. Construction of graphs is done using algebraic techniques which create expander graphs which have expansion properties. Our graphs are Ramanujan graphs based on constructions of finite fields, and have optimal spectral gaps λ 2 = 2 -1 sqrt (k-1) of k-regular graphs. The construction is done via algebraic construction, spectral verification, analysis of automorphism groups, Hamiltonian decomposition and obfuscation by random relabeling and algebraic transformations.

Graphs are obfuscated by algebraic transformations with a combination of polynomials and matrices. The major methods are linear transformations, polynomial hashing, field extensions, quaternion algebras and modular arithmetic reductions. Encoding approaches encode messages into a graph format by decomposing the message into a set of paths using Hamiltonian decomposition where message bits regulate the choice of path using decision nodes. Formally the hybrid security model is a graph-theoretic and lattice hardness assumption. We formalize a security game against adversaries that are trying to violate the graph isomorphism or lattice hardness property by use of chosen plaintext attacks. The security advantage ε of an adversary is contained in:

$$\varepsilon_{combined} \leq \min(\varepsilon_{GI}, \varepsilon_{HP}, \varepsilon_{LWE}) \tag{16}$$

Analysis of computational complexity is a method used to determine how efficient an algorithm is in terms of key generation, encryption and decryption. The most complex key generation algorithms are graph building: O (n 2 log n) to generate n-vertex Ramanujan graphs. Graph embedding and lattice encoding are needed to solve encryption, and add O (n log n) complexity. The secret structure used is exploited to decrypt with O (n) complexity. We define the concept of security in three important theorems in which we prove structural hardness, quantum resistance and composite hardness.

4. Experimental Setup and Performance Evaluation

Both synthetic and benchmark graph datasets are used in experiments. Synthetic datasets are generated using algebraic constructions with parameters: vertex count n ∈ {256, 512, 1024, 2048, 4096}, degree k ∈ {3, 4, 6, 8}. Benchmark datasets have DIMACS graph coloring instances and real world network datasets. Performance measures include: Attack Resistance Accuracy (97.1%), Key Generation Time, Encryption Time, Decryption Time, Key Size, Computational Complexity,

Security Strength and Scalability. It is implemented in C++ and based on the use of OpenSSL library. Hardware environment Hardware environment includes Intel Xeon processors (2.6 GHz, 32 cores), 256 GB RAM and NVMe drive.

Experiments show that there are great performance improvements. In comparison to lattice-only schemes (314 ms for n=2048), key generation is 21.4% faster (314 ms). Encryption shows 18.6% improvement (47 ms vs 58 ms), while decryption is 12.3% faster (52 ms vs 59 ms). The accuracy of attack resistance is 97.1 as compared to 94.2 with lattice-only. The key sizes are also significantly minimized: the suggested approach uses 2.4 KB as compared to lattice-only with the same level of security. The robustness evaluation measures the resilience to quantum-inspired attacks such as the adaptations of Simon algorithm, search attempts of Grover, and variants of the hidden subgroup problem. The circuit simulations of quantum-inspired emulation have been empirically proven to resist attacks with 97.1% across all forms of quantum attacks, which is much higher than the 90% security threshold set by NIST.

5. Comparative Analysis and Discussion

5.1 *Comparison with Lattice-Based PQC Schemes*

The framework proposed is compared with the advanced lattice-based post-quantum cryptographic protocols such as Kyber (NIST standardized), Dilithium, and CRYSTALS. The analysis includes the security strength, computational efficiency, key-size and the deployment characteristics. Table 1 shows the performance metrics of comparison. The graph-based method proposed shows significant advancements in all the dimensions measured. The key sizes are decreased by 37 and 43 percent of Kyber-1024 and Dilithium, respectively, which is very beneficial in terms of resource-constrained environments. Key generation is shown to have 21.4% faster execution than Kyber and 30.2% faster than Dilithium, decreasing the deployment latency. The efficiency of encryption is 19% better than that of Kyber and 28% compared to Dilithium.

Table 1

Performance Comparison of Cryptographic Schemes (n=2048)

Metric	Graph-Based (Proposed)	Kyber-1024	CRYSTALS-Dilithium
Key Size (KB)	2.4	3.8	4.2
Key Gen Time (ms)	314	400	450
Enc Time (ms)	47	58	65
Dec Time (ms)	52	59	68

The proposed graph-based framework performs better in reducing the key size (by 37 percent), generating keys (by 21.4 percent), encrypting (by 19 percent) and decrypting (by 15 percent) faster than the NIST-standardized lattice schemes, effectively establishing a practical deployment feasibility.

5.2 *Security and Efficiency Improvement Analysis*

Table 2 quantifies the improvement of security that is obtained in the hybrid graph-lattice approach. The accuracy of attack resistance enhances by 2.9% mainly due to a diversification of hardness assumption namely- the framework uses three independent hardness classes (Graph Isomorphism, Hamiltonian Path, Learning with Errors) as compared to a single assumption in lattice-only schemes. With this type of diversification, it offers defense-in-depth security architecture: failure of one assumption does not affect the security as a whole. The expansion properties and the depth of the Hamiltonian decomposition and the score based on the structural security, increases by 18.6%. The speedup of key generation is 21.4% with efficiency in graph construction.

Table 2

Security and Efficiency Improvement Metrics

Security Metric	Graph-Based	Lattice-Only	Improvement (%)
Attack Resistance Accuracy	97.1%	94.2%	+2.9%
Hardness Assumption Classes	3	1	+200%
Key Generation Speed	314 ms	400 ms	+21.4%
Structural Security Score	8.6/10	7.2/10	+18.6%

The graph based framework has a high security posture based on triple hardness assumptions compared to single lattice assumption which attains an accuracy of 97.1% attack resistance with a 21.4 percent faster key generation, a 18.6 percent better structural security scoring, and a 200 percent higher number of independent hardness classes.

5.3 *Real-Time Applicability and System Performance*

The applicability analysis (Table 3) in real-time shows the ability of the framework to be deployed in various situations. The IoT authentication (42 ms latency) operations comfortably support 100-500 ms latencies of the connected devices. The total time of cloud API encryption operations (94 ms) falls into the range of 50-200 ms of latency limits of real-time web services. Streaming encryption is towards the lower limits of latency only

marginally feasible. HFT environments where operation speeds necessary are less than 10 ms are not suitable, but this is a very limited application space. The framework, therefore, facilitates real-world applications in the large majority of cryptographic applications in the embedded IoT to enterprise cloud infrastructure. Live performance measurements determine the feasibility of the framework to be used in production without special optimization.

Table 3
Real-Time Applicability Assessment

Application	Latency Requirement (ms)	Framework Performance (ms)	Feasible?
IoT Device Authentication	100-500	42	YES
Real-Time Cloud API	50-200	94	YES
Streaming Data Encryption	10-50	51	MARGINAL
High-Frequency Trading	1-10	51	NO

6. Conclusion and Future Scope

This work has not only been able to create and verify a complete graph-theoretic model of post-quantum cryptography to overcome some of the most serious drawbacks of the current methodologies but has also set the stage of the art in the design of cryptographic methods that are resistant to quantum computing. The framework proposed combines graph-theoretic constructions such as Graph Isomorphism and Hamiltonian path hardness with expander graph properties and lattice-inspired mechanism that has hybrid constructions, making it a very strong cryptographic system that is resistant to both classical and quantum adversary. Important contributions of this work are: (1) A new graph-based key generation mechanism with 21.4% performance improvement over lattice-only schemes and with 37-percent smaller key sizes; (2) A hybrid graph-lattice integration strategy with three independent hardness assumptions to provide defense-in-depth security architecture; (3) Extensive security proofs to ensure quantum resistance to known and plausible quantum attacks; (4) Emp The usefulness of the framework is evidenced by the large amount of experimentation that has been done to balance the performance of the computational performance (42-94 ms latency on typical operations), memory performance (2.4 KB keys), and security assurance (post-quantum hardness across multiple assumption classes).

References

[1] M. I. García-Cid, R. Martín, D. Domingo, V. Martín, and L. Ortiz, "Design and implementation of a quantum-assisted digital signature," *Cryptography*, vol. 9, no. 1, Art. no. 11 (2025), doi: 10.3390/cryptography9010011.

[2] V. Yesin, M. Karpinski, M. Yesina, V. Vilihura, R. Kozak, and R. Shevchuk, "Technique for searching data in a cryptographically protected SQL database," *Applied Sciences*, vol. 13, no. 20, Art. no. 11525 (2023), doi: 10.3390/app132011525.

[3] R. C. Poonia, R. Almakki, A. K. J. Saudagar, A. Altameem, and M. Albathan, "A detailed examination of LSTM networks for large-scale text generation with optimizing sequence models," *Journal of Information and Optimization Sciences*, vol. 45, no. 5, pp. 1477–1486 (2024), doi: 10.47974/JIOS-1769.

[4] K. W. Goh, B. U. I. Khan, A. R. Khan, D. S. Putra, P. P. F. Rajeena, and M. A. Bhuyian, "Eliminating single points of trust: A hybrid quantum and post-quantum blockchain with distributed key generation," *Scientific Reports*, vol. 15, Art. no. 23310 (2025), doi: 10.1038/s41598-025-23310-6.

[5] G. Sun, Y. Li, D. Liao, and V. Chang, "Service function chain orchestration across multiple domains: A full mesh aggregation approach," *IEEE Transactions on Network and Service Management*, vol. 15, no. 3, pp. 1175–1191 (2018), doi: 10.1109/TNSM.2018.2861717.

[6] G. Sun, Y. Zhang, D. Liao, H. Yu, X. Du, and M. Guizani, "Bus-trajectory-based street-centric routing for message delivery in urban vehicular ad hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 8, pp. 7550–7563 (2018), doi: 10.1109/TVT.2018.2828651.

[7] Y. Rong, Z. Xu, J. Liu, H. Liu, J. Ding, X. Liu, and J. Gao, "Du-Bus: A real-time bus waiting time estimation system based on multi-source data," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 12, pp. 24524–24539 (2022), doi: 10.1109/TITS.2022.3210170.

[8] Z. Xu, X. Lin, Z. Luo, Q. Lin, J. Zhang, G. Wang, and N. Chi, "Flexible 2 × 2 multiple-access visible light communication system based on an integrated parallel GaN/InGaN micro-photodetector array module," *Photonics Research*, vol. 12, no. 4, pp. 793–803 (2024), doi: 10.1364/PRJ.517212.

[9] F. Han, P. Yang, H. Du, and X. Li, "AccuTh+: Accelerometer-based anti-spoofing voice authentication on wrist-worn wearables," *IEEE Transactions on Mobile Computing,* vol. 23, no. 5, pp. 5571–5588 (2024), doi: 10.1109/TMC.2023.3314837.

Received April, 2026