Mathematica Eterna
ISSN: 1314-3344
OPEN ACCESS Freely available online
Opinion Article

Modular Arithmetic and Double Phase Encoding: A New Asymmetric Cryptosystem

Adem John*

Department of Mathematics, Technical University of Berlin, Berlin, Germany

DESCRIPTION

In the ever-evolving field of cryptography, asymmetric cryptosystems have become pivotal in securing digital communications and data. These systems rely on pairs of keys-one public and one private-to encrypt and decrypt information. Among the various techniques enhancing cryptographic security, modular arithmetic and phase encoding techniques are significant. This article examines an asymmetric cryptosystem that leverages modular arithmetic and double random phase encoding to bolster cryptographic security.

Introduction to asymmetric cryptosystems

Asymmetric cryptosystems, also known as public-key cryptosystems, use two distinct keys for encryption and decryption. The public key is widely distributed, while the private key is kept secret by the owner. The security of these systems is based on mathematical problems that are computationally difficult to solve, such as factoring large prime numbers or computing discrete logarithms.

Modular arithmetic in cryptography

Modular arithmetic is a type of arithmetic that deals with remainders when numbers are divided. In cryptographic systems, modular arithmetic plays a important role due to its properties of arithmetic operations within a finite set of numbers. This is essential for ensuring the efficiency and security of cryptographic algorithms.

Basic operations and properties: In modular arithmetic, calculations are performed with respect to a modulus. For instance, in modulo n arithmetic, numbers wrap around after reaching n. This arithmetic is foundational for several cryptographic algorithms, including RSA and ElGamal.

Application in asymmetric cryptosystems: Modular arithmetic is used in key generation, encryption, and decryption processes. For example, in RSA encryption, messages are transformed into integers and then exponentiated modulo a product of two large primes. This ensures that decryption is computationally feasible only with the correct private key.

Double random phase encoding

Double Random Phase Encoding (DRPE) is a technique used to enhance the security of data encryption by introducing randomness in the encoding process. It involves encoding the message twice using randomly generated phase factors, adding complexity and security to the encryption process.

Principles of phase encoding: Phase encoding involves altering the phase of a signal or data to encode information. By introducing randomness in the phase, the encoded data becomes less predictable and more resistant to attacks.

Double encoding mechanism: In DRPE, the message is encoded twice with two different sets of random phases. This double encoding increases the entropy of the encrypted data, making it more secure against cryptographic attacks. Each phase introduces an additional layer of encryption, significantly enhancing security.

Integrating modular arithmetic and DRPE in ban asymmetric cryptosystem

Combining modular arithmetic with double random phase encoding can create a robust asymmetric cryptosystem with enhanced security features.

Key generation: The key generation process involves generating large prime numbers and computing modular inverses. These keys are then used in combination with DRPE to encode and decode messages securely.

Encryption process: During encryption, the plaintext message is first transformed using modular arithmetic operations, such as modular exponentiation. The encoded message is then subjected to double random phase encoding, adding an additional layer of security through phase variations.

Decryption process: The decryption process reverses the encryption steps. First, the encoded message undergoes phase decoding using the corresponding private key. Next, modular arithmetic operations are applied to retrieve the original plain text message.

Correspondence to: Adem John, Department of Mathematics, Technical University of Berlin, Berlin, Germany, E-mail: ademjohn07@fernuni-hagen.de

Received: 28-May-2024, Manuscript No. ME-24-33176; **Editor assigned:** 30-May-2024, PreQC No. ME-24-33176 (PQ); **Reviewed:** 14-Jun-2024, QC No. ME-24-33176; **Revised:** 21-Jun-2024, Manuscript No. ME-24-33176 (R); **Published:** 28-Jun-2024, DOI: 10.35248/1314-3344.24.14.218

Citation: John A (2024) Modular Arithmetic and Double Phase Encoding: A New Asymmetric Cryptosystem. Math Eter. 14:218.

Security advantages: The use of modular arithmetic ensures efficient and secure encryption and decryption operations. Double random phase encoding adds an extra layer of protection by making the encrypted data more resistant to attacks. The combination of these techniques enhances the overall security of the cryptosystem.

Practical considerations and challenges

Here are some potential titles focusing on practical considerations and challenges.

Computational complexity: While modular arithmetic and DRPE provide robust security, they also introduce computational complexity. The encryption and decryption processes may require significant computational resources, especially for large keys and data sets.

Random phase generation: The security of DRPE relies on the quality of random phase generation. Ensuring true randomness in phase generation is critical for maintaining the security of the cryptosystem.

Implementation and performance: Implementing a cryptosystem that combines modular arithmetic and DRPE requires careful consideration of performance and efficiency. Optimizing algorithms and hardware resources is essential for practical applications.

An asymmetric cryptosystem utilizing modular arithmetic and double random phase encoding represents a powerful approach to enhancing cryptographic security. By leveraging the mathematical properties of modular arithmetic and the randomness introduced by phase encoding, this cryptosystem offers robust protection against various cryptographic threats. As technology advances and computational capabilities evolve, the integration of these techniques will continue to play a important role in securing digital communications and data.