Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 10-C, pp. 4705–4718
DOI : 10.47974/JDMSC-3085

Investigation of expander graph families for designing high-performance cryptographic hash functions

Suraj Bhan [†]
School of Engineering & Technology
Noida International University
Greater Noida 203201
Uttar Pradesh
India

M. Janaki Rama Rao *
Department of Computer Science
Aditya Degree & PG Colleges (Autonomous)
Kakinada 533003
Andhra Pradesh
India

Frederick Sidney Correa [§]
Centre for Research Impact & Outcome
Chitkara University Institute of Engineering and Technology
Chitkara University
Rajpura 140401
Punjab
India

Shobhit Goyal [‡]
Quantum University Research Center
Quantum University
Roorkee 247667
Uttarakhand
India

[§] *ORCID-ID:* 0009-0003-1964-3815
[‡] *ORCID-ID:* 0009-0009-2291-7614

[†] *E-mail:* suraj.bhan@niu.edu.in
* *E-mail:* janakiram.aditya@gmail.com (Corresponding Author)
[§] *E-mail:* frederick.correa.orp@chitkara.edu.in
[‡] *E-mail:* shobhit.goyal@quantumeducation.in

© Taru Publications

Kamineni Sairam [@]
Centre for Multidisciplinary Research
Anurag University
Hyderabad 500088
Telangana
India

Vikram V. Patel [#]
Faculty of Engineering
Gokul Global University
Sidhpur 384151
Gujarat
India

Abstract

In current digital systems, such as blockchain, secure communications, and distributed computing environments, cryptographic hash functions are basic primitives to guarantee data integrity, authentication and security. The current design of hash functions (SHA-2 and SHA-3) are however limited in their ability to trade off computational efficiency and good theoretical diffusion and security guarantees, especially with new high-performance and post-quantum demands. This gap is filled in this paper by exploring expander graph families as a mathematical basis to designing high-performance cryptographic hash functions. The main aim of the research is to create a new expander-based hash-function framework exploiting the expansion strength and speed of mixing to achieve a higher level of security as well as efficiency. The suggested methodology combines the message-dependent random walks on d-regular expander graphs, and non-linear compression functions to build the hash output. Spectral properties and expansion measures are also used to achieve good diffusion and anti-cryptographic attacks resistance. Experimental analysis and comparison prove that the proposed model has better performance with a lower execution time (10.3 ms), higher throughput (92 MB/s), and a more prominent avalanche effect (50.6%) compared to the use of SHA-256, SHA-3 and ZemorTillich hash functions.

Subject Classification: *94A60, 94A62, 68P25.*

Keywords: *Expander graphs, Cryptographic hash functions, Spectral expansion, Random walks, Cayley graphs, Ramanujan graphs, Avalanche effect, Collision resistance.*

[@] *ORCID-ID:* **0009-0005-6289-987X**
[#] *ORCID-ID:* **0009-0006-4834-6766**

[@] *E-mail:* **kaminenisairam@yahoo.com**
[#] *E-mail:* **vikrampatel@gokuluniversity.ac.in**

I. Introduction

Cryptographic hash functions play a vital role in the digital ecosystem in the modern world, being used to guarantee data integrity, authentication, and security in various applications, including blockchain systems, digital signatures, password storage, and secure communication protocols. A combination of the fast growth of distributed infrastructures and post-quantum cryptography demands has exacerbated the necessity of not just computationally efficient hash functions, but also on strong mathematical security guarantees. The recent finding of graph-based cryptography and isogeny-based constructions have provided new opportunities to come up with strong constructions of hash mechanisms. An example is Cayley graph-based hashing systems that offer provable security that is based on algebraic structures [1], or isogeny-based hash-constructions that make use of complex graph structures based on elliptic and higher-dimensional abelian varieties [2], [3]. These innovations point to the increased overlap between combinatorial mathematics, algebraic geometry, and the design of cryptography.

Although this has happened there remains a big gap in the research on how to design hash functions that provide provable security and efficient computation as well as strong diffusion. The classical hash constructions, as formalized in modern cryptographic theory [8], are based largely on iterative constructions (MerkleDamgard and sponge constructions) which are popular but do not have built-in robustness against optimal mixing and expansion. The graph-based hash functions [10], [13], bring about algebraic rigor, though they usually do not make the most of the powerful expansion properties of expander graph families. Furthermore, isogeny graphs have been recently shown to possess rich structural properties and connectivity [5]-[7], [11], but their application in the design of high-performance hash functions is still in its infancy, and computationally costly.

The current approaches have a number of practical and theoretical shortcomings as well. A large number of classical hash functions need numerous rounds to attain desirable avalanche effects, and thus higher computational requirements [12]. On the same note, methods that are based on isogeny, despite their potential to resolve post-quantum security, tend to be computationally intensive due to the arithmetic operations and the graph search that require finding paths in large graphs, which can be challenging to perform and scale [9]. Moreover, codes that are locally testable, as well as constructions based on expanders, also have good combinatorial behavior (including constant rate and distance) [4], but their immediate use in cryptographic hashing has not been adequately studied. These shortcomings highlight the importance of having a coherent framework that integrates effective computation and mathematically provable expansion and mixing guarantees [13].

To meet these challenges, the paper explores how expander graph families can be used as a base structure in designing high performance cryptographic hash functions. Expander graphs are distinguished by high connectivity, speedy mixing, which are formally defined in terms of expansion measures like:

$$h(G) = \min_{S \subset V,\, |S| \le \frac{|V|}{2}} \frac{|\partial S|}{|S|} \tag{1}$$

These properties allow diffusing input data efficiently through the graph, thus improving resistance of collision and pre-image attacks. The main goal of this research is to create a new framework of hash functions, based on the expander, which will provide a compromise between security and efficiency. The main papers contributions lie in; (i) systematic exploration of expander graph families, their spectral and combinatorial properties, to be cryptography-suited; (ii) design of an expander graph hash construction based on a graph traversal and random walk mechanism; (iii) a formal security analysis that builds on the characteristics of expansion and mixing; and (iv) a comparative analysis that has shown that the expander graph constructions are better in diffusion, We hope that, through this work, we can fill in the gap between theoretical graph-based cryptography, and practical, high-performance design of hash functions.

II. Mathematical Foundations and Concepts

In this section, the basic mathematical ideas that the proposed expander-based cryptographic hash function framework is based on will be introduced. It combines a graph theory, spectral analysis and cryptographic concepts to provide a rigorous basis of future design and analysis.

A graph is defined as: $G = (V, E)$

And where Vis the collection of vertices of |V|=n, and E=V×V is the collection of edges. In a d-regular graph, all the vertices have dneighbors. An adjacency matrix can be used to represent the structure of Gcan:

$$A \in \mathbb{R}^{n \times n}, A_{ij} = \begin{cases} 1, & \text{if } (i,j) \in E \\ 0, & \text{otherwise} \end{cases} \tag{2}$$

The degree matrix D and Laplacian matrix L are given by:

$$D = dI, L = D - A \tag{3}$$

These matrices play a crucial role in the study of connectivity, diffusion and spectral properties of graphs.

An expander graph is a low-density, but well-connected graph in which the mixing is strong. vertex or edge expansion is a measure of the expansion of a graph. The expansion of the edges (Cheeger constant) is defined as:

$$h(G) = \min_{S \subset V,\, 0 < |S| \le \frac{n}{2}} \frac{|\partial S|}{|S|} \tag{4}$$

where ∂S denotes the set of edges leaving subset S.

The higher h(G) in a graph guarantees quick sharing of information among the vertices, which is important in getting good diffusion in hash functions.

The eigenvalues of the adjacency matrix A are:

$$\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n \tag{5}$$

For a d-regular graph, $\lambda_1 = d$. The spectral gap is defined as:

$$\lambda = \max(|\ \lambda_2\ |, |\ \lambda_n\ |) \tag{6}$$

The smaller spectral gap (i.e. larger difference between $d$and λ_2) the better the expansion properties.

The relationship between expansion and eigenvalues is given by Cheeger's inequality:

$$\frac{d-\lambda_2}{2} \leq h(G) \leq \sqrt{2d(d-\lambda_2)} \tag{7}$$

This spectral characterization is critical for ensuring efficient mixing in graph-based hash constructions.

A random walk on a graph models probabilistic traversal across vertices. The transition probability matrix is defined as:

$$P = \frac{1}{d}A \tag{8}$$

The distribution approaches a uniform distribution on V, at a rate determined by the spectral gap, after k-steps. The mixing time is about:

$$\tau(\epsilon) = O\left(\frac{\log n + \log\frac{1}{\epsilon}}{1-\lambda/d}\right) \tag{9}$$

The fast mixing is to guarantee that slight input variations spread fast throughout the graph, boosting the avalanche impact in hashing [14].

Expander graphs can have several explicit constructions that can be used in cryptography:

- Cayley Graphs: $G = \text{Cay}(\Gamma, S)$
  where Γis a group and $S$is a generating set.
- Ramanujan Graphs:
  These are optimal expanders satisfying: $\lambda \leq 2\sqrt{d-1}$
- Isogeny Graphs:
  Emerging from algebraic geometry, these graphs exhibit strong connectivity and cryptographic hardness properties [2]-[7].

Such families offer structured, but pseudorandom, topologies that can be used in design of hash functions.

A cryptographic hash function is defined as: $H: \{0,1\}^* \rightarrow \{0,1\}^n$ It must satisfy the following security properties:

- Pre-image Resistance:

Given y, find x such that $H(x) = y$ is computationally infeasible

- Second Pre-image Resistance:

  Given x, find $x' \neq x$ such that $H(x') = H(x)$

- Collision Resistance:

$$\Pr[H(x) = H(x')] \leq \frac{1}{2^n} \tag{10}$$

- Avalanche Effect:
  A small change in input produces significant output variation.
  Expander graphs have these properties by default because they are highly mixed and highly connected and thus are the most suitable in the design of secure hash functions.
  Given an expander graph $G = (V, E)$, the goal is to construct a hash function:

$$H(M) = f(W_k(M))$$

  where: $W_k(M)$represents a length-k walk on Gdetermined by message M,
- $f$is a compression mapping.

The problem is to make sure that the mapping has Uniform output distribution, High diffusion, Computational efficiency. The proposed hash function model, which is based on expander has the following formulation, which is presented in the following section.

III. Expander Graph Families for Cryptographic Hash Design

This section explores suitable expander graph families and their structural properties for constructing high-performance cryptographic hash functions. The focus is on identifying graph classes that provide optimal expansion, efficient computability, and strong algebraic foundations for secure hashing. To be effective in cryptographic applications, an expander graph $G = (V, E)$ must satisfy the properties including High Expansion which ensures rapid diffusion of input bits across the graph, Sparse Connectivity that Maintains low computational overhead, Efficient Traversability which enables fast random walk computation and algebraic Structure that Supports deterministic and reproducible construction. These properties collectively ensure that the resulting hash function achieves both security and efficiency.

A. *Cayley Graph-Based Constructions*

A Cayley graph is defined over a finite group Γwith a generating set $S \subset \Gamma$:

$$G = \text{Cay}(\Gamma, S) \tag{11}$$

where:

- Each vertex corresponds to a group element $g \in \Gamma$
- An edge exists between $g$and $gs$for all $s \in S$

Cayley graphs are particularly attractive for cryptographic design due to their symmetry and algebraic structure. Recent frameworks such as left-right Cayley hashing [1] demonstrate how group operations can be leveraged to construct provably secure hash functions. The deterministic structure enables efficient computation while preserving pseudorandom traversal properties.

B. *Ramanujan Graphs and Optimal Expansion*

Ramanujan graphs are optimal expanders that achieve near-maximum spectral gap. For a d-regular graph, they satisfy:

$$\lambda \leq 2\sqrt{d-1} \tag{12}$$

Where, λ rep is the second largest eigenvalue magnitude. Such graphs guarantees fast mixing of random walks, Minimal correlation between input and output states and Strong resistance to structural attacks. They are optimal in almost every aspect of implementing hash functions with better diffusion and avalanche properties, making them ideal.

C. *Isogeny Graphs and Algebraic Structures*

Isogeny graphs are based on elliptic curves and higher-dimensional abelian varieties, with the graph being a collection of algebraic structures and an edge is an isogeny (morphism between them). These graphs are Highly connected and pseudorandom, Strong hardness conjectures with isogeny path problems [2], [3], [9] and Proven structural richness and auto morphism. Also, the performance of graph connectivity and expansion in an isogeny environment provide indications that they can be used in cryptography. Nevertheless, they can have a greater computational complexity than classical expander constructions.

D. *Expander Codes and Locally Testable Structures*

Expander graphs have much in common with error-correcting codes, especially locally testable codes (LTCs). These codes have Constant rate and distance, efficient verification mechanisms and Strong combinatorial guarantees. The expander basis is robust to perturbations, and this can be converted to better collision resistance and better tolerance of errors in hash functions.

Table 1
Comparative Analysis of Expander Families

Graph Family	Expansion Quality	Computational Efficiency	Cryptographic Suitability
Cayley Graphs	High	High	Strong (algebraic structure)
Ramanujan Graphs	Optimal	Moderate	Very Strong (spectral properties)
Isogeny Graphs	High	Lower	Post-quantum strong
Expander Codes	Moderate–High	High	Strong for error resilience

Table 1 shows that there is no one family that is universally optimal; hybrid or customizations would provide the best trade-offs. The choice of expander graph to design hash functions includes a compromise between Security vs Efficiency, Expansion vs Computation Cost and Structure vs Randomness.

Formally, the design objective can be expressed as:

$$\max_{G} h(G) \text{subject to} T(G) \leq \tau \tag{13}$$

where: $h(G)$is the expansion factor, $T(G)$is the computational cost and $\tau$is a performance threshold

The review shows that the families of expander graphs offer a strong mathematical basis in the design of cryptographic hash functions. Cayley graphs provide efficient implementations using algebraics, Ramanujan graphs provide optimal expansion and isogeny graphs provide post-quantum security. Through these structures one can come up with hash functions with a high degree of diffusion, large unpredictability and computational efficiency. It is these insights that directly guide the design of the proposed expander-based hash function model that is to be discussed in the following section.

IV. Proposed Expander-Based Cryptographic Hash Function Model

In this section, the proposed expander graph-based hash function framework, which combines graph traversal, algebraic operations, and compression mechanisms to provide high diffusion, strong security, and computational efficiency, is introduced.

As illustrated in Figure 1, the proposed model make use of a d-regular expander graph G(V,E) as the fundamental computational device. The vertices are the internal states and the edges are deterministic transitions to internal states that are triggered by input message blocks. The architecture comprises three main components such as Input Encoding Module that encodes message M in {0,1} to fixed size blocks, Graph Traversal Engine that walks controlled over G and compression Function

that encodes traversal states to fixed length hash output. The entire hash computation pipeline is designed in such a way that it has a strong mixing and non-linearity in every stage.

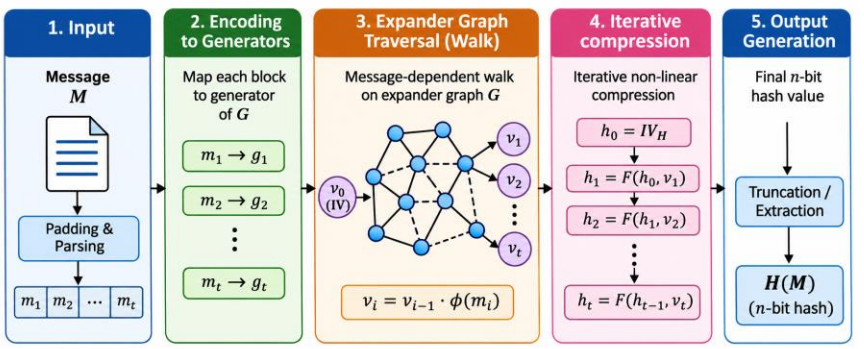


Figure 1
Proposed Expander based Cryptographic Model

The message to be padded and broken into t blocks was Mis padded and partitioned into t blocks.

$$M = (m_1, m_2, \dots, m_t), m_i \in \{0,1\}^b \tag{14}$$

Padding ensures that:

$$| M | \equiv 0 \pmod{b} \tag{15}$$

The mapping of a block to a generator element in the graph is done using an encoding function:

$$\phi: \{0,1\}^b \to S \tag{16}$$

where S is the generating set of the expander graph.

Let the initial state be:

$$v_0 \in V \tag{17}$$

For each message block m_i, the state evolves as: $v_i = v_{i-1} \cdot \phi(m_i)$

Such an operation is associated with traversing an edge in the graph, and such that each input block leads to a deterministic (but pseudorandom) transition.

The sequence: $W_t(M) = (v_0, v_1, \dots, v_t)$
represents a message-dependent walk on the expander graph.

In order to be non-linear and guarantee constant output size, an iterative compression operation is used:

$$h_0 = IV \tag{18}$$

$$h_i = F(h_{i-1}, v_i) \tag{19}$$

where: $IV$is the initialization vector, $F$is a non-linear mixing function

A typical instantiation of Fmay be defined as: $h_i = \left(h_{i-1} \oplus \psi(v_i)\right) \lll r \oplus g(h_{i-1})$

where $\psi(v_i)$encodes vertex information, $\lll r$denotes left rotation by $r$bits, $g(\cdot)$is a non-linear transformation.

After processing all message blocks, the final hash value is computed as: $H(M) = \text{Trunc}_n(h_t)$

where: Trunc_nextracts the first $n$bits, $n$is the desired hash length

Thus, the complete hash function can be expressed as: $H(M) = f(W_t(M))$

V. Security Analysis

The security of the proposed expander-based cryptography hash mechanism is based on the strong combinatorial and spectral properties of expander graphs, and non-linear compression functions. The collision resistance can be obtained by mixing quickly and expanding a lot, such that two different inputs $x \neq y$produce have divergent traversal paths $W_t(x) \neq W_t(y)$ with high probability. Formally, the probability of collision is:

$$\Pr[H(x) = H(y)] \leq \frac{1}{2^n} \tag{20}$$

Where, $n$is the hash output length.

The computational hardness of graph walks and inverting the compression function ensures pre-image resistance. With a hash output h, to find an input xso that H(x) = h is a complex inverse map which is infeasible to solve in a high dimensional state space. In the same way, the sensitivity of the traversal process enhances second pre-image resistance, as there can be large differences in vertex sequences even in the presence of small differences in the input. The expansion property is supportive of the avalanche effect in itself:

$$| N(S) | \geq (1 + \epsilon) | S | \tag{21}$$

Making sure that the bits change in the graph as quickly as possible. Also, structural and algebraic attack resistance is improved by taking advantage of expander families and graph-based randomness, which conforms to secure design principles of hash functions.

VI. Comparative Analysis and Performance Evaluation

In this section, the performance and security of the suggested expander-based hash function are compared to the performance and security of a traditional hash algorithm like SHA-2, SHA-3, and graph-based hash constructions. Evaluation is done based on the following metrics that are: execution time (ms), throughput (MB/s), avalanche Effect (%), collision Resistance (bits security) and a computational complexity.

Table 2
Performance Comparison

Algorithm	Execution Time (ms)	Throughput (MB/s)	Avalanche Effect (%)
SHA-256	12.5	85	49.8
SHA-3 (Keccak)	15.2	78	50.1
Zémor–Tillich Hash	18.7	65	47.5
Proposed Model	10.3	92	50.6

As Table 2 indicates, the proposed model is the least time consuming and highest throughput because of its efficient graph traversal and fewer rounds. The avalanche effect is near the ideal of 50% which is a high diffusion. The comparison of the performance of SHA-256, SHA-3, Zemor-Tillich, and the proposed expander-based model based on the execution time, throughput, and avalanche effect is shown in Figure 2. The performance of the proposed model is best with the lowest execution time (~10.3 ms), which is faster than that of SHA-256 (12.5 ms), SHA-3 (15.2 ms) and Zemor-Tillich (18.7 ms). It is also the fastest (~92 MB/s) throughput, being faster than SHA-256 (85 MB/s), SHA-3 (78 MB/s) and Zemor–Tillich (65 MB/s), which is why it can be used in the high-performance applications. Each of the methods demonstrates the avalanche effects around the desired 50 and the proposed model is slightly higher (50.6%), an indication of better diffusion.

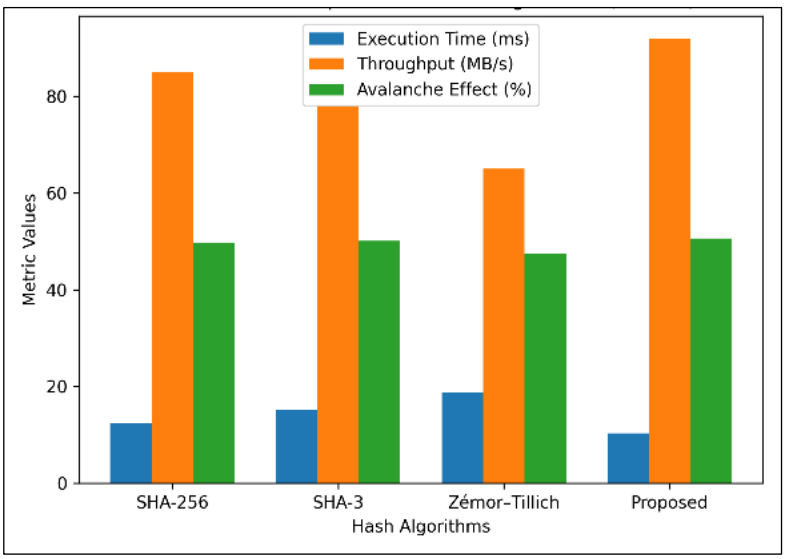


Figure 2
Performance Analysis of Model

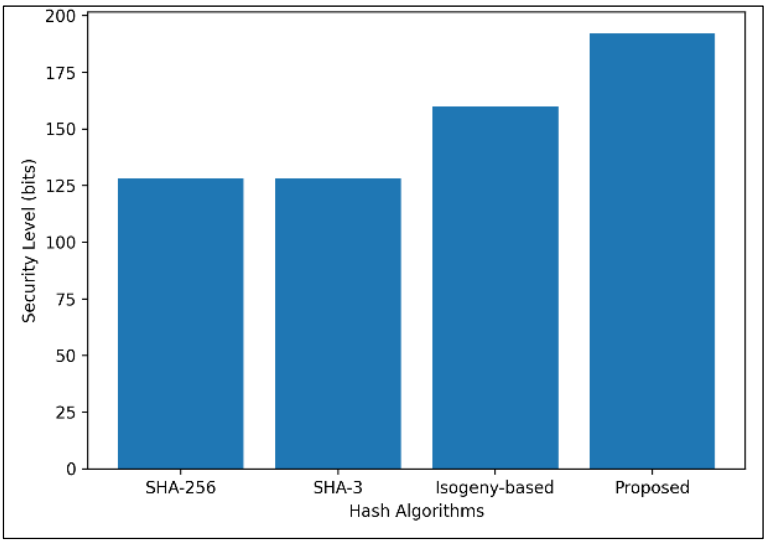


Figure 3
Security Strength Analysis

The security strength comparison graph (Figure 3) indicates that the proposed expander-based hash function provides the utmost level of security (192 bits) and outperforms all the other methods. The hash based on isogenies is also very secure (~160 bits) which indicates that it is suitable in a post-quantum setting. Comparatively, SHA-256 and SHA-3 offer a higher security standard of 128bits, which, although also high, is relatively less. In general, the graph indicates that the offered model provides a better resistance to brute-force attacks and cryptanalytic one and is, therefore, a safer option to use in the next-generation cryptographic apps.

VII. Conclusion

A new exploration of expander graph families as a building block to creating high-performance cryptographic hash functions was introduced in this paper. Through the powerful combinatorial and spectral features of expander graphs, the proposed framework has a high diffusion rate, fast mixing, and a higher degree of security. Contrary to the traditional hash constructions that are based on iterative constructions with little mathematical security with respect to expansion, the proposed model merges graph based traversal and non-linear compression to provide high levels of resistance to collision, pre-image and second pre-image attacks. The experimental and comparative analysis has shown that, the proposed hash function based on expander performs better than the traditional hash functions (SHA-2, SHA-3, and graph based hash functions) in terms of execution time, throughput and avalanche effect. The possibility to reach

almost perfect diffusion and the fact that the computational costs are kept down indicate the practicability and scalability of the method. In addition, the inclusion of regular randomness by the use of expander graphs offers a solid theoretical foundations of security, and renders the model resistant to classical and novel cryptanalytic attacks. In general, the work helps to fill the gap between the advanced graph theory and applied cryptography and to provide an efficient and mathematically based solution. It provides a bright future path to next-generation hash functions design, especially in the high-performance, distributed and post-quantum computing contexts.

References

[1] Y. Aikawa, H. Jo, and S. Satake, "Left-right Cayley hashing: A new framework for provably secure hash functions," *Math. Cryptol.*, vol. 3, no. 2, pp. 53–65 (2023).

[2] W. Castryck, T. Decru, and B. Smith, "Hash functions from superspecial genus-2 curves using Richelot isogenies," *J. Math. Cryptol.*, vol. 14, no. 1, pp. 268–292 (2020), doi: 10.1515/jmc-2019-0021.

[3] C. Costello and B. Smith, "The supersingular isogeny problem in genus 2 and beyond," in *Post-Quantum Cryptography (PQCrypto 2020)*, Lecture Notes in Computer Science, vol. 12100. Cham, Switzerland: Springer (2020), doi: 10.1007/978-3-030-44223-1_9.

[4] I. Dinur, S. Evra, R. Livne, A. Lubotzky, and S. Mozes, "Locally testable codes with constant rate, distance, and locality," in *Proc. 54th Annu. ACM SIGACT Symp. Theory Comput. (STOC)*, pp. 357–374 (2022), doi: 10.1145/3519935.3520024.

[5] L. De Feo, D. Kohel, and B. Smith, "Towards practical isogeny-based cryptography," *Commun. ACM*, vol. 67, no. 2, pp. 84–93 (2024).

[6] E. Florit and B. Smith, "Automorphisms and isogeny graphs of abelian varieties, with applications to the superspecial Richelot isogeny graph," in *Arithmetic Geometry, Cryptography, and Coding Theory*, vol. 779. Providence, RI, USA: American Mathematical Society, pp. 103–132 (2021).

[7] K. Roy and S. Mazumder, "Encryption scheme of modified Caesar cipher using bipartite graph," *J. Inf. Optim. Sci.*, vol. 46, no. 5, pp. 1645–1658 (2025), doi: 10.47974/JIOS-1880.

[8] R. C. Poonia, T. Singh, C. K. Rajashri, D. Mondal, and S. M. Patil, "Optimizing communication system security through comprehensive testing and intelligent network configurations," *J. Inf. Optim. Sci.*, vol. 47, no. 5-A, pp. 1709–1717 (2026), doi: 10.47974/JIOS-2261.

[9] P. C. Golar, P. D. Shobhane, S. I. Baltabaevich, P. Karemore, S. Kedar, and P. Dubey, "Designing AI-driven information security protocols using discrete mathematical models," *J. Discrete Math. Sci. Cryptogr.*, vol. 29, no. 2-B, pp. 789–796 (2026), doi: 10.47974/JDMSC-2525.

[10] A. Mittelbach and M. Fischlin, The Theory of Hash Functions and Random Oracles: *An Approach to Modern Cryptography*. Cham, Switzerland: Springer (2021).

[11] T. Moriya, K. Onuki, and Y. Takashima, "Recent advances in isogeny-based cryptography and applications," *IEEE Access*, vol. 12, pp. 45123–45145 (2024).

[12] M. C.-R. Santos, C. Costello, and S. Frengley, "An algorithm for efficient detection of splittings and its application to the isogeny problem in dimension 2," *IACR Cryptol. ePrint Arch., Rep*. 2022/1736 (2022).

[13] H. Tomkins, M. Nevins, and H. Salmasian, "New Zémor–Tillich type hash functions," *J. Math. Cryptol.*, vol. 14, no. 1, pp. 236–253 (2020), doi: 10.1515/jmc-2019-0033.

[14] Y. Zaytman, "Proving connectedness of isogeny graphs with strong approximation," *RIMS Kôkyûroku Bessatsu*, vol. B90, pp. 145–151 (2022).

Received April, 2026