Date: 1st June-2026

ADVANCED ANALYSIS OF ONE-WAY FUNCTIONS AND THEIR IMPLICATIONS FOR MODERN CRYPTOGRAPHY

[1]Boykuziev Ilkhom
[2]Salimov Sirojiddin
[3]Seidullayev Madiyar
[1,2,3]Tashkent University of Information Technologies named after Muhammad ibn Musa al-Khwarizmi
[1]salyut2017@gmail.com
[2]sirojiddin1224@gmail.com
[3]m.seidullayev@tuit.uz

Abstract: This thesis investigates the theoretical foundations, mathematical properties, and practical applications of one-way functions in modern cryptography and information security. One-way functions are characterized by their asymmetry, whereby forward computation is computationally efficient while inversion remains computationally infeasible in the absence of additional secret knowledge. The security of numerous cryptographic primitives, including public-key encryption, digital signature algorithms, authentication mechanisms, and cryptographic hash functions, is fundamentally based on the computational complexity of such functions. The paper presents a comprehensive analysis of prominent one-way function paradigms, including modular exponentiation, integer factorization, discrete logarithm problems, and hash-based constructions. Furthermore, the role of one-way functions in post-quantum cryptography and the design of secure communication systems is critically evaluated. The results demonstrate that one-way functions remain foundational elements for ensuring security, trust, and resilience in contemporary digital infrastructures.

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

The rapid development of information and communication technologies has significantly increased the importance of information security in modern society. Today, digital communication systems, cloud technologies, e-commerce platforms, online banking services, and Internet of Things (IoT) devices require reliable mechanisms to protect sensitive information from unauthorized access and cyber threats. In this context, cryptography has become one of the primary tools for ensuring secure communication and data protection [1].

Among the mathematical foundations of cryptography, one-way functions occupy a central position. A one-way function is a special mathematical transformation that can be computed efficiently in one direction while being practically impossible to reverse within polynomial time using current computational resources [2]. This asymmetry between

forward computation and inverse computation forms the basis of many cryptographic algorithms and security protocols.

The concept of one-way functions emerged from computational complexity theory and gradually evolved into a practical instrument for designing secure cryptographic systems. Public-key cryptography, introduced by Diffie and Hellman in 1976, relies heavily on mathematical problems believed to possess one-way properties [3]. Similarly, the RSA cryptosystem is based on the computational difficulty of factoring large composite integers, whereas the Diffie–Hellman key exchange protocol depends on the hardness of the discrete logarithm problem [4].

Modern cybersecurity challenges have further increased the relevance of one-way functions. The emergence of quantum computing technologies threatens many classical cryptographic algorithms because quantum algorithms such as Shor's algorithm can efficiently solve integer factorization and discrete logarithm problems [5]. Consequently, researchers are actively developing post-quantum cryptographic systems based on new classes of one-way functions resistant to quantum attacks [6].

This article investigates the theoretical and practical aspects of one-way functions, analyzes their mathematical properties, and examines their applications in contemporary cryptographic systems.

Mathematical Definition of One-Way Functions

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.

The computational hardness of one-way functions depends on several factors, including key size, algorithmic complexity, and available hardware resources. Advances in parallel computing, GPU acceleration, and quantum computing continually influence the practical security margins of cryptographic systems.

Another important aspect is probabilistic polynomial-time security. In many cryptographic models, inversion may theoretically be possible, but the probability of successful inversion within feasible computational limits remains negligible. This probabilistic perspective allows cryptographers to design secure systems even when mathematical impossibility cannot be formally proven.

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].

RSA remains one of the most widely used public-key cryptographic algorithms in digital communication systems. However, the security of RSA depends heavily on the selection of sufficiently large prime numbers and secure key generation procedures.

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].

Discrete logarithm-based systems are particularly important in secure communication protocols because they enable secure key establishment over insecure communication channels. Elliptic curve cryptography (ECC) further improves efficiency by implementing discrete logarithm problems on elliptic curves.

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.

Algorithms such as SHA-256, SHA-3, and BLAKE2 are commonly used in modern cybersecurity applications [11]. Hash functions are employed in password storage, blockchain technologies, digital signatures, and integrity verification mechanisms.

Applications in Modern Cryptography

One-way functions are fundamental to numerous cryptographic applications. Their practical significance extends across multiple domains of information security.

Public-Key Cryptography

Public-key cryptography relies entirely on one-way mathematical transformations. In asymmetric encryption systems, the public key can be openly distributed, while the private key remains secret. The inability to derive the private key from the public key ensures communication security.

The RSA algorithm, Diffie-Hellman protocol, and elliptic curve cryptography all depend on one-way computational problems. These systems are widely implemented in secure web protocols such as TLS/SSL, VPN technologies, and encrypted email systems.

Digital Signatures

Digital signatures use one-way functions to provide authentication, integrity, and non-repudiation. In a typical digital signature scheme, a message digest is generated using a cryptographic hash function and then encrypted with the sender's private key.

This process ensures that any modification to the original message changes the hash value, enabling the recipient to detect tampering attempts. Digital signatures are extensively used in electronic commerce, software distribution, and electronic government systems.

Password Protection

Modern authentication systems store password hashes instead of plaintext passwords. When a user enters a password, the system computes its hash value and compares it with the stored hash. Even if attackers gain access to the database, recovering the original passwords remains computationally difficult.

To improve security, additional techniques such as salting, key stretching, and memory-hard functions are used. Algorithms such as bcrypt, PBKDF2, and Argon2 provide enhanced protection against brute-force attacks [12].

Blockchain and Cryptocurrencies

Blockchain technologies extensively utilize one-way hash functions. Each block in a blockchain contains the cryptographic hash of the previous block, forming a secure and immutable chain.

Cryptocurrencies such as Bitcoin rely on SHA-256-based mining mechanisms, where miners repeatedly compute hash values to solve computational puzzles. The one-way nature of hash functions prevents unauthorized manipulation of transaction records.

One-Way Functions and Quantum Computing

Quantum computing presents serious challenges to classical one-way functions. Shor's algorithm can efficiently solve both integer factorization and discrete logarithm problems using quantum computers [5]. As a result, traditional cryptographic systems such as RSA and ECC may become vulnerable in the future.

To address this issue, researchers are developing post-quantum cryptographic algorithms based on alternative hard mathematical problems, including:

– Lattice-based cryptography;
– Code-based cryptography;
– Multivariate polynomial cryptography;
– Hash-based signature schemes.

These approaches aim to construct quantum-resistant one-way functions capable of maintaining security even in the presence of large-scale quantum computers [13].

Post-quantum cryptography has become a strategic research area because future communication infrastructures, government systems, financial institutions, and military networks require long-term cryptographic security. Standardization organizations such as NIST are actively evaluating candidate algorithms for next-generation cryptographic standards.

Challenges and Limitations

Despite their importance, one-way functions also face several theoretical and practical challenges. One major issue is the absence of a formal mathematical proof confirming the existence of true one-way functions. Their security currently relies on unproven assumptions regarding computational hardness [14].

Another challenge involves advances in cryptanalysis and hardware technologies. Improvements in algorithmic techniques may reduce the practical security of previously trusted cryptographic systems. For example, advances in distributed computing and specialized hardware acceleration have significantly increased the efficiency of brute-force attacks.

Side-channel attacks also pose risks to systems based on one-way functions. Even when the underlying mathematical problem remains difficult, attackers may exploit implementation weaknesses such as timing information, power consumption, or electromagnetic leakage to recover secret information [15].

Consequently, modern cryptographic engineering requires not only mathematically secure one-way functions but also secure software and hardware implementations resistant to practical attacks.

One-way functions constitute one of the most essential mathematical foundations of modern cryptography and information security systems. Their asymmetrical computational

structure enables the development of secure encryption algorithms, digital signature schemes, authentication protocols, and blockchain technologies. Mathematical problems such as integer factorization, discrete logarithms, and cryptographic hash functions continue to provide the basis for many contemporary cybersecurity solutions.

The increasing complexity of cyber threats and the emergence of quantum computing technologies have intensified research into stronger and more efficient one-way functions. Although classical cryptographic algorithms remain widely used, future information security infrastructures will likely depend on post-quantum cryptographic systems resistant to quantum attacks.

Overall, one-way functions remain indispensable for ensuring confidentiality, integrity, authentication, and trust in digital communication environments. Continued research in computational complexity, cryptanalysis, and quantum-resistant cryptography will play a critical role in strengthening global cybersecurity systems in the coming decades.

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.