ISSN 2350-1022

International Journal of Recent Research in Mathematics Computer Science and Information Technology
Vol. 13, Issue 1, pp: (43-55), Month: April 2026 – September 2026, Available at: www.paperpublications.org

A Novel Public–Private Key Cryptosystem Based on Matrix Transformations in Generalized Fuzzy Metric Spaces

[1] Shikha Shende, [2]Namrata Tripathi

[1]Research Scholar, Govt. College M.V.M Bhopal, M.P, India

[2]Sr. Assistant Professor, Department of Mathematics,

Govt. College Phanda, Bhopal M.P -462001, India

DOI: https://doi.org/10.5281/zenodo.21921222

Published Date: 13-August-2026

Abstract: **The rapid expansion of digital communication, cloud computing, Internet of Things (IoT), and distributed information systems has significantly increased the demand for efficient and secure cryptographic techniques. Conventional public-key cryptosystems such as RSA and Diffie–Hellman primarily rely on number-theoretic principles, which may encounter computational challenges with the emergence of advanced computing technologies. Consequently, researchers have explored alternative mathematical frameworks capable of providing enhanced security while maintaining computational efficiency. This paper presents a novel public–private key cryptosystem based on Matrix Transformations within the framework of generalized fuzzy metric spaces. The proposed approach employs invertible matrices for encryption and decryption, while generalized fuzzy metric spaces are utilized to analyze the stability, convergence, and robustness of the key-generation process. Furthermore, fixed-point theory is incorporated to establish the existence and uniqueness of cryptographic keys through an iterative contraction mapping. The integration of matrix algebra, generalized fuzzy metric spaces, and fixed-point theory provides a rigorous mathematical framework for analyzing the stability and convergence of the proposed key-generation process, while the cryptographic security depends on the underlying encryption and key-generation mechanisms. A numerical example demonstrates the implementation of the proposed encryption and decryption procedures, while a theoretical security analysis highlights resistance against brute-force attacks, improved key stability, and robustness against transmission uncertainty. The proposed framework provides a mathematical basis for integrating matrix transformations, generalized fuzzy metric spaces, and fixed-point theory in cryptographic key generation. Experimental validation and formal security analysis remain subjects for future research.**

Keywords: **Cryptography, Public Key Cryptosystem, Matrix Transformations, Generalized Fuzzy Metric Space, Fixed Point Theory, Matrix Encryption, Information Security.**

1. INTRODUCTION

This digital transformation has made information security one of the most significant challenges in modern computing. Protecting confidential information from unauthorized access, modification, and cyberattacks requires robust cryptographic techniques capable of ensuring confidentiality, integrity, authentication, and non-repudiation. Consequently, cryptography has become an indispensable component of secure communication systems and continues to evolve with the emergence of new computational paradigms.

Traditional public-key cryptographic systems, including the Rivest–Shamir–Adleman (RSA) algorithm, Diffie–Hellman key exchange, and Elliptic Curve Cryptography (ECC), are primarily based on computationally difficult number-theoretic problems such as integer factorization and discrete logarithms. These cryptosystems have demonstrated remarkable success

in securing digital communications for several decades. However, recent developments in high-performance computing, parallel processing, and quantum computing have raised concerns regarding the long-term security of these conventional approaches. As computational capabilities continue to improve, researchers have increasingly focused on identifying alternative mathematical frameworks that provide enhanced security while maintaining computational efficiency and scalability.

Several researchers have investigated cryptographic systems based on matrix algebra, graph theory, fuzzy mathematical models, and optimization techniques. Matrix-based cryptography offers efficient encryption and decryption operations, while fuzzy mathematical models enhance the representation of uncertainty in secure communication environments. Nevertheless, relatively few studies have explored the integration of matrix transformations, generalized fuzzy metric spaces, and fixed-point theory within a unified public–private key cryptographic framework. This lack of comprehensive integration represents an important research gap and motivates the present investigation.

The present work proposes a matrix-based cryptographic framework that integrates matrix transformations, generalized fuzzy metric spaces, and fixed-point theory. In the proposed approach, cryptographic keys are generated through an iterative fixed-point process in a generalized fuzzy metric space. The public key is derived through the key-generation procedure, while the private key is generated independently from the secret fixed-point value rather than being obtained directly by matrix inversion. Matrix transformations are subsequently employed for encryption and decryption. This framework combines matrix algebra with fuzzy metric analysis to provide a mathematically consistent approach for secure communication under uncertain environments.

The principal contributions of this paper are summarized as follows:

1. A novel public–private key cryptosystem based on invertible matrix transformations is proposed.
2. Generate a secret key using the fixed-point iteration in the generalized fuzzy metric space. The public key is then derived through the proposed key-generation procedure and is used during the encryption process.
3. Fixed-point theory is employed to establish the convergence and uniqueness of the iterative key-generation process.
4. A detailed numerical example illustrates the practical implementation of the proposed encryption and decryption procedures.
5. A theoretical security analysis demonstrates the effectiveness of the proposed approach against common cryptographic attacks while highlighting its potential applications in cloud computing, IoT security, blockchain systems, and secure digital communication.

Conventional public-key cryptosystems, including RSA, Diffie–Hellman, and Elliptic Curve Cryptography (ECC), derive their security from well-established computational hardness assumptions such as integer factorization and the discrete logarithm problem. Matrix-based cryptographic methods, including the classical Hill cipher, provide efficient algebraic transformations but are susceptible to linear cryptanalysis when used without additional security mechanisms. Recent research has also explored post-quantum cryptographic techniques to address emerging computational challenges. The proposed framework contributes to this area by investigating the integration of matrix transformations, generalized fuzzy metric spaces, and fixed-point theory within a unified mathematical framework.

2. MATHEMATICAL PRELIMINARIES

This section presents the fundamental mathematical concepts required for the development of the proposed public–private key cryptosystem. The cryptographic framework integrates matrix algebra, generalized fuzzy metric spaces, and fixed-point theory to establish a secure and mathematically rigorous encryption model.

2.1 Matrix Algebra

Matrices play an essential role in modern cryptography because they provide an efficient mechanism for representing, transforming, and encrypting information

ISSN 2350-1022

International Journal of Recent Research in Mathematics Computer Science and Information Technology
Vol. 13, Issue 1, pp: (43-55), Month: April 2026 – September 2026, Available at: www.paperpublications.org

Invertible matrix

Let

$$K \in GL(n, \mathbb{Z}_p),$$

Where $\mathbb{Z}_p$ is a finite field.

The matrix K is invertible if

$$\det(K) \not\equiv 0 \pmod{p}.$$

Hence,

$$KK^{-1} \equiv I \pmod{p},$$

Where I is the identity matrix.

Definition 2.2 Generalized Fuzzy Metric Space

Let X be a non-empty set, $*$ be a continuous t-norm and

$$\mathrm{M}: \mathrm{X} \times \mathrm{X} \times (0, \infty) \rightarrow [0,1]$$

be a fuzzy metric satisfying:

1. $M(x, y, t) > 0 \; \forall \; x, y \in X, t > 0.$
2. $M(x, y, t) = 1 \; if \; and \; only \; if \; x = y$
3. $M(x, y, t) = M(y, x, t)$
4. $M(x, z, t + s) \geq M(x, y, t) * M(y, z, s)$, for all $x, y, z \in X$ and $t, s > 0$.
5. Continuity in t

Then $(X, M, *)$ is called a generalized fuzzy metric space.

2.2 Matrix Transformations

Let represent plaintext data.

$$p = \begin{bmatrix} p_1 & p_2 \\ p_3 & p_4 \end{bmatrix}$$

Represent plaintext data.

An encryption matrix

$$K = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

must satisfy

$$\det(K) \neq 0$$

to ensure invertibility.

2.3 Finite Field and Modular Arithmetic

All cryptographic operations in the proposed framework are performed over the finite field Z_p, where p is a prime number. Every element of the plaintext matrix, key matrix, and ciphertext matrix belongs to $Z_p = \{0, 1, 2, \ldots . p - 1\}$ Matrix addition, multiplication, and inversion are carried out modulo ppp. The encryption key matrix KKK is selected such that $\det(K) \equiv /(\mathrm{modp})$, ensuring that K is invertible in the finite field. This algebraic setting guarantees mathematically well-defined cryptographic operations and avoids the limitations of real-number matrix computations

ISSN 2350-1022

International Journal of Recent Research in Mathematics Computer Science and Information Technology
Vol. 13, Issue 1, pp: (43-55), Month: April 2026 – September 2026, Available at: www.paperpublications.org

2.4. Key Generation Using Fixed Point Theory

Define

$$T: X \to X$$

by

$$T(x) = Ax + b$$

where A is a contraction matrix.

If

$$M(Tx, Ty, t) \geq \emptyset\big(M(x, y, t)\big)$$

for some increasing function $\emptyset$, then T admits a unique fixed point

$$x^* = T(x^*)$$

which can be used as the secret seed for cryptographic key generation.

key Algorithm

1. Select initial vector x_0
2. Compute

$$x_{n+1} = T(x_n)$$

3. Continue until

$$M(x_n, x_{n+1}, t) \to 1$$

4. Generate cryptographic key from x^*

3. PROPOSED CRYPTOGRAPHIC FRAMEWORK

3.1 Proposed Cryptographic Framework

Step 1: Data Transformation

Convert plaintext into numerical form.

Example

Character	Value
A	1
B	2
C	3
…	…

Message:

DATA

becomes

$$[4, 1, 20, 1]$$

represented as

$$P = \begin{bmatrix} 4 & 1 \\ 20 & 1 \end{bmatrix}$$

Where P denotes the plaintext matrix.

Step 2: Public-Key Generation: Generate a secret key using the fixed-point iteration in the generalized fuzzy metric space. The public- key is then derived through the proposed key-generation procedure and is used during the encryption process.

Choose an invertible matrix

$$K_{pub} = \begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix}$$

with determinant

$$det(K_{pub}) = 1$$

The public key is distributed openly.

Step 3: Encryption

Cipher matrix:

$$C = KP(mod\ p)$$

where:

- P = plaintext matrix,
- K = encryption key matrix,
- C = ciphertext matrix,
- p = prime modulus.

Thus

$$C = \begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} 4 & 1 \\ 20 & 1 \end{bmatrix} = \begin{bmatrix} 52 & 5 \\ 24 & 2 \end{bmatrix}$$

Step 4: Private Key: The private key is generated from the confidential fixed-point value obtained during the iterative key-generation process. It is maintained as secret information and is not computed directly as the inverse of the public key.

The private key is

$$K_{priv} = K_{pub}^{-1}$$

which equals

$$\begin{bmatrix} 1 & -2 \\ -1 & 3 \end{bmatrix}$$

Step 5: Decryption

$$\mathrm{P} = \mathrm{K}_{-1}C \quad (mod\ p)$$

Where K^{-1} denotes the inverse of K in the finite field $\mathbb{Z}_p$.

3.2 Key Generation

Generate the secret key through the iterative mapping

$$x_{n+1} = T(x_n),$$

Where

$$T: X \to X$$

is a contraction satisfying

$$M(Tx, Ty, t) \geq M(x, y, t)^k,$$

ISSN 2350-1022

International Journal of Recent Research in Mathematics Computer Science and Information Technology
Vol. 13, Issue 1, pp: (43-55), Month: April 2026 – September 2026, Available at: www.paperpublications.org

with

$$0 < k < 1.$$

The sequence converges to a unique fixed point

$$x^* = T(x^*),$$

which is used to derive the cryptographic key.

Algorithm 1: Key Generation

Input: Initial vector x_0

Output: Secret key K_s

Step 1

Choose the initial point

$$x_0 \in X.$$

Step 2

Compute

$$x_{n+1} = T(x_n).$$

Step 3

Repeat until

$$\| x_{n+1} - x_n \| < \epsilon.$$

Step 4

Obtain

$$x^*.$$

Step 5

Generate the secret key

$$K_s = f(x^*),$$

Where $f(.)$ is the key-generation function.

3.3 Numerical Example

To illustrate the proposed encryption and decryption process, consider the plaintext message **"DATA"**

Step 1: Plaintext Encoding

The characters are converted into numerical values as follows:

CHARACTER	D	A	T	A
VALUE	4	1	20	1

The plaintext matrix is

$$P = \begin{bmatrix} 4 & 1 \\ 20 & 1 \end{bmatrix}$$

Step 2: Encryption Key

Choose the invertible key matrix

$$K = \begin{bmatrix} 3 & 2 \\ 5 & 7 \end{bmatrix}$$

ISSN 2350-1022

International Journal of Recent Research in Mathematics Computer Science and Information Technology
Vol. 13, Issue 1, pp: (43-55), Month: April 2026 – September 2026, Available at: www.paperpublications.org

The determinant is

$$\det(K) = 3 \times 7 - 2 \times 5 = 11$$

Since

$$11 \neq 0 \pmod{26},$$

The matrix is invertible.

Step 3: Encryption

The ciphertext matrix is obtained using

$$C = KP \pmod{26}.$$

Therefore,

$$C = \begin{bmatrix} 3 & 2 \\ 5 & 7 \end{bmatrix} \begin{bmatrix} 4 & 1 \\ 20 & 1 \end{bmatrix} = \begin{bmatrix} 52 & 5 \\ 160 & 12 \end{bmatrix}.$$

Reducing modulo 26,

$$C = \begin{bmatrix} 0 & 5 \\ 4 & 12 \end{bmatrix}.$$

Step 4: Decryption

Let K^{-1} denote the inverse of K in the finite field.

The plaintext is recovered by

$$P = K^{-1}C \pmod{26}.$$

After performing the inverse matrix multiplication,

$$P = \begin{bmatrix} 4 & 1 \\ 20 & 1 \end{bmatrix},$$

Which correspond to the original message **"DATA"**

Result

The numerical example demonstrates that the proposed matrix-based encryption ad decryption procedure successfully transforms the plaintext into ciphertext and correctly recovers the original message through the inverse transformation. This example illustrates the practical implementation of the proposed cryptographic framework.

Security Analysis in Generalized Fuzzy Metric Spaces

In the proposed framework, generalized fuzzy metric spaces are employed to analyze the stability, convergence, and robustness of the iterative key-generation process under uncertain conditions. Their primary role is to provide a rigorous mathematical framework for studying the behaviour of the key-generation algorithm and to ensure the existence and uniqueness of the generated keys through fixed-point theory. However, generalized fuzzy metric spaces are not used as the underlying source of cryptographic hardness or computational security. The cryptographic strength of the proposed framework depends on the overall key-generation and encryption mechanisms, while the fuzzy metric space provides mathematical support for stability analysis. A formal cryptographic security proof based on computational hardness assumptions remains an important direction for future research. The current framework provides a mathematical foundation for secure key generation; however, a formal proof of resistance against known-plaintext attacks is beyond the scope of this study and is identified as future work. The use of modular arithmetic over a finite field provides a precise algebraic framework for encryption and decryption, ensuring that all matrix operations are mathematically well-defined and suitable for practical cryptographic computation.

ISSN 2350-1022

International Journal of Recent Research in Mathematics Computer Science and Information Technology
Vol. 13, Issue 1, pp: (43-55), Month: April 2026 – September 2026, Available at: www.paperpublications.org

Define the fuzzy distance between two keys K_1 and K_2 as

$$M(K_1, K_2, t) = \frac{t}{t + d(K_1, K_2)}$$

where d is a matrix norm.

Security Properties

- **Confidentiality**

Without knowledge of

$$K_{priv}$$

an attacker cannot recover plaintext.

- **Key stability**

Fixed-point convergence ensures stable key generation.

- **Resistance to Noise**

Fuzzy metric structures tolerate uncertainty during transmission.

- **Large key space**

Higher-dimensional matrices increase computational complexity.

After excluding singular matrices, the remaining invertible matrices still constitute a very large search space. As the matrix dimension increases, the number of possible keys increases exponentially, making exhaustive key search computationally impractical.

- **Resistance to Brute-Force Attacks**

A brute-force attack attempts to recover the secret key by testing every possible candidate until the correct key is found. The proposed cryptosystem offers strong resistance to this attack because of the enormous number of invertible matrices that may serve as valid encryption keys.

4. SECURITY ANALYSIS

The security of the proposed cryptographic framework is evaluated from a theoretical perspective by considering the key space, computational complexity, attack model, and robustness of the key-generation process. The present work focuses on the mathematical properties of the proposed framework, while experimental benchmarking and formal cryptographic validation remain subjects for future investigation.

4.1 Key Space Analysis

The encryption key is selected from the set of invertible matrices over the chosen algebraic domain. As the matrix dimension increases, the number of possible invertible matrices grows rapidly, thereby enlarging the key space and increasing the computational effort required for exhaustive key search. Consequently, larger matrix dimensions improve theoretical resistance to brute-force attacks.

4.2 Computational Complexity

Let nnn denote the order of the key matrix. Matrix multiplication used during encryption and decryption has computational complexity

O(n3),O(n^{3}),O(n3),

using the conventional matrix multiplication algorithm. Therefore, the computational cost increases polynomially with the matrix dimension, making the proposed framework suitable for moderate-sized secure communication systems.

ISSN 2350-1022

International Journal of Recent Research in Mathematics Computer Science and Information Technology
Vol. 13, Issue 1, pp: (43-55), Month: April 2026 – September 2026, Available at: www.paperpublications.org

4.3 Attack Model

The proposed framework is analyzed under the following attack scenarios:

- **Brute-force attack:** The large number of possible invertible matrices increases the search space for an attacker.
- **Known-plaintext attack:** Since matrix-based encryption is linear, resistance against known-plaintext attacks is not formally established in this work. Additional nonlinear transformations and formal security proofs are required for stronger protection.
- **Ciphertext-only attack:** Recovering the original plaintext without knowledge of the secret key remains computationally challenging under the assumed mathematical framework; however, a rigorous cryptographic proof is beyond the scope of the present study.

4.4 Stability of Key Generation

Generalized fuzzy metric spaces and fixed-point theory are employed to analyze the convergence and stability of the iterative key-generation process. These mathematical tools ensure the existence and uniqueness of the generated key but are not claimed to provide computational cryptographic hardness.

4.5 Performance and Future Validation

The present study provides a theoretical mathematical framework and does not include implementation-based benchmark timing or entropy measurements. Performance evaluation, statistical security testing, entropy analysis, and comparison with established cryptographic algorithms such as RSA and ECC are identified as important directions for future research.

Resistance to Known-Plaintext Attacks

In a known-plaintext attack, an adversary attempts to recover the encryption key using one or more plaintext–ciphertext pairs. Since the proposed framework is based on matrix transformations, a sufficient number of independent plaintext–ciphertext pairs may permit recovery of the transformation matrix under certain assumptions. Therefore, the present work does not claim formal resistance to known-plaintext attacks. Instead, the proposed framework emphasizes the mathematical stability of key generation through generalized fuzzy metric spaces and fixed-point theory. A rigorous cryptographic proof of resistance to known-plaintext attacks and the incorporation of additional nonlinear mechanisms remain important directions for future research.

5. COMPARATIVE ANALYSIS

The proposed framework is compared with conventional cryptographic approaches to highlight its mathematical characteristics and intended application. The comparison is qualitative because the present study focuses on theoretical development rather than implementation-based performance evaluation.

Feature	RSA	Matrix-Based Cryptography	Proposed Framework
Mathematical foundation	Integer factorization	Matrix algebra	Matrix algebra, generalized fuzzy metric spaces and fixed-point theory
Key generation	Number-theoretic	Matrix-based	Fixed-point iterative key generation
Algebraic domain	Finite field	Matrix operations	Matrix operation over a define algebraic domain
Computational complexity	High for large key sizes	Moderate	Moderate (matrix multiplication based)
Key space	Large	Depends on matrix size	Depends on matrix dimension and key-generation process
Stability analysis	Not considered	Limited	Supported through generalized fuzzy metric spaces

ISSN 2350-1022

International Journal of Recent Research in Mathematics Computer Science and Information Technology
Vol. 13, Issue 1, pp: (43-55), Month: April 2026 – September 2026, Available at: www.paperpublications.org

Security proof	Well established	Limited	Theoretical framework formal cryptographic proof remains future work
Brute-force resistance	High	Depends on key size	Improved with increasing matrix dimension
Known-plaintext attack	Well studied	Vulnerable if purely linear	Requires additional nonlinear mechanisms for stronger resistance
Practical implementation	Widely deployed	Limited applications	Requires further implementation and benchmarking

6. DISCUSSION

The proposed cryptosystem achieves secure communication through the integration of three complementary mathematical concepts. Matrix Transformations provide efficient encryption and decryption, generalized fuzzy metric spaces model uncertainty and evaluate key robustness, and fixed-point theory guarantees convergence to a unique and stable cryptographic key.

The enlarged key space improves resistance to brute-force attacks, while the convergence properties of the iterative key-generation algorithm ensure consistent and repeatable key computation. These characteristics make the proposed approach suitable for secure cloud computing, Internet of Things (IoT) devices, blockchain networks, distributed information systems, and other applications where reliable and mathematically justified security mechanisms are required.

7. THEORETICAL RESULT

The proposed public–private key cryptosystem relies on the stability of the iterative key-generation process. This section establishes the existence and uniqueness of the generated secret key using fixed-point theory in generalized fuzzy metric spaces.

7.1. Theorem

Let $(X, M, *)$ be a complete generalized fuzzy metric space and $T: X \to X$ satisfy

$$M(Tx, Ty, t) \geq M(x, y, t)^k$$

for $0 < k < 1$.

Then T has a unique fixed point.

Proof Sketch

by repeated application,

$$M(T^n x, T^n y, t) \to 1$$

as $n \to \infty$

Completeness implies convergence of $\{T^n x\}$.

Let

$$x^* = \lim_{n \to \infty} T^n x$$

Then

$$T(x^*) = x^*$$

showing existence.

Uniqueness follows from the contractive condition.

ISSN 2350-1022

International Journal of Recent Research in Mathematics Computer Science and Information Technology
Vol. 13, Issue 1, pp: (43-55), Month: April 2026 – September 2026, Available at: www.paperpublications.org

7.2 Theorem

Let

$$(X, M, *)$$

be a complete generalized fuzzy metric space and let

$$T: X \to X$$

be a contraction mapping satisfying

$$M(Tx, Ty, t) \geq M(x, y, t)^k,$$

Where

$$0 < k < 1.$$

Then T possesses a unique fixed point x^*.

Proof

Starting from any

$$x_0 \in X,$$

Construct the sequence

$$x_{n+1} = T(x_n).$$

Since T is contractive,

$$M(x_n, x_{n+1}, t) \to 1 \quad \text{as} \quad n \to \infty.$$

Hence, $\{x_n\}$ is a Cauchy sequence.

Because $(X, M, *)$ is complete, there exists

$$x^* \in X$$

Such that

$$x_n \to x^*.$$

By continuity of T,

$$T(x^*) = x^*.$$

Therefore, the fixed point exists and is unique.

8. APPLICATIONS

Secure cloud data storage.

- Military communication systems.
- IoT device authentication.
- Digital signatures.
- Blockchain security.
- Secure key exchange protocols.

9. FUTURE SCOPE

❖ **Secure Cloud Computing**

Cloud computing has become one of the most widely adopted technologies for storing and processing large volumes of data. Organizations frequently outsource confidential information to remote cloud servers, making data security a primary concern.

❖ **Internet of Things (IoT)**

The Internet of Things consists of interconnected sensors, smart appliances, wearable devices, and industrial monitoring systems that continuously exchange information over communication networks.

❖ **Blockchain and Distributed Ledger Technology**

Blockchain technology relies on secure communication and authentication among distributed participants. Cryptographic algorithms play a crucial role in protecting transaction integrity, digital identities, and distributed consensus mechanisms.

❖ **Secure Military and Government Communications**

Military organizations and government agencies routinely transmit confidential information through communication networks operating under challenging environmental conditions. Any compromise of sensitive information may have serious national security consequences.

❖ **Digital Signatures and Authentication**

Digital signatures provide authentication, integrity verification, and non-repudiation in electronic communication.

❖ **Financial and Banking Systems**

Modern banking systems process millions of financial transactions each day through online banking platforms, payment gateways, and mobile applications.

❖ **Healthcare Information Systems**

Healthcare institutions increasingly rely on electronic medical records and telemedicine platforms to improve patient care.

❖ **Artificial Intelligence and Smart Systems**

Artificial intelligence applications frequently exchange large quantities of training data and model parameters through distributed computing environments.

❖ **Future Smart Communication Networks**

The evolution of sixth-generation (6G) wireless communication, autonomous vehicles, smart cities, and cyber-physical systems will require cryptographic techniques capable of operating under dynamic and uncertain environments.

10. CONCLUSION

The proposed framework also demonstrates considerable application potential in modern information systems. Possible areas of application include secure cloud computing, Internet of Things (IoT) networks, blockchain technology, digital signatures, healthcare information systems, financial transactions, military communication, and other distributed computing environments where secure communication is essential. The flexibility of the mathematical framework further allows adaptation to emerging technologies and future cryptographic requirements.

Although the proposed model establishes a strong theoretical foundation, several limitations remain. The present work focuses primarily on the mathematical formulation and theoretical analysis of the cryptographic framework. Experimental implementation, performance benchmarking, and comparison with established cryptographic standards such as RSA, Elliptic Curve Cryptography (ECC), and post-quantum cryptographic algorithms have not been investigated in detail. These aspects provide valuable opportunities for future research.

Overall, the proposed public–private key cryptosystem demonstrates that the integration of matrix transformations, generalized fuzzy metric spaces, and fixed-point theory provides a promising direction for the development of secure communication systems. The proposed framework demonstrates how generalized fuzzy metric spaces and fixed-point theory can be used to analyze the stability and convergence of cryptographic key generation. While the mathematical framework is rigorous, a formal security proof based on established computational hardness assumptions remains an important topic for future investigation.

REFERENCES

[1] Moussaoui, A., & Radenović, S. (2025). Fuzzy metric spaces: A survey on fixed point results, contraction principles and simulation functions. Fixed Point Theory and Algorithms for Sciences and Engineering, 2025, Article 24.

[2] **2**.Kanwala, S., Rasheed, F., Munawar, T., Thabet, S. T. M., & Kedim, I. (2025). Generalized fixed-point results for fuzzy mappings in metric and extended fuzzy b-metric spaces. Research in Mathematics, 12(1), 1–10.

[3] **3**.Wong, K. S., Salleh, Z., Younis, M., et al. (2026). An analysis of fixed point results in graphical fuzzy b-metric spaces with applications. Fixed Point Theory and Algorithms for Sciences and Engineering, 2026, Article 13.

[4] Kumar, N., & Kumar, R. (2026). Common coupled fixed point theorems on generalized k-fuzzy metric spaces with an application. Boletim da Sociedade Paranaense de Matemática, 44, 1–16.

[5] Altuhovs, Ș. O., & Varol, B. P. (2026). Hicks-Type Fixed Point Results and Uniform Structure in Intuitionistic Fuzzy b-Metric Spaces. Axioms, 15(6), 399.

[6] Osman Ibnouf, H. I. (2026). Fixed Point Theorems for Contractive Mappings in Non-Archimedean Fuzzy Metric-Like Spaces. International Journal of Analysis and Applications, 24.

[7] Yadav, A. S., & Chauhan, M. S. (2026). Fixed Point Theorem of Generalized Contraction for Multi-valued Mapping on Fuzzy Metric Spaces. International Journal of Mathematics and Its Applications, 13(4), 55–62.

[8] Kamal, A., & Abd-Elal, A. M. (2022). Fixed point for fuzzy mappings in different generalized types of metric spaces. Journal of Mathematics and Computer Science, 25(1), 84–90.

[9] Jeyaraman, M., Vinoba, V., & Pazhani, V. (2021). Convex Structure in Generalized Fuzzy Metric Spaces. European Journal of Mathematics and Statistics, 2(4).

[10] **10.** Ravinder, J., Raj, A. B., Velankanni, A., & Nandakumar, C. D. (2026). Fixed Point Theorem for a Generalized H–F Contractive Mapping in Complete Fuzzy Metric Spaces. Far East Journal of Mathematical Sciences.

[11] Diffie, W., & Hellman, M. E. (1976). *New Directions in Cryptography*. IEEE Transactions on Information Theory, **22**(6), 644–654.

[12] Rivest, R. L., Shamir, A., & Adleman, L. (1978). *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*. Communications of the ACM, **21**(2), 120–126.

[13] Koblitz, N. (1987). *Elliptic Curve Cryptosystems*. Mathematics of Computation, **48**(177), 203–209.

[14] Miller, V. S. (1986). *Use of Elliptic Curves in Cryptography*. Advances in Cryptology—CRYPTO'85, Lecture Notes in Computer Science, Vol. 218, Springer, 417–426.

[15] Hill, L. S. (1929). *Cryptography in an Algebraic Alphabet*. American Mathematical Monthly, **36**(6), 306–312.

[16] Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). *Handbook of Applied Cryptography*. CRC Press.

[17] Stallings, W. (2017). *Cryptography and Network Security: Principles and Practice* (7th ed.). Pearson.

[18] Katz, J., & Lindell, Y. (2020). *Introduction to Modern Cryptography* (3rd ed.). CRC Press.

[19] Bernstein, D. J., Buchmann, J., & Dahmen, E. (Eds.). (2009). *Post-Quantum Cryptography*. Springer.

[20] Paar, C., & Pelzl, J. (2010). *Understanding Cryptography: A Textbook for Students and Practitioners*. Springer.