Transactions on Computer Science and Intelligent Systems Research
ISSN: 2960-1800, eISSN: 2960-2238 | Volume 5
AIDML 2024

An Overview of the Chinese SM9 Algorithm: A Cutting-Edge Cryptographic Breakthrough

Wenbo Ma[1], Zejun Ni[2, *]

[1]School of Computer and Information Engineering, Henan University of Economics and Law, Zhengzhou, China

[2]School of Information Science and Engineering, East China University of Science and Technology, Shanghai, China

* Corresponding Author Email: 22013162@mail.ecust.edu.cn

Abstract. The SM9 algorithm represents a sophisticated advancement in cryptographic protocols, characterized by its unique implementation of bilinear pairing techniques and identity-based encryption mechanisms. Unlike conventional approaches, SM9 leverages the user's identity directly in the generation of cryptographic keys, streamlining the process and enhancing security. This method stands in contrast to traditional schemes like SM2, which typically rely on external certificate management for public key association. Central to its innovation is the seamless integration of identity information into the public key itself, thereby simplifying the encryption process and reducing the overhead associated with certificate handling. SM9's versatility extends to various applications, including digital signature creation, robust data encryption, secure key exchange, and reliable identity verification. This algorithm has garnered significant attention for its ability to maintain a high level of security while offering greater efficiency and user convenience. By directly binding keys to user identities, it eliminates several complexities and potential vulnerabilities inherent in certificate-based systems. As a result, SM9 has demonstrated remarkable performance and utility across a wide range of research and practical applications, making it a noteworthy subject of study in the field of modern cryptography.

Keywords: Cryptography; Identity-Based Cryptograph; SM9; Digital signature.

1. Introduction

As science and technology relentlessly advance, the safeguarding of personal information in the digital landscape has become more critical and challenging. This escalating vulnerability of private data in the online world has been widely acknowledged and documented in numerous studies and reports [1, 2]. Amidst this backdrop, a significant development occurred in April 2016, when China announced the official release of its indigenously developed SM9 identity-based cryptographic algorithm. This groundbreaking algorithm represents a pivotal stride in information security, offering a novel approach to protecting individual identities and sensitive data in the digital domain.

The SM9 algorithm, with its unique identity-based encryption framework, stands out for its capacity to directly integrate user identity into the encryption process, thereby fortifying the security of personal information against unauthorized access and exposure. Its innovative design has garnered international recognition and acclaim, culminating in its inclusion in the ISO/IEC 14888-3:2018 text in November 2018. This inclusion not only marks the SM9 algorithm as an international standard but also underscores China's growing influence and contribution to the global cryptographic landscape.

The recognition of the SM9 algorithm at this level is a testament to its robustness, efficiency, and adaptability, making it an essential tool in the arsenal against the escalating threats to personal information security in the online world. Its adoption and implementation on a global scale represent a major leap forward in the quest to safeguard personal data and maintain privacy in our increasingly interconnected digital society.

2. Relevant theories

2.1. Introduction Of Public Key Encryption

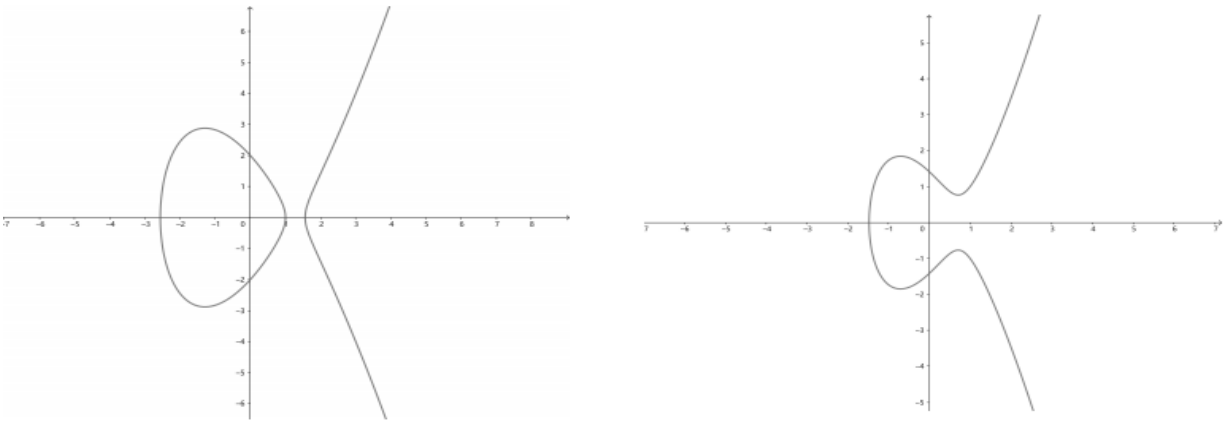
Public-key cryptography, often referred to as asymmetric cryptography, represents a paradigm shift in cryptographic methodology with its distinctive use of two interrelated keys. This dual-key system comprises a publicly accessible key for encryption, aptly named the public key, and a confidential, user-specific key for decryption, known as the private key. This dichotomy allows for secure communication in an open network environment [3]. A fundamental attribute of this system is the asymmetry between the encryption and decryption processes; while the public key is widely available and used to encrypt messages, the private key remains exclusively with the recipient and is the only means to decrypt the incoming data. This ensures that even if the encryption process is transparent and the public key is known, the security of the communication remains intact, as the private key necessary for decryption is computationally infeasible to derive from the public key. The elegance of this approach lies in its combination of openness and security, making it a cornerstone of modern cryptographic practices [4].

2.2. Elliptic Curve

An elliptic curve over a finite field consists of a point P= (x, y) whose coordinate values satisfy a certain equation, usually an equation of the following form [5]:

$$y^2 + axy + by = x^3 + cx^2 + dx + e \tag{1}$$

The coefficients a, b, c, d, and e are all in a finite domain and meet certain conditions, and Figure 1 is an example of two elliptic curves.



(a) $y^2 = 2x^3 - 3x + 2$ (b) $y^2 = x^3 - 5x + 4$

Fig. 1 Elliptic curves (Photo/Picture credit: Original).

2.3. Definition of Digital Signature

In digital signature verification, a public verification algorithm is utilized alongside a corresponding verification key, streamlining the process for authenticating the signature's legitimacy. This method employs the signer's public key, which is readily accessible, ensuring transparency in the verification process. However, it is critical to note that the integrity of the system is maintained through the confidentiality of the signer's private key, which remains undisclosed. Upon receiving a message M that has been digitally signed, recipients use the public key to verify the signature. This process ensures that the message has indeed been sent by the holder of the private key and has not been tampered with during transmission. The strength of this system lies in its ability to provide a secure method of confirming the authenticity and integrity of digital communications. It offers a robust solution in environments where trust and security are paramount, reinforcing the confidence in digital interactions.

2.4. Identity-Based Cryptograph

In conventional public-key cryptography, a sender must first acquire the recipient's public key and digital certificate from a trusted source to ensure secure communication. This process, often laden with multiple data exchanges and validations, culminates in the sender using the public key to encrypt and transmit the initial message. Contrastingly, identity-based encryption algorithms streamline this procedure substantially [6]. In these systems, a central authority, typically referred to as the Private Key Generator (PKG), initiates the process by running the system construction algorithm S(λ), where λ is a security parameter. This algorithm generates a master key pair (msk, mpk), encompassing both public and private components [7]. Subsequently, the PKG executes the key generation algorithm G(msk, id), taking as input the master public key (mpk) and a unique user identifier (id). This process results in the creation of a personalized private key (sk_id) for the user. Furthermore, the encryption algorithm E(msk, id, m) plays a pivotal role in this setup. Here, the cryptographer inputs the master public key (mpk), the intended recipient's identifier (id), and the plaintext message (m), producing the encrypted ciphertext (c). This innovative approach negates the need for preliminary key exchanges, significantly enhancing efficiency and security in digital communications..

$$\Pr\left[V(mpk, id, m, I(G(msk, id), m)) = \text{accept} \begin{vmatrix} (mpk, msk) \leftarrow S(\lambda) \\ id \in ID \\ m \in M \end{vmatrix}\right] = 1 \tag{2}$$

Where: ID represents a limited identifier space; M denotes limited message space; C referto a finite ciphertext space.

2.5. Bilinear Pairing

Mapping e maps two elements in G1 and G2 to one element in G3 and satisfies the bilinear property [8]. Suppose g1 and g2 are elements in groups G1 and G2, respectively, and e represents a bilinear mapping from G1 × G2 to G3 then there is [8]:

$$\begin{aligned} &e(ag_1, bg_2) = ab \\ &e(g_1, g_2) = e(abg_1, g_2) = e(g_1, abg_2) \\ &e(ag_1, bg_2) + e(cg_1, dg_2) = (ab + cd)e(g_1, g_2) \end{aligned} \tag{3}$$

3. Current Status of Chinese Cryptographic Algorithms

3.1. SM4 Algorithm

In this cryptographic framework, both the encryption and key expansion algorithms are defined by a nonlinear iterative process that encompasses 32 rounds. This design is a deliberate choice to enhance the complexity and security of the algorithm. Each round contributes to the transformation of the input data, making it increasingly difficult for unauthorized parties to decipher the message without the correct key [9]. The decryption algorithm, while structurally similar to its encryption counterpart, differs significantly in how it utilizes the round keys. In the decryption process, the order of these keys is reversed compared to the encryption phase. This inversion is crucial for the decryption process, enabling the reversal of the encryption's complex transformations. Such an approach ensures that although the underlying structure of the encryption and decryption algorithms is similar, their operations are sufficiently distinct [10]. This distinction is essential for maintaining the security integrity of the system. The iterative nature of the process, combined with the careful management of key usage, provides a robust and secure cryptographic solution, capable of withstanding various types of cryptographic attacks.

3.2. ZUC Algorithm

This cryptographic system boasts the capacity to generate a series of 32-bit key streams, each of which comprises individual 32-bit words that are designated as keys in their own right. This key stream generation is a critical feature, enabling the system to produce a diverse array of keys, thereby enhancing the security and versatility of the encryption process. These key streams are not only plentiful but also distinct, ensuring that each encryption and decryption operation can be tailored with a unique key, significantly reducing the likelihood of key reuse and the associated security risks. This approach is particularly advantageous in scenarios requiring high levels of data security and integrity, as it provides a robust defense against various forms of cryptographic attacks, including those that exploit key repetition or predictability. The ability to generate and employ these multiple key streams effectively positions this system as a reliable and secure choice for modern cryptographic applications. As shown in Figure 2.

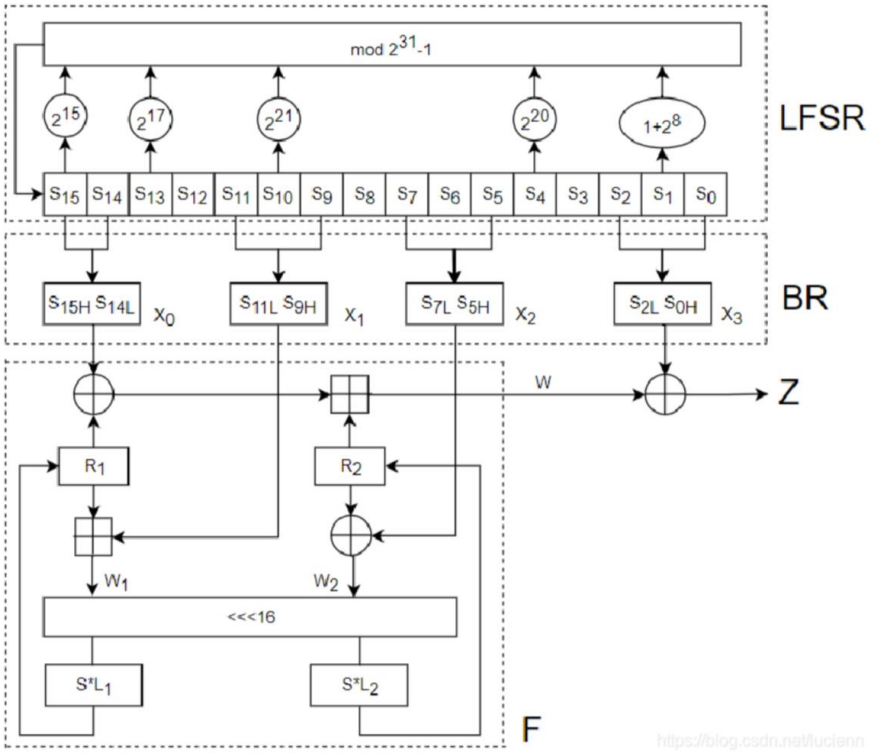


Fig. 2 ZUC algorithm structure (Photo/Picture credit: Original).

4. Conclusion

In conclusion, the evolution and implementation of Chinese cryptographic algorithms, notably the SM9, SM4, and ZUC, mark a significant stride in the field of digital security and encryption. The SM9 algorithm, with its innovative identity-based encryption system, has revolutionized the way personal information is secured online. By incorporating user identity directly into key generation, it simplifies the encryption process and elevates security, making it a vital tool against the increasing vulnerabilities in the digital realm. The SM4 algorithm's 32-round nonlinear iterative structure for both encryption and key expansion demonstrates China's capability in developing robust symmetric key algorithms. Meanwhile, the ZUC algorithm's proficiency in generating multiple 32-bit key streams showcases versatility in stream cipher technology. These advancements reflect a broader trend in global cybersecurity, where the focus is shifting towards more sophisticated, efficient, and user-centric cryptographic solutions. The inclusion of the SM9 algorithm in the ISO/IEC international standards is not just an acknowledgment of its technical excellence, but also a sign of the growing global influence of Chinese cryptographic research and development. This trend underscores the importance of continued innovation and collaboration in the cryptographic community to address the ever-evolving challenges in digital security.

Authors Contribution: All the authors contributed equally and their names were listed in alphabetical order.

Authors Contribution

All the authors contributed equally and their names were listed in alphabetical order.

References

[1] Bergman Martinkauppi, L., & He, Q. (2019). Performance Evaluation and Comparison of Standard Cryptographic Algorithms and Chinese Cryptographic Algorithms.

[2] Tian, C., Wang, L., & Li, M. (2020, September). Design and implementation of SM9 Identity based Cryptograph algorithm. In 2020 International Conference on Computer Network, Electronic and Automation (ICCNEA) (pp. 96-100). IEEE.

[3] Shi, Y., Ma, Z., Qin, R., Wang, X., Wei, W., & Fan, H. (2019). Implementation of an attribute-based encryption scheme based on SM9. Applied Sciences, 9(15), 3074.

[4] Liu, X., Huang, X., Cheng, Z., & Wu, W. (2024). Fault-tolerant identity-based encryption from SM9. Science China Information Sciences, 67(2), 122101.

[5] Zhu, X., Xu, H., Zhao, Z., & others. (2021). An Environmental Intrusion Detection Technology Based on WiFi. Wireless Personal Communications, 119(2), 1425-1436.

[6] Piao, L., NuanQiang, Y., Han**an, H., Man, L. J., ShuFeng, Y., RuiJue, F., & MengZhen, S. (2021, December). Power Data Collection Terminal Protection Based on SM9. In 2021 International Conference on Power System Technology (POWERCON) (pp. 1877-1882). IEEE.

[7] Martinkauppi, L. B., He, Q., & Ilie, D. (2020, June). On the design and performance of Chinese OSCCA-approved cryptographic algorithms. In 2020 13th International Conference on Communications (COMM) (pp. 119-124). IEEE.

[8] Shen, S., Yang, Y., & Liu, X. (2023). Toward data privacy preservation with ciphertext update and key rotation for IoT. Concurrency and Computation: Practice and Experience, 35(20), e6729.

[9] Zhu, X., Huang, Y., Wang, X., & Wang, R. (2023). Emotion recognition based on brain-like multimodal hierarchical perception. Multimedia Tools and Applications, 1-19.

[10] Yin, D., Zhang, M., & Wei, B. (2021, September). Blockchain E-voting scheme based on SM9 partial blind signature. In 2021 International Conference on Computer Information Science and Artificial Intelligence (CISAI) (pp. 1005-1011). IEEE.