Fixed Point Based Secure Key Generation in Generalized Fuzzy Metric Spaces for Cryptographic Applications

[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/10.51584/IJRIAS.2026.11060162

Received: 15 June 2026; Accepted: 20 June 2026; Published: 04 July 2026

ABSTRACT

This research introduces a novel cryptographic framework based on fixed point theory in generalized fuzzy metric spaces. The proposed model combines concepts of fuzzy distance, nonlinear contractions, and iterative fixed point mappings to generate secure cryptographic keys. The framework improves uncertainty handling, resistance against attacks, and secure communication in distributed systems. Existence and uniqueness of fixed points are established using generalized fuzzy contraction mappings. Applications in symmetric key generation, authentication systems, and secure communication are discussed.

Keywords: Cryptography, Fixed Point, Key and Security.

INTRODUCTION

Modern cryptography depends heavily on secure key generation. Classical methods use number theory and algebraic structures, but uncertainty in communication systems motivates the use of fuzzy mathematical models(Tripathi, 2019a).

Secure key generation is a fundamental requirement in modern cryptography, ensuring the confidentiality and integrity of digital communications(Tripathi, 2019b). Traditional key generation methods often rely on computational complexity and random number generation techniques. However, increasing security demands have encouraged the exploration of alternative mathematical frameworks(Tripathi & Srivastava, 2017).

Fixed point theory, which studies the existence and uniqueness of invariant points under mappings, has found applications in various fields, including computer science and information security.(Tripathi & Sharma, 2020) Generalized fuzzy metric spaces provide an effective framework for modeling(Tripathi, 2020a) uncertainty and imprecision in complex systems. By combining fixed point principles with generalized fuzzy metric spaces, it is possible to develop secure and robust key generation mechanisms(Tripathi Assistant Professor, n.d.; Tripathi et al., 2021).

This paper proposes a fixed point-based approach for secure key generation in generalized fuzzy metric spaces. The unique fixed points obtained through suitable contractive mappings are utilized to generate cryptography (Kaur et al., 2008)keys with enhanced security characteristics. The proposed framework establishes a connection between advanced fixed point theory and practical cryptographic applications(Tripathi, 2020b), offering a novel direction for secure communication systems(Patil et al., n.d.).

Fixed point theory plays an essential role in:

- Cryptographic stability
- Iterative encryption systems
- Secure key synchronization
- Authentication protocols

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue VI June 2026

This paper develops a generalized fuzzy metric fixed point model for secure cryptographic key generation.

Preliminaries

Fuzzy set

A fuzzy set A in a universal set X is characterized by a membership function

$$\mu_A : X \to [0,1]$$

Where $\mu_A(x)$ represents the degree of membership of x.

2.2 Generalized fuzzy metric space

Let X be a non-empty set and $M: X^2 \times (0,\infty) \to [0,1]$ be a fuzzy metric satisfying:

1. $M(x,y,t) > 0$
2. $M(x,y,t) = 1 \Leftrightarrow x = y$
3. $M(x,y,t) = M(y,x,t)$
4. $M(x,z,t+s) \geq M(x,y,t) * M(y,z,s)$

   Where $*$ is a continuous t-norm.

Continuous t-Norm

A binary operation $* : [0,1] \times [0,1] \to [0,1]$ is called a continuous t-norm if:

- Commutative
- Associative
- Continuous
- $a * 1 = a$

Example:

$a * b = ab$

Proposed Cryptographic Model

We define a nonlinear operator $T: X \to X$ for iterative secure key generation.

The iteration sequence is:

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

The cryptographic key is generated from the unique fixed point

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

Generalized Fuzzy Contraction

Define the contraction condition:

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

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue VI June 2026

Where

$$\emptyset : [0,1] \to [0,1]$$

Satisfies:

$$\emptyset(r) > r$$

For all $0 < r < 1$.

Example contraction:

$$\emptyset(r) = \frac{r+1}{2}$$

Main Theorem

Theorem

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

$M(Tx, Ty, t) \geq \emptyset\big(M(x, y, t)\big)$ For all $x, y \in X$. Then T has a unique fixed point.

Proof of Theorem

Take an arbitrary point $x_0 \in X$.

Construct sequence:

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

Then,

$$M(x_{n+1}, x_n, t) = M(Tx_n, Tx_{n-1}, t)$$

Using contraction,

$$M(x_{n+1}, x_n, t) \geq \emptyset\big(M(x_n, x_{n-1}, t)\big)$$

Iterating repeatedly,

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

Hence x_n is a fuzzy Cauchy sequence. Since X is complete,

$$x_n \to x^*$$

Now using continuity of T,

$$Tx^* = x^*$$

Thus x^* is a fixed point.

For uniqueness, assume another fixed point y^*

Then,

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

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue VI June 2026

Which is possible only if

$$M(x^*, y^*, t) = 1$$

Hence,

$$x^* = y^*$$

Therefore the fixed point is unique.

Secure Key Generation Algorithm

Algorithm

Step 1: Initialization

Choose

Nonlinear mapping T

Step 2: Iteration

Compute

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

Until convergence.

Step 3: Fixed Point Computation

Obtain

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

Step 4: Key Extraction

Generate cryptographic key:

$$K = H(x^*)$$

Where H is a hash function.

Cryptographic Interpretation

The fixed point acts as:

- Stable secret parameter
- Shared session key
- Authentication token

The fuzzy metric introduces:

- Noise tolerance
- Uncertainty handling
- Robustness against perturbation

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue VI June 2026

Security Analysis

Resistance Against Brute Force

The nonlinear fuzzy iteration produces highly complex trajectories.

Sensitivity Property

Small changes in initial conditions generate different fixed point behaviors.

Hash-Based Protection

Final key:

$$K = H(x^*)$$

ensures:

- irreversibility
- collision resistance
- integrity protection

Numerical Example

Consider:

$$X = [0,1]$$

Define fuzzy metric:

$$M(x, y, t) = \frac{t}{t + |x - y|}$$

Take mapping:

$$T(x) = \frac{x + 1}{2}$$

Then,

$$x_{n+1} = \frac{x_n + 1}{2}$$

Starting from

$$x_0 = 0$$

we get:

$$x_1 = 0.5$$

$$x_2 = 0.75$$

$$x_3 = 0.875$$

$$x_4 = 0.9375$$

Thus,

$$x_n \to 1$$

Hence fixed point:

$$x^* = 1$$

Generated key:

$$K = H(1)$$

Applications:

- Secure communication
- Key exchange protocols
- Blockchain security
- Cloud authentication
- IoT security systems
- Applications in Engineering
- Wireless sensor networks
- Secure AI systems
- Cyber-physical systems
- Quantum-resistant frameworks

Future Scope

- Future research may include:
- Hybrid fuzzy-neural cryptography
- Quantum fuzzy cryptographic systems
- Blockchain integration
- Machine learning based adaptive contractions

CONCLUSION

This paper presents a new framework for secure key generation using fixed point theory in generalized fuzzy metric spaces. The proposed approach combines fuzzy mathematics and cryptography to develop robust and secure key generation techniques. The existence and uniqueness of fixed points guarantee stability of generated keys, while fuzzy structures improve robustness under uncertainty.

REFERENCES

1. Kaur, G., Tripathi, N., & Verma, M. (2008). Applications of Graph Theory in Science and Computer Science. International Journal of Advances in Engineering and Management (IJAEM), 2(6), 736. https://doi.org/10.35629/5252-0206736739
2. Patil, R. N., Dhanke, J. A., & Tripathi, N. (n.d.). ENHANCEMENT OF SURFACE GRINDING PROCESS USING GRAPHITE AS A LUBRICANT BASED ON THE TAGUCHI METHOD. Journal of Data Acquisition and Processing, 38(1), 5277. https://doi.org/10.5281/zenodo.7766255
3. Tripathi Assistant Professor, N. (n.d.). INTERNATIONAL JOURNAL OF HIGHER EDUCATION AND RESEARCH IJHER A STUDY OF SKILLED LEARNING IN TEACHING THE CONCEPT OF CONTINUITY, DIFFERENTIABILITY AND VECTOR FOR STUDENT-TEACHERS. 10(2), 167–172. https://doi.org/10.7755/ijher170720.09
4. Tripathi, N. (2019a). A New Technique Developed for production planning using parabolic demand by Laplace Transform. International Journal of Scientific Research in Research Paper. Multidisciplinary Studies E, 5(8), 49–55. www.isroset.org

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue VI June 2026

5. Tripathi, N. (2019b). A Novel Approach for Production Planning for Deteriorating Items with Logarithmic Demand. In World Academics Journal of Research Paper. Management (Vol. 7, Number 2). www.isroset.org
6. Tripathi, N. (2020a). And Cubic Equation. International Journal of Higher Education and Research (IJHER, 10(2), 254–271. https://doi.org/10.7755/ijher170720.16
7. Tripathi, N. (2020b). Computational Thinking for Mathematics and Sciences: an Overview of Learning Approach. International Journal of Scientific Research in Research Paper Mathematical and Statistical Sciences, (7), 69–74. www.isroset.org
8. Tripathi, N., Kaur, G., & Sharma, R. K. (2021). An Artificial Intelligence Technique used in Mathematical Model for Predictions Symptoms of COVID-19 Pandemic. Engineering and Scientific International Journal, 7(4), 112–114. https://doi.org/10.30726/esij/v7.i4.2020.74021
9. Tripathi, N., & Sharma, R. K. (2020). Network Security and Communication Planning Production Agenda for Deteriorating Items with Time Exponential-Proportional Demand. www.ijsrnsc.org
10. Tripathi, N., & Srivastava, N. (2017). OPTIMIZATION PROBLEMS SOLVED BY DIFFERENT PLATFORMS SAY OPTIMUM TOOL BOX (MATLAB) AND EXCEL SOLVER. International Research Journal of Engineering and Technology. www.irjet.net