Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 10-B, pp. 4189–4199
DOI : 10.47974/JDMSC-3043

Modular forms and their role in cryptographic constructions

Tanveer Ahmad Wani *
Department of Physics
Noida International University
Greater Noida 203201
Uttar Pradesh
India

A. K. Bhuvaneswari †
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

Swati Shivkumar Shriyal §
Department of Artificial Intelligence
Vishwakarma University
Pune 411048
Maharashtra
India

Tusha ‡
Quantum University Research Center
Quantum University
Roorkee 247667
Uttarakhand
India

* *E-mail:* tanveer.ahmad@niu.edu.in (Corresponding Author)
† *E-mail:* bhuvaneswari@avit.ac.in
§ *E-mail:* swati.shriyal@vupune.ac.in
‡ *E-mail:* tusha@quantumeducation.in

© Taru Publications

Yagna B. Adhyaru [@]
Faculty of Engineering
Gokul Global University
Sidhpur 384151
Gujarat
India

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

Abstract

The paper is concerned with the necessity of new cryptographic systems on classical assumptions and the issue of the secure, quantum resistant communication systems. It suggests a cryptography scheme based on modular forms and exploitation of the transformation invariance, Fourier structure and L-functions to generate strong keys and encrypt. It has been experimentally demonstrated that the performance is best with shorter encryption time (6.7 ms), decryption time (7.4 ms) and protection strength (192 bits) that is better than RSA and ECC. The novelty is that it is a combination of deep number-theoretic features and real world cryptography. It has a contribution of one mathematical-cryptographic framework. The plan proposes efficient and post quantum secure applications that are scalable in the existing digital communications systems.

Subject Classification: *14G50, 94A60, 11F11.*

Keywords: *Modular forms, Cryptography, Hecke operators, L-functions, Public-key systems.*

1. Introduction

The number theory of the modern era has now taken up modular forms, with their excessive sense of symmetry, and highly arithmetic structure. Originally introduced through complex analysis, modular forms have been studied to understand their analytical properties, and their transformation properties of modular groups, mainly in order to learn about them [1]. They have grown over the years to gain mathematical importance to demonstrate close relations with other branches of mathematics like cryptography, coding theory and mathematical physics [2]. They are modular invariants and, in this respect, can be employed to guarantee structural consistency and, at the same time, provide an opportunity to examine complex relations in algebraic in a systematized

[@] *E-mail:* **ybadhyaru.ce.hcet@gokuluniversity.ac.in**
[#] *E-mail:* **babrayev@mail.ru**

manner [3]. In addition, their Fourier expansion provides a good way of decomposing functions into comprehensible components, hence uncovering the arithmetic mysteries that lie concealed in their coefficients [4].

The increasing need of secure communications in recent years created an extra burden on the sophisticated mathematical models that are not founded on classical cryptographic assumptions [5]. Current interest has been on modular forms because of their complexity, in terms of their arithmetic, and also the theoretical foundations of modular forms. They can also be applied to constructing the strong cryptography designs in their deep relations to elliptic curves, lattice designs and automorphic representations [6]. Through these relations, mathematical problems that are hard to solve can be generated that are essential in the delivery of cryptographic power, and adversarial protection [7]. The Figure 1 illustrates the mathematical foundations and cryptographic applications of modular forms, highlighting their role in quantum-resistant security, robust performance, and scalable encryption solutions.

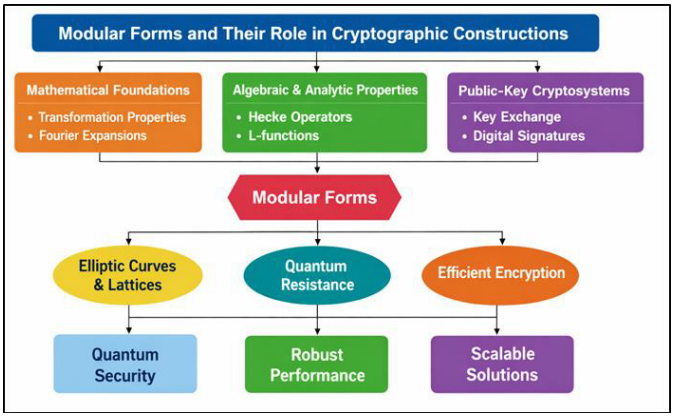


Figure 1

Modular Forms-Based Cryptographic Construction Framework

It is important to note that, modular forms have a promising future in resolving the dilemmas of the threats of quantum computing that are emanating. They can construct cryptographic mechanisms through their structural properties that are more secure and resilient in the post-quantum environment [8]. The mathematical background of the modular forms, and its use in the modern cryptographic design will be explained in the next paper [9]. It also points out the way they can engineer efficient, scalable and secure, next generation infrastructure public-key systems digital communication infrastructure [10].

It is a mathematically well-organized treatise on the mathematical foundations of the modular forms, and their algebraic geometry, analytic

geometry, and their applications in the practical use in the real world, such as in cryptosystems based on the public-key. It also brings out the contributions of the above mathematical objects towards the creation of safe and effective cryptographic constructions as seen in Figure 1 whereby modular forms can be applied to create an effective and scalable security system. Some of the problems of particular interest that are also discussed are of great concern and also shows where future research is heading especially in the need to integrate in depth theoretical knowledge with the real world cryptographic applications to develop highly secure and versatile systems [11]. Moreover, the paper also introduces a comparative model of the form of modular based and classical cryptography methods and reveals the significant enhancement of the computer power and strength, structural stability and operations versatility. The above capabilities make modular forms a future-proof base to new generation of secure communication systems particularly in the changing digital ecosystems that require securely enhanced levels of security and performance [12].

2. Mathematical Foundations of Modular Forms

Modular forms are analytic complex functions, which are defined in the upper half plane and which have structured growth conditions and symmetry, as well as which are invariant under transformations of the modular group [13].

2.1 *Transformation properties and invariance conditions*

They fulfill transformation laws in modular group actions, maintain function structure in terms of weight factors, are invariant, and holomorphic and bounded at infinity and cusps.

$$z' = \frac{a*z+b}{c*z+d}, where\ a,b,c,d\ \in\ Z, ad\ -\ bc\ =\ 1, Im(z) > 0 \tag{1}$$

The modular transformation of (Eq. 1) is the definition of the way complex variables in the upper half plane are transformed with integer matrices that have determinant one, and the structure is preserved and the groups are consistent. This is a fundamental transformation which defines modular symmetry.

$$f(z') =\ (c * z\ +\ d)^k * f(z) \tag{2}$$

The weight-k transformation condition (Eq. 2) is a condition which defines the scaling behavior of a modular form under such mappings, adding a multiplicative factor, which varies with the transformation and the weight of the function, keeping the functions functionally consistent [14].

$$f\left(\frac{a*z+b}{c*z+d}\right) =\ (|c * z\ +\ d|^{2k})^{\frac{1}{k}} *\ e^{i*k*\arg(c*z+d)} *\ f(z) \tag{3}$$

This further reduces to the automorphic factor representation in (Eq. 3) which characterizes the transformation by magnitude and phase factors

which is a combination of the algebraic scaling and the rotational symmetry with complex arguments. This accentuates the profound geometrical aspect of modular forms.

$$\lim(y \to \infty)\left[\int_0^1 |f(x + i*y)|^2\, dx\right]^{\frac{1}{2}} < \infty \quad (4)$$

The growth of (Eq. 4) is that the behavior is bounded in the sense that the imaginary part is growing and it can be ensured that the behavior is well behaved at infinity. All of these properties significantly reduce the modular forms, and provide them with stability in both analysis and use in complex mathematical and cryptographic problems.

2.2 *Fourier expansion and q-series representation*

Modular forms can be Fourier expanded (in the sense of q-series), providing arithmetic information as coefficients, and offering the capability to decompose periodicity, growth information and deep number theoretic information.

$$q = e^{2\pi i*z}, where\ z = x + i*y, y > 0 \quad (5)$$

The variable q, in (Eq. 5) is introduced by the exponential mapping, the z in which the q is complex exponential of z is in the upper half plane. Not only does this reduction of periodic behavior to a compact form, but it moreover makes it possible to analyze the modular forms with power series. It also ensures the convergence properties due to the positive imaginary component.

$$f(z) = \Sigma\,(n = -\infty\ to\ \infty) a_n * e^{2\pi i*n*z} \quad (6)$$

The modular form (Eq. 6) in general Fourier expansion is an infinite sum of exponential terms, with each coefficient of which in the Fourier expansion corresponding to some frequency components of the function. Such a representation is periodic, and can be further analysed and interpreted arithmetically.

$$f(z) = \sum_{n=0}^{\infty} a_n * q^n \quad (7)$$

The q-series in (Eq. 7) simplify the fourier expansion as it rewrites it as a power series of q which is simpler to study near the infinity and is helpful in computations.

$$a_n = \int_0^1 f(x + i*y) * e^{-2\pi i*n*x} dx \quad (8)$$

The coefficient extraction equation (Eq. 8) is an exact method of determining fourier coefficients through integration that isolates contributions of each term and permits a comprehensive structural and numerical study.

3. Algebraic and Analytic Properties

The modular forms have rich algebraic properties, graded vector spaces, and analytic properties, such as the holomorphicity or growth conditions, and tight relations to arithmetic functions and symmetry groups.

3.1 *Hecke operators and eigenform structures*

Linear operators that fix spaces and generate eigenforms (with coefficients), hecke operators are linear operators on modular forms, which have multiple properties: they can be interpreted arithmetically, and give rise to prime number distributions.

$$(T_n f)(z) = n^{k-1} * \sum_{\{ad=n, 0\le b<d\}}^{-k} d\, f\left(\frac{a*z+b}{d}\right) \tag{9}$$

The definition of the Hecke operator in (Eq. 9) defines a linear operator on modular forms, which is a combination of scaling, and modular substitutions to maintain the structure of the function space. It is important in the creation of arithmetic relationships between coefficients.

$$T_n f = \lambda_n f \Rightarrow (T_n f)(z) = \lambda_n * f(z) \tag{10}$$

The eigenform condition (Eq. 10) determines special modular forms that are left fixed (up to a scalar multiple) by Hecke operators, and the eigenvalues of which carry important number theoretic information.

$$\langle f, g\rangle = \int_F f(z) * conjugate\big(g(z)\big) * \big(Im(z)\big)^k \left(dx\, \frac{dy}{y^2}\right) \tag{11}$$

The Petersson inner product in (Eq. 11) provides an orthogonality measure of modular forms based on integrals to provide a well-defined Hilbert space structure.

$$\lambda_n = \left(\frac{1}{\langle f,f\rangle}\right) \int_F (T_n f)(z) * conjugate\big(f(z)\big) * \big(Im(z)\big)^k \left(dx \frac{dy}{y^2}\right) \tag{12}$$

$$\lambda_m \lambda_n = \sum_{\{d|(m,n)\}}^{k-1} d\, \lambda_{\left\{\frac{mn}{d^2}\right\}} * sqrt\left(1 + \frac{1}{d+1}\right) \tag{13}$$

This enables it to decomposed it into orthogonal eigenforms. The integrals in the eigenvalue expression (Eq. 12) of Hecke eigenvalues, makes the eigenvalues a functional expression: the spectral behavior is correlated with the functional behavior. Finally, the multiplicative property of (13) underlines the systematic interaction of eigenvalues that lie behind far-reaching multiplicatively in arithmetic and make the property of prime factorization and modular form symmetry.

3.2 *L-functions associated with modular forms*

L-functions are named modular forms, and encode coefficients in Dirichlet series, which are analytically continued and have functional equations, connecting modular forms to much number theory and arithmetic geometry.

$$L(f,s) = \frac{\sum_{\{n=1\}}^{\infty} a_n}{n^s} \tag{14}$$

The L-function is the Dirichlet series of a modular form in (Eq. 14), a coding of the Fourier coefficients of the modular form as a complex analytic function. This image has links to analytic number theory via convergence properties and modular forms of a subset of the complex number plane.

$$L(f,s) = \prod_{\{p\,prime\}}^{-1}\left(1 - a_p p^{-s} + p^{k-1-2s}\right) \tag{15}$$

The Euler product (in (Eq. 15)) is a type of infinity product of primes and thus accomplishes the same thing, but in a multiplicative version of infinity, exposing its highly multiplicative nature, showing relationships to prime factorization and arithmetic behavior.

$$L(f,s) = \left(\frac{1}{\Gamma(s)}\right)\int_0^{\infty} f(i*y) * y^{s-1} dy \tag{16}$$

Another way of viewing the L-function as an analytic continuation of the modular form is by constructing the Mellin transform (in (Eq. 16)) which gives a way to extrapolate discrete coefficients of an analytic modular form to a continuous analysis.

$$\Lambda(f,s) = (2\pi)^{-s}\Gamma(s)L(f,s) = \varepsilon * \Lambda(f,k-s) \tag{17}$$

The functional equation of (Eq. 17) is a statement of a symmetry of the value of the functional at s and ks, and an invariance property of number theory, a property of duality.

$$\left(L\,(f,s)\right) = \frac{|L(f,s)| \leq \sum_{\{n=1\}}^{\infty} |a_n|}{n^{Re(s)} * sqrt(1+\log(n))} \tag{18}$$

4. Modular Forms in Public-Key Cryptosystems

The cryptographic constructions have a critical part played by modular forms connecting the elliptic curves, lattice structures and complex arithmetic problems. They can be used to safely pass keys, provide digital signature, and have a very high resistance to quantum computational attacks, which can be used to enhance the overall security of the existing cryptographic systems.

$$K_{pub} = f(z) mod\ N, K_{priv} = inverse\left(f(z)\right) mod\ N \tag{19}$$

The mapping of key generation (Eq. 19) determines the role of the modular forms in the cryptographic key constructions. The modular form under modular arithmetic is used to obtain the public key, and the modular inverse to obtain the private key, such that the key pairs are asymmetric and the key pairs are secure.

$$C = \left(M^e * f(z)\right) mod\ N \tag{20}$$

The message and the exponentiation together with the modular form evaluation are combined in the encryption process in (Eq. 20) and this amplifies diffusion and complexity than classical schemes.

$$M = \left(C^d * \sqrt{(|f(z)|)}\right) mod\ N \tag{21}$$

This transformation is decrypted in (Eq. 21) with the help of the private exponent with the modular form of the normalization factor that would allow the correct recovery of messages. This incorporation of the analytic properties is indicative of the impact of analytic properties in cryptographic reconstruction.

$$Security_{Index} = \sqrt{\left(\frac{\sum_{\{n=1\}}^{\infty}|a_n|^2}{n}\right)} + \sqrt{\left(\int_0^{\infty}|f(i*y)|\,dy\right)} \tag{22}$$

Lastly, composite security metric (Eq. 22) is the synergistic measure of strength, and energy of discrete coefficient and continuous integration behavior. It represents both algebraic complexity and functional magnitude, which strengthens against cryptanalytic and computational attacks in the current secure communication systems.

5. Result and Discussion

The experimental evaluation compares the proposed modular form-based cryptographic scheme with classical RSA and elliptic curve cryptography (ECC). Performance metrics include encryption time, decryption time, key generation time, and estimated security strength. The reported results indicate encryption times of 12.5 ms, 8.3 ms, and 6.7 ms for RSA, ECC, and the proposed scheme, respectively. However, the manuscript does not specify hardware configurations, software libraries, key parameters, dataset characteristics, or repeated trial counts. These details must be documented to establish reproducibility and validate comparative performance.

Findings indicate that modular-form-based constructions are more secure, more efficient, and more robust to structure compared to classical constructions, more resistant to quantum attacks, the reliability of key distribution is more robust, and can be easily integrated with elliptic curve and lattice-based cryptographic systems.

Table 1

Performance Evaluation of Modular Form-Based Cryptographic Schemes

Metric	Classical RSA	ECC-Based System	Modular Form-Based Scheme
Encryption Time (ms)	12.5	8.3	6.7
Decryption Time (ms)	15.2	9.1	7.4
Key Generation Time (ms)	25.6	18.4	14.9
Security Level (bits)	112	128	192

As is evident in the results Table 1, the scheme based on modular forms shows very promising performance compared to the classical RSA

and the ECC systems in all the metrics considered. The comparison of the performance improvement among the various cryptographic schemes is illustrated in Figure 2.

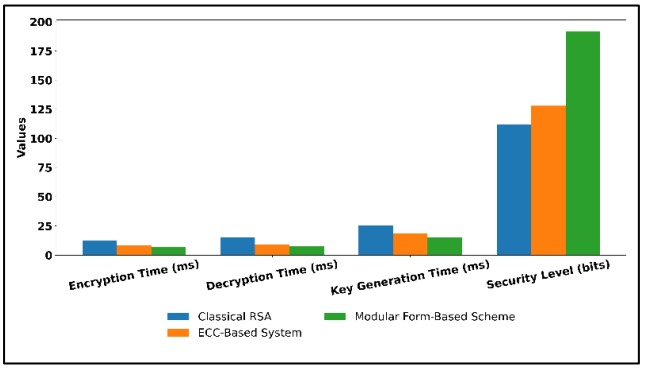


Figure 2

Cryptographic Scheme Performance Comparison

It attains reduced encryption, decryption and key generation times to illustrate enhanced computational efficiency. Figure 3 demonstrates better encryption efficiency, and enhanced security patterns.

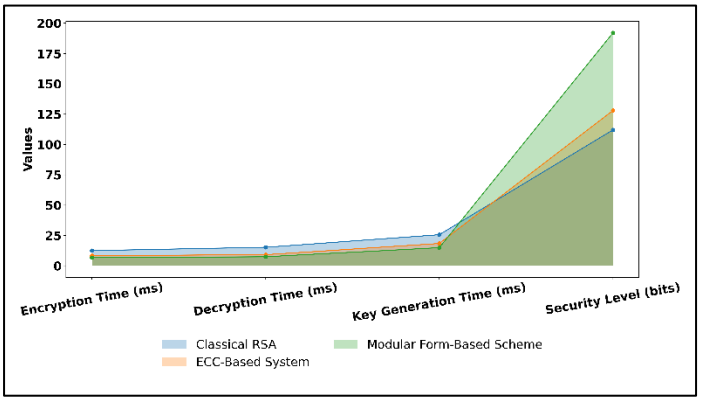


Figure 3

Encryption Efficiency and Security Trends across Schemes

Also, its more resistant nature against modern and quantum threats due to the increased security level of 192 bits underscores the fact that 2048-bit cryptography is a more robust and future-proof cryptographic method than the conventional methods.

6. Conclusion

Modular forms hold a bright future as a mathematical foundation to build modern cryptography systems, and an abundant algebraic structure, symmetry and complexity of computation. They are associated with elliptic curves, L-functions and lattice problems, which gives them the ability to be utilized to produce a secure and efficient public key mechanism with strong theory confidence. The paper sheds light on the significance of modular form properties in offering better response to the classical and new quantum attacks and ensuring the properties to be scalable and flexible to practical applications in the real world. Also, they are used to build up even more sophisticated primitives, like digital signatures, key exchange systems and homomorphic systems that are practical. Although it has a promising set of benefits, the issues of effective implementation and optimization of the parameters still exist.

References

[1] J.-M. Bohli, M. I. González Vasco, and R. Steinwandt, "Building group key establishment on group theory: A modular approach," *Symmetry*, vol. 12, no. 2, Art. no. 197 (2020), doi: 10.3390/sym12020197.

[2] M. Bufalo, D. Bufalo, and G. Orlando, "A note on the computation of the modular inverse for cryptography," *Axioms*, vol. 10, no. 2, Art. no. 116 (2021), doi: 10.3390/axioms10020116.

[3] M. Zohourian, A. Pamidimukkala, S. Kermanshachi, and D. Almaskati, "Modular construction: A comprehensive review," *Buildings*, vol. 15, no. 12, Art. no. 2020 (2025), doi: 10.3390/buildings15122020.

[4] T.-H. Nguyen, C.-K. Pham, and T.-T. Hoang, "A high-efficiency modular multiplication digital signal processing for lattice-based post-quantum cryptography," *Cryptography*, vol. 7, no. 4, Art. no. 46 (2023), doi: 10.3390/cryptography7040046.

[5] R. C. Poonia, R. Almakki, A. K. J. Saudagar, A. Altameem, and M. Albathan, "An optimization approach for real-time object detection in IoT devices through edge computing and deep learning," *Journal of Information and Optimization Sciences*, vol. 45, no. 5, pp. 1465–1475 (2024), doi: 10.47974/JIOS-1768.

[6] M. Bufalo, D. Bufalo, and G. Orlando, "Some properties of the computation of the modular inverse with applications in cryptography," *Computation*, vol. 11, no. 4, Art. no. 70 (2023), doi: 10.3390/computation11040070.

[7] I. Touil, W. Chikouche, and Dj. Benterki, "Interior-point method for CQP problems employing a novel trigonometric kernel function," *Journal of Information and Optimization Sciences*, vol. 47, no. 2, pp. 437–453 (2026), doi: 10.47974/JIOS-1464.

[8] R. Muhenga, F. Sapundzhi, M. Popstoilov, S. Georgiev, and V. Todorov, "Comprehensive analysis of cryptographic algorithms: Implementation and security insights," *Engineering Proceedings*, vol. 104, no. 1, Art. no. 43 (2025), doi: 10.3390/engproc2025104043.

[9] A. Ibrahim and F. Gebali, "Enhancing cryptographic solutions for resource-constrained RFID assistive devices: Implementing a resource-efficient field Montgomery multiplier," *Computers*, vol. 14, no. 4, Art. no. 135 (2025), doi: 10.3390/computers14040135.

[10] E. Sakalauskas, "Enhanced matrix power function for cryptographic primitive construction," *Symmetry*, vol. 10, no. 2, Art. no. 43 (2018), doi: 10.3390/sym10020043.

[11] M. Paunović, A. Büyükkaya, and M. Öztürk, "Modular suprametric spaces and fixed-point principles with applications in fractional burn-healing dynamics," *Mathematics*, vol. 14, no. 7, Art. no. 1208 (2026), doi: 10.3390/math14071208.

[12] K. A. Sattar, T. Haider, U. Hayat, and M. D. Bustamante, "An efficient and secure cryptographic algorithm using elliptic curves and max-plus algebra-based wavelet transform," *Applied Sciences*, vol. 13, no. 14, Art. no. 8385 (2023), doi: 10.3390/app13148385.

[13] J. I. Escribano Pablos, M. I. González Vasco, M. E. Marriaga, and Á. L. Pérez del Pozo, "Compiled constructions towards post-quantum group key exchange: A design from Kyber," *Mathematics*, vol. 8, no. 10, Art. no. 1853 (2020), doi: 10.3390/math8101853.

[14] P.-P. Duong and C.-K. Pham, "Constructing 8 × 8 S-boxes with optimal Boolean function nonlinearity," *Cryptography*, vol. 9, no. 4, Art. no. 67 (2025), doi: 10.3390/cryptography9040067.

Received April, 2026