INTERNATIONAL CONFERENCE ON SCIENCE, INNOVATION AND GLOBAL DEVELOPMENT,
VOLUME-1, ISSUE-5, 2026

# ANALYTICAL STUDY OF ONE-WAY FUNCTIONS AND THEIR IMPACT ON SECURE DIGITAL COMMUNICATION

***Kholliyev Bakhriddin***

*Department Of Economics And Computer Engineering of International School of Finance Technology and Science*

*xolliyevb45@gmail.com*

**Abstract**

This thesis investigates the mathematical foundations, computational properties, and applied significance of one-way functions within the domains of modern cryptography and information security. Defined by their asymmetric computational behavior, one-way functions permit efficient forward computation while rendering inverse computation computationally intractable in the absence of auxiliary secret knowledge. The security of numerous cryptographic constructs—including public-key encryption algorithms, digital signature schemes, authentication protocols, and cryptographic hash functions—is intrinsically dependent on the complexity assumptions underlying these functions. A comprehensive evaluation of prominent one-way paradigms, including modular exponentiation, integer factorization, discrete logarithm problems, and hash-based constructions, is presented. Furthermore, the study assesses the relevance of one-way functions in post-quantum cryptographic frameworks and the development of resilient secure communication systems. The results demonstrate that one-way functions remain indispensable theoretical and practical components for maintaining confidentiality, integrity, authentication, and trust in modern digital infrastructures.

**Keywords**

one-way function, cryptography, hash function, RSA, discrete logarithm, modular arithmetic, public-key cryptography, cybersecurity, post-quantum cryptography, computational complexity.

The continuous growth of digital technologies has intensified the need for effective information security mechanisms across communication networks, cloud services, e-commerce environments, financial systems, and IoT infrastructures. Cryptography plays a central role in protecting sensitive information and ensuring secure digital communication [1].

One-way functions constitute one of the most fundamental mathematical concepts underlying modern cryptography. These functions are characterized by efficient forward computation combined with computationally infeasible inversion under current computational models [2]. Such asymmetry forms the basis of numerous cryptographic constructions, including public-key encryption, digital signatures, and authentication protocols.

The security of major cryptographic systems, including RSA and Diffie–Hellman, depends on mathematical problems exhibiting one-way properties, such as integer factorization and discrete logarithms [3,4]. However, the emergence of quantum computing and algorithms such as Shor's algorithm poses serious challenges to these traditional assumptions [5]. As a result, the development of quantum-resistant one-way functions has become an important research direction within post-quantum cryptography [6]. Therefore, this article focuses on the theoretical principles, mathematical characteristics, and practical applications of one-way functions in modern cryptographic systems.

In computational complexity theory, a one-way function can be formally defined as a function:

$$f: X \to Y$$

that satisfies the following conditions:

The function $f(x)$ can be computed efficiently for every input $x \in X$.

Given the output $y = f(x)$, it is computationally infeasible to determine the

original input $x$.

The term "computationally infeasible" generally means that no known polynomial-time algorithm exists for solving the inverse problem efficiently [7]. In practical cryptography, the security of a system often depends not on the impossibility of inversion, but on the enormous computational resources required to perform inversion attempts.

One-way functions differ from ordinary mathematical functions because of their asymmetrical computational complexity. Multiplication of large prime numbers, for example, is computationally simple, while factoring the resulting composite number into its prime components is significantly more difficult. This asymmetry provides the security foundation for many cryptographic mechanisms.

***Computational Complexity and Security***

The security strength of one-way functions is closely related to computational complexity theory. Complexity classes such as P, NP, and NP-complete problems play an important role in evaluating cryptographic security [8]. If a mathematical problem belongs to a class that lacks efficient solving algorithms, it may serve as a suitable basis for constructing a one-way function.

For example, the integer factorization problem involves finding prime factors of a composite number:

$$n = pq$$

where $p$ and $q$ are large prime numbers. Computing $n$ from $p$ and $q$ is easy, but recovering $p$ and $q$ from $n$ becomes extremely difficult when the primes are sufficiently large.

***Types of One-Way Functions***

One-way functions can be classified into several categories depending on their structural properties and cryptographic applications.

*Integer Factorization-Based Functions*

Integer factorization-based functions form the basis of the RSA cryptosystem. In RSA, encryption and decryption operations rely on modular exponentiation:

$$c \equiv m^e (\mathrm{mod} n)$$

where $m$ is the plaintext message, $e$ is the public exponent, and $n = pq$ is the RSA modulus. The difficulty of recovering the private key depends on the infeasibility of factoring $n$ into its prime components [9].

*Discrete Logarithm-Based Functions*

Another important category involves the discrete logarithm problem. Given a generator $g$, a modulus $p$, and a value:

$$y \equiv g^x (\mathrm{mod} p)$$

it is computationally difficult to determine the exponent $x$. This property is utilized in the Diffie-Hellman key exchange protocol and the ElGamal cryptosystem [10].

*Hash-Based One-Way Functions*

Cryptographic hash functions are another widely used class of one-way functions. A hash function transforms input data of arbitrary size into a fixed-length output:

$$h = H(m)$$

where $H$ represents the hash algorithm and $h$ is the resulting hash value. Hash functions possess several important security properties:

Preimage resistance;

Second preimage resistance;

Collision resistance.

*Applications in Modern Cryptography*

One-way functions represent indispensable building blocks of modern cryptographic architectures, with practical applications spanning multiple domains of information security.

*Public-Key Cryptography*

Public-key cryptographic systems are fundamentally based on one-way mathematical transformations. Within asymmetric encryption frameworks, public keys may be openly distributed, whereas private keys remain confidential. The computational infeasibility of deriving a private key from its corresponding public key constitutes the principal security guarantee of such systems.

*Digital Signatures*

Digital signature schemes employ one-way functions to ensure authentication, integrity, and non-repudiation. In a conventional digital signature process, a message digest is first produced using a cryptographic hash function and subsequently encrypted with the signer's private key.

*Password Security*

Modern authentication mechanisms typically store cryptographic password hashes rather than plaintext credentials. During authentication, the system computes the hash of the submitted password and compares it with the stored value. Even in cases of database compromise, recovering the original passwords remains computationally challenging.

To strengthen security, supplementary techniques such as salting, key stretching, and memory-hard computations are commonly employed. Algorithms including bcrypt, PBKDF2, and Argon2 offer improved resistance against brute-force and dictionary-based attacks [12].

**REFERENCES**

[1] William Stallings, *Cryptography and Network Security: Principles and Practice*, Pearson Education, 2017.

[2] Oded Goldreich, *Foundations of Cryptography*, Cambridge University Press, 2001.

[3] Whitfield Diffie and Martin Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[4] Ronald L. Rivest, Adi Shamir, and Leonard Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[5] Peter W. Shor, "Algorithms for Quantum Computation: Discrete Logarithms and Factoring," *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, 1994.

[6] Daniel J. Bernstein, Johannes Buchmann, and Erik Dahmen, *Post-Quantum Cryptography*, Springer, 2009.

[7] Jonathan Katz and Yehuda Lindell, *Introduction to Modern Cryptography*, CRC Press, 2020.

[8] Michael Sipser, *Introduction to the Theory of Computation*, Cengage Learning, 2012.

[9] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996.

[10] Neal Koblitz, *A Course in Number Theory and Cryptography*, Springer, 1994.

[11] National Institute of Standards and Technology (NIST), *Secure Hash Standard (SHS)*, FIPS PUB 180-4, 2015.

[12] Alex Biryukov, Daniel Dinu, and Dmitry Khovratovich, "Argon2: The Memory-Hard Function for Password Hashing and Other Applications," 2016.

[13] National Institute of Standards and Technology (NIST), *Post-Quantum Cryptography Standardization*, 2024.

[14] Christof Paar and Jan Pelzl, *Understanding Cryptography*, Springer, 2010.

[15] Jean-Philippe Aumasson, *Serious Cryptography: A Practical Introduction to Modern Encryption*, No Starch Press, 2017.