IPRPD
International Journal of Business & Management Studies
ISSN 2694-1430 (Print), 2694-1449 (Online)
Volume 06; Issue no 06: June, 2025
DOI: 10.56734/ijbms.v6n6a14

A FEASIBLE FAIL-STOP SECURITY CONTROL MECHANISM FOR BLOCKCHAIN

Ching-Min Lee[1], Shin-Yan Chiou[2], Jonathan Jen-Rong Chen[3]

[1 2] Chang Gung University, Taiwan
[3]Hungkuo Delin University of Technology, Taiwan

Abstract

Since the inception of blockchain in 2008, it has played a crucial role in cryptography. In recent years, its applications have expanded beyond cryptography, evolving into a comprehensive information technology framework across various fields. Traditionally, the security of digital signatures has relied on the assumption of computational parity between attackers and defenders—that is, both parties possess equal computing power. However, this assumption inherently carries the risk of a significant disparity between offense and defense. Users must remain vigilant against potential attacks from counterfeiters impersonating decrypted users.

In this study, we propose a feasible Fail-Stop Scheme (FSS) technology to address this issue, providing a more robust framework to enhance blockchain security.

Keywords

Blockchain, Cryptography, Digital Signature, Fail-stop Signature Scheme

1. Introduction

Information security technology has become an integral part of modern life. As cybercrime and digital threats continue to evolve, security has emerged as a critical requirement in the era of information technology and digitalization. Consequently, robust information security measures are now indispensable for safeguarding technological systems and applications.

Cryptography is a fundamental technology in the field of information security. For thousands of years, humans have used encryption techniques to safeguard critical information, reflecting the evolution of civilization itself. Beyond its role in intelligence operations, cryptography is also a race against time, continuously adapting to emerging threats.

Modern cryptography has widespread applications across military, technical, commercial, and everyday domains. In the realm of e-commerce, for instance, cryptographic techniques secure business communications, financial transactions, file transfers, online banking, shopping platforms, and digital bookstores. As online services proliferate and cybercrime becomes more prevalent, the importance of cryptography has grown significantly, making it an indispensable pillar of information security.

The security of modern cryptography is often assessed based on probabilistic models. In this context, cryptographic security is measured by the time required to crack an algorithm using brute force methods, with the assumption that an attacker's computational power is comparable to that of potential defenders. The longer it takes to break a password or encryption algorithm, the stronger the security. Conversely, a shorter cracking time indicates weaker algorithm strength.

In cryptography-related applications, traditional digital signatures operate under the assumption that attackers and defenders possess comparable computational resources. However, in the e-commerce

environment, this assumption does not always hold true. As the saying goes, "For every foot of height, there is ten feet of magic"—meaning that when criminal organizations leverage supercomputers with immense computational power, they can rapidly break password protections, impersonate legitimate users, and conduct fraudulent financial or commercial transactions.

Such attacks not only result in financial losses for victims but also disrupt business operations, causing widespread inconvenience to users. The full extent of these damages can be difficult to estimate. In such situations, impostors must either prove their innocence, or system owners must ensure robust security measures that protect user rights and prevent fraudulent activity. Strengthening cryptographic frameworks is essential to restoring trust and normal business operations.

Blockchain, the foundational technology behind cryptocurrencies, traces its origins to the challenge of digitally verifying timestamps in the late 1980s and early 1990s. In 1990, Haber and Stornetta published a seminal paper titled How to Timestamp a Digital Document, in which they proposed a hash chain mechanism that linked issued timestamps together, preventing documents from being forward-dated or backdated.

In 1992, Haber, Stornetta, and Dave Bayer introduced the concept of Merkle Trees to further enhance this design. Merkle Trees improved system efficiency by aggregating multiple time-stamped documents into a cryptographically secured chain of blocks. Each record in the chain is linked to its predecessor, ensuring that the latest entry retains knowledge of the entire chain's history.

Then, Wei Dai one of the noted researchers, introduced the concept of b-money which is used to create money through solving computational puzzles and decentralized consensus. But this proposal lacks implementation details. (Blockchain, an emerging technology for the future - Data Driven Investor - Medium n.d.) (The Exponential Guide to Blockchain - Singularity University n.d.)(History of blockchain | Technology | ICAEW n.d.)(A brief history in the evolution of blockchain technology platforms - By n.d.) In 2005, a concept called "Reusable Proof of Work" (RPoW) was introduced by Hal Finney, a cryptographic activist. This concept combined the ideas of both b-money and computationally difficult Hashcash puzzle by Adam Back for the creation of cryptocurrency. RPoW registers the ownership of tokens on a trusted server. These servers allow the users to check the correctness and integrity of users which in turn helps to solve double spending problem. (History of Blockchain | Binance Academy n.d.)

In 2008, a groundbreaking white paper titled Bitcoin: A Peer-to-Peer Electronic Cash System, authored by the enigmatic Satoshi Nakamoto, introduced the concept of blockchain. In this paper, Nakamoto integrated principles from cryptography, computer science, and game theory to outline the digital currency Bitcoin. This innovation enabled participants to transact directly between accounts without the need for intermediaries such as central authorities or banks.

(A Brief History of Blockchain: Blockchain Basics Book, ConsenSys Academy, n.d.) The following timeline table (Table 1) provides a concise overview of the emergence of blockchain technology (Padmavathi U. and N. Rajagopalan, 2021).

Table 1. Timeline for the Emergence of Blockchain

Year	Emergence of Blockchain
1990	Stuart Haber & Stornetta introduced timestamping a digital document so that they could not be tampered.
1992	The concept of Merkle trees was proposed to collect several documents in one block.
2000	The theory and idea of cryptographic secured chains was proposed by Stefen Konst.
2005	Hal Finney introduced "Reusable Proof of Work" (RPoW) that helps users to solve double spending problem in the creation of cryptocurrencies.
2008	Satoshi Nakamoto Proposed Bitcoin, a digital currency which makes use of Blockchain as the underlying concept.

Since the emergence of blockchain technology in 2008, its capabilities—such as decentralization, multi-party verification, tamper resistance, anonymity, transaction traceability, and distributed ledger applications—have driven widespread adoption. Countries around the world continue to explore blockchain-based business models, technologies, and applications, each shaping their own vision and policies for blockchain development. (Kuo and Shyu, 2021).

Scholars mentioned that blockchain technology has the following advantages: (1) Decentralization, (2) Reduced Transaction Costs, (3) Efficiency, (4) Traceability, (5) Security, (6) Faster Processing. And it also has considerable practical application in the following related fields: (1) Finance, (2) HealthCare (Cornelius C. Agbo and Qusay H. Mahmoud, 2020), (3) Land Registry, (4) Insurance (Priti Sharma and Ritesh Chandra, 2022), (5) Digital Voting (Kashif Khan *et al.*, 2018), (6) Global Trade, (7) Copyright and royalty protection, (8) Inheritance, (9) Drug traceability, (10) Government, (11) Supply chain monitoring (Padmavathi U. and N. Rajagopalan, 2021).

Owing to the incremental and diverse applications of cryptocurrencies and the continuous development of distributed system technology, blockchain has been broadly used not only in above mentioned field but also in fintech, smart homes, public health, and intelligent transportation due to its properties of decentralization, collective maintenance, and immutability. Although the dynamism of blockchain abounds in various fields, concerns in terms of network communication interference and privacy leakage are gradually increasing. Because of the lack of reliable attack analysis systems, fully understanding some attacks on the blockchain, such as mining, network communication, smart contract, and privacy theft attacks, has remained challenging. (Chen *et al.*, 2022)

In blockchain applications, it maybe exists the following problems: (1) the attack and defense methods of mining pool attacks for blockchain security issues, such as block withholding, 51%, pool hopping, selfish mining, and fork after withholding attacks, in the attack type of consensus excitation; (2) the attack and defense methods of network communication and smart contracts for blockchain security issues, such as distributed denial-of-service, Sybil, eclipse, and reentrancy attacks, in the attack type of middle protocol; and (3) the attack and defense methods of privacy thefts for blockchain privacy issues, such as identity privacy and transaction information attacks, in the attack type of application service. (Chen *et al.*, 2022) How to improve the security of blockchain applications will be the focus of continuous research.

Considering the current advancements and practical requirements of blockchain application technology, this study aims to propose a feasible Fail-Stop Scheme (FSS) algorithm architecture. This framework not only addresses the security challenges associated with digital signatures but also enhances practical security across various blockchain applications.

2. Literature Review

A digital signature guarantees the validity and authenticity of electronic documents. Enhancing security measures to reduce the likelihood of forgery—or even enabling proof of forgery—can significantly strengthen digital signature integrity. The key characteristics of digital signatures include: (Chen, J. J. R. *et al.*, 2000; Diffie, W. and Hellman, M. 1976)

(1) Authenticity: Determining the source of legality of the information, i.e., that the information has been sent by the sender rather than a forgery or recycled old messages.
(2) Integrity: Ensuring that the information has not been altered intentionally or unintentionally or replaced with new or deleted text.
(3) Non-repudiation: After sending messages.
(4) Uniqueness – Generates a distinct signature for each document, based on cryptographic algorithms.
(5) Tamper Resistance – Protects the document from unauthorized modifications using encryption techniques.

In addition, another type of fail-stop signature scheme (FSS) can satisfy the aforementioned requirements.

Kitajima (Kitajima *et al.*, 2015) showed that an FSS has to have at least two security properties. (1) A scheme based on information-theoretic security has to be secure, even against a computationally unbounded adversary. (2) If the computational assumption is broken, an honest signer should be able to prove that a signature is a forgery by virtue of information-theoretic security. (Chen, J. J. R. *et al.*, 2021)

In 1990, the German scholar Birgit Pfitzmann et al. firstly proposed the concept of failure to stop signature Strategies (Bleumer *et al.*, 1991; Pfitzmann and Waidner, 1990; Pfitzmann, 1991), to protect the attacker cracks and the possibility of counterfeit signature issue.

In 1993, an efficient FSS scheme based on discrete logarithm is presented (Van Heyst and Pedersen, 1993), and FSS schemes using schemes "bundling homomorphism" is proposed (Van Heyst *et al.*, 1993).

In 2000, the Australian scholar Willy Susilo *et al.* propose a new signature policy Fail-Stop (Susilo *et al.*, 2000), according to Strong factorization hypothesis explanation the difficulties of signature cracks. Since in 2004, the German scholar Katja Schmidt-Samoa proposed a modified version to Willy Susilo's method (Schmidt-Samoa, 2004). They use of Fail-Stop signature policy based on the difficulty of factoring (Bari'c and Pfitzmann, 1997; Diffie and Hellman, 1976), While those who can prove to be counterfeit innocence, but also exposed the secret of $n = p \times q$ (Boneh *et al.*, 1999; Takagi, 2004).

The whole system in order to continue to function properly, it is necessary to rebuild or replace the system parameters, not only affect the functioning of the whole system, the system also caused the owners of the credit crisis. This is worth exploring, how can we not expose the secret of $n = p \times q$, to prove to be forged by innocence. Moreover, we also must guard against malicious attackers to deny behavior.

In 2014, Chain, K. *et al.* proposed an improved fail-stop signature scheme based on dual complexities of the the discrete logarithm and factorization to solve the expose $n = p \times q$ secret problem effectively. The scheme can be implemented in e-commerce information security environments and provides the user with the possibility of preventing attacks and enhancing system safety (Chain *et al.*, 2014).

Over the years, relevant information security scholars and researchers are still trying to combine various schemes to propose more effective FSS security mechanisms for application in various fields, especially in the blockchain.

In 2020, L. Lingareddy and P. Krishnamoorthy mentioned related technologies of blockchain. A blockchain is continuous linked list of blocks and each block is called a record, which will keep track of the transaction data, unique hash value, and previous hash value to link with the previous record. Since there is no central node to maintain the records and data is distributed to all the nodes, data protection will be more. If the intruders try to attack or hack the network then they must modify all the copies of data in the blocks, so it is less possible to compute the hash values which will consume huge computation power and attack the blockchain network. Hence it is highly suggestable in financial services (L. Lingareddy and P. Krishnamoorthy, 2020).

Scholar Lingareddy *et al.* also proposed Blockchain Technology and Its Applications, especially the concept of security, which also provides a comprehensive discussion of this research.

3. Research Methods

We propose a feasible fail-stop strategy and algorithmic architecture for blockchain, based on discrete logarithm and factorization complexity. This approach ensures that confidential information remains protected throughout the transfer process. To substantiate our design, we employ formal mathematical deduction and proof to articulate the system development process.

This study provides a comprehensive analysis of the proposed security architecture and the security requirements of blockchain, ensuring alignment with the research objectives.

The content outline is as follows: The second part of the literature review. The fourth part is preliminary discussion. The fifth part is our proposed signature strategy. Part sixth presents security analysis of the signature algorithms scheme and comprehensive discussion, both the conclusions and future research directions described in endnote.

4. Review Of Fail-Stop Scheme And Preliminary Discussion

4.1 Notation

n 、 p 、 q 、 p_1 、 g are integer and p_1 、 p 、 q are prime, $n = p \times q$ 、 and m is message.

4.2 Fail-stop policy mechanisms

System Center select a large prime number p_1 which satisfies the following formula $n \mid p_1 - 1$. $n = p \times q$, p 、 q are two large prime numbers. Then System Center select an element g whose order modulo p_1 is p. That is satisfies as follow:

$$g^{\frac{1}{2}p} \equiv -1(\text{mod } p_1) \quad \text{……(1)}$$

The public Key of System Center is p_1 、 g 、 n, private key is p 、 q (Rabin, 1979; Rivest *et al.*, 1978; Wagstaff, 1979).

4.2.1 Key Generation

The signer A chooses 2 integers x_1 、 $x_2 \in z_n^*$ and calculates:

$$y_i \equiv g^{x_i} (\text{mod } p_1) \text{ , } 1 \le i \le 2 \quad \text{…..……...…(2)}$$

The signer A uses $\{y_1, y_2\}$ in a trusted center. Thus, signer A's public key is y_i, and the private key is x_i from $1 \le i \le 2$ 。

4.2.2 Algorithm for signing a message m

Suppose the signer A wants to sign a message m to receiver B. The digital signature calculation is below:

$$m_1 \equiv mx_1 + x_2 (\text{mod} n) \quad \text{……..…(3)}$$

Then, the signer A produces $\{m_1\}$ as a signature of message m.

4.2.3 Algorithm for verifying the signature

The receiver B confirms the validity of the signature $\{m_1\}$ by testing whether the following equation holds:

$$g^{m_1} \equiv y_1^m y_2 (\text{mod } p_1) \quad \text{……..……(4)}$$

If the algorithm that generates the parameters, keys, and signing messages is successful, then the confirmation of the signature in the signature verification algorithm is the same.

If the above equation was established, then accept information m, otherwise, it is rejected.

4.2.4 Proof of Forgery

Assume the receiver B uses the signature $\{m_2\}$, which is an acceptable signature on m that signer A wants to forge. To do so, signer A calculates his own signature:

$$m_1 \equiv mx_1 + x_2 (\text{mod} n)$$

and $GCD\,(m, -m_2, n)$, and GCD(a1, a2). GCD(a1, a2) means that two numbers a1 and a2 of the greatest common factor. Then, the composite number n could be factorized by the signer A. Therefore, the signature $\{m_2\}$ is proof of forgery. (Brickell and McCurley, 1991; Chen and Liu, 2000; Laih and Kuo, 1997; Lenstra and Lenstra, 1993; Niven *et al.*, 1991)

4.2.5 Schmidt-Samoa attack

Schmidt-Samoa proposed an attack mode in 2004 (Schmidt-Samoa, 2004; Chain *et al.*, 2014) as follows. Assume that an attacker E, who received signer A's signature, and per the method of producing $\{m, m_1\}$, chooses an integer $x_1^{'} \in z_n^*$ and calculates:

$$y_1 \equiv g^{x_1^{'}} (\text{mod } p_1)$$

and E chooses another integer $x_2^{'}$ that satisfies:

$$m_1 \equiv mx^{'}_1 + x^{'}_2 (\text{mod} n)$$

Then, E selects an interger $t \in z_n^*$ and calculates:

$$s_0 \equiv (m_1 + tp)x^{'}_1 + x^{'}_2 (\text{mod } p)$$

$$s_0 \equiv (m_1 + tp)x'_1 + x'_2 (\mathrm{mod}\, q)$$

We calculate with the Chinese remainder theorem (CRT), m_0 can be calculated, and the attacker E can send the forged messages: $m_0 \equiv (m_1 + tp(\mathrm{mod}\, n))$. In addition, the attacker E can send the same digital signature s_0 with signer A. To resolve these weaknesses of Susilo *et al.*'s scheme (Susilo *et al.*, 2000), Schmidt-Samoa proposed another model, in which $n = p^2q$. If the reader is interested, specifics are provided in Schmidt-Samoa's scheme (Schmidt-Samoa, 2004).

5. Our Propose Scheme

The Public & Secret Key generated by the System Center, all with the same way as the previous section. But in this section, Then System Center add select an element g_1 whose order modulo p_1 is n. Then g_1 also is a Public Key that satisfies:

$$g_1^{\frac{n}{2}} \equiv -1 (\mathrm{mod}\, p_1)$$

5.1 Key Generation

This step is the same as above. The signer A chooses 2 integers x_1 、 $x_2 \in z_n^*$ and calculates:

$$y_i \equiv g^{x_i} (\mathrm{mod}\, p_1) \text{ ， } 1 \le i \le 2 \text{ ….……....(5)}$$

The signer A uses $\{y_1, y_2\}$ in a trusted center. Thus, signer A's public key is y_i ,and the private key is x_i from $1 \le i \le 2$ 。

5.2 Algorithm for signing a message m

Suppose the signer A wishes to sign a message m to receiver B. The calculations are as follows:

（**1**）**Calculations:**

The signer A chooses one number a , and calculate:

$$t \equiv a \cdot x_1 (\mathrm{mod}\ n) \text{ ……..….(6)}$$

$$a \equiv m^2 \cdot x_1 + x_2 (\mathrm{mod}\ n) \text{ ……(7)}$$

$$y_2 \equiv \mathrm{g}^{\mathrm{x}_2} (\mathrm{mod}\ p_1) \text{ ……...……..(8)}$$

$$s \equiv \mathrm{g}^{\mathrm{a}} (\mathrm{mod}\ p_1) \text{ ……...(9)}$$

And chooses a number $k_1 \in z_m^*$, and calculate:

$$r_1 \equiv \mathrm{g}^{\mathrm{k}_1} (\mathrm{mod}\ p_1) \text{ ……..(10)}$$

$$s \equiv \mathrm{a} \cdot r_1 + \mathrm{k}_1 \cdot b_1 (\mathrm{mod}\ n) \text{ ……..…(11)}$$

（2）The signer A chooses a number $k_2 \in z_m^*$, and calculates:

$$r_2 \equiv g^{k_2} (\mathrm{mod}\ p_1) \text{ ……..……(12)}$$

$$y_2 + m \equiv x_2 \cdot r_2 + k_2 \cdot b_2 (\mathrm{mod}\ n) \text{ ……(13)}$$

（3）Then, signer A sends $\{t, r_1, b_1, r_2, b_2, y_2, s, m\}$ to receiver B.

5.3 Algorithm for verifying the signature

B receives $\{t, r_1, b_1, r_2, b_2, y_2, s, m\}$, then calculates and tests the following equations to determine whether they hold:

$$g^{m+y_2} \equiv y_2^{r_2} \cdot r_2^{\ b_2} (\mathrm{mod}\ p_1) \text{ ……..(14)}$$

$$g^s \equiv s^{r_1} \cdot r_1^{b_1} (\mathrm{mod}\ p_1) \text{ ……...…(15)}$$

$$y_2 \equiv s \ \cdot y_1^{-m^2} (\mathrm{mod}\ p_1) \text{ ……(16)}$$

If the equations above are established, the message m is accepted, otherwise, it is rejected.

5.4 Proof of Forgery

Assume that receiver B uses the message $\{t', r_1', b_1', r_2', b_2', y_2', s', m\}$, which is an acceptable signature on m that signer A wants to forge. Therefore, signer A calculates the steps of the signature stage, and receiver B calculates the steps of the verification stage. Between both probabilities is $(1-q^{-1})$, and $s_1 \neq s_2' (\mathrm{mod}\, n)$; thus, the innocent signer A can be restored.

6. Security Analysis

6.1 Lemma 1: Assume the sender is honest, then verify the equation (14), (15), (16) will be satisfy.

Proof：

(1)Calculate equation (13) both sides of the full equation base on g, then:

$$g^{y_2+m} \equiv g^{x_2 \cdot r_2} \cdot g^{k_2 \cdot b_2} (\mathrm{mod}\ \ p_1)$$

According equation (7), (8), we can get:

$$g^{y_2+m} \equiv y_2^{r_2} \cdot r_2^{b_2} (\mathrm{mod}\ \ p_1)$$

(2)Calculate equation (11) both sides of the full equation base on g, according equation (9)~(11), then we can get:

$$g^{s} \equiv s^{r_1} \cdot r_1^{b_1} (\mathrm{mod}\ \ n)$$

(3)Calculate equation (7) both sides of the full equation base on g, then:

$$g^{a} \equiv g^{m^2 x_1} \cdot g^{x_2} (\mathrm{mod}\ \ p_1)$$

$$s \equiv g^{m^2 x_1} \cdot y_2 (\mathrm{mod}\ \ p_1)$$

$$s \equiv y_1^{m^2} \cdot y_2 (\mathrm{mod}\ \ p_1)$$

According equation (7),(8), then we can get:

$$y_2 \equiv s \cdot y_1^{-m^2} (\mathrm{mod}\ \ p_1)$$

Thus, this lemma has been proved.

6.2 Lemma 2: The password x_i of the sender (Signer) is not to be leaked.

Proof:

(1) Assume that the attacker I has the ability to manipulate and attack, According to equation (2), he can get :

$$x_1 \equiv x_0 + \alpha \cdot p (\mathrm{mod}\ \ n),\ 0 \leq x_0 < p,\ 0 \leq \alpha < q$$

For I, x_0 is known, and α is unknown.

(2) According equation (6), The attacker I can know:

$$a \equiv a_0 + \alpha' \cdot p (\mathrm{mod}\ \ p_1)$$

In it, a_0 is known, and α & a' is unknown. That $0 \leq a$, $\alpha' < q$.

(3) According equation (7), The attacker I can calculate:

$x_2 \equiv x_2' + x_2'' \cdot p (\mathrm{mod}\ \ n)$, $0 \leq x_2' < p$, x_2' is known, But $0 \leq x_2'' < q$, x_2'' is unknown.

(4) Analysis from (1) to (3), the password x_i of the sender (Signer) is not to be leaked out.

6.3 Theorem 1: The probability of $s_2 \neq s_2' (\mathrm{mod}\, n)$ is $(1-\frac{1}{q})$.

Proof: From lemma 1、lemma 2, we know that signer A has the same value c in signing a message m and that attacker I has the same value $c^{'}$. From (Bleumer *et al.*, 1991), we know that: $c^{'} \equiv c + lp(\mathrm{mod} n), 0 \le l < q-1$, and that the probability of $c^{'} \equiv c(\mathrm{mod} n)$ is $\frac{1}{q}$.

According to Equation (7)，the probability of s_2 is equal to $s_2^{'}$ and is $\frac{1}{q}$，Thus, Theorem 1 is proven.

From the discussion above, in (Chen *et al.*, 2007; Hu and Huang, 2006; Susilo and Mu, 2005; Van Heijst *et al.*, 1993; Van Heyst and Pedersen, 1993), there are proofs that the algorithms are secure for the signer.

Establishing a situation in which signer A does not need to replace his private and public keys (ELGamal, 1985; Okamoto and Uchiyama, 1998) in the proof-of-forgery stage after restoring his innocence is the chief proposal of this paper.

7. Disscussion

7.1 A comparison

We compare our proposed scheme with the other 2 FSS schemes as Table 2. Due to the interactions between parameters, a general evaluation was difficult to perform. To explain the computational complexity, we define certain operation symbols as follows:

σ : related to the signer's security
k : related to the recipient's security
K :max (k, σ)

Table 2. Comparison of computational and efficiency parameters

	Susilo *et al.*'s scheme	Schmidt-Samos's scheme	Our proposed scheme
PK (mult)	4K	k	4K
Sign (mult)	1	$\sigma = \max(\sigma, k/3)$	2
Test (mult)	4K	$4\sigma = \max(4\sigma, 4k/3)$	3K
Length of PK	2	$6\sigma = \max(6\sigma, 2k)$	2
Length of SK	4K	$6\sigma = \max(6\sigma, 2k)$	4K
Length of a signature	2K	$3\sigma = \max(3\sigma, k)$	2K
Underlying hard problem	DL & Factorization	Factorization	DL & Factorization

As shown in the table 2, the proposed scheme performs as well as the FSS scheme of Susilo (2000), but the security of Chain and our scheme are higher than Susilo (2000).

In our method, the design of the parameter "t" is adopted in the equation (6) to protect the parameter " a ", so as to prevent the attack of Schmidt-Samoa Scheme.

7.2 Blockchain security discussion

(1) Decentralization

The decentralization of the blockchain is a particular advantage, reducing the use of numerous data centers to verify transactions and ensuring that the entire network is not compromised even if it is attacked. In addition to obtaining the public key (p_1、g、g_1、n) and private key (p、q) from the system center, the participants (signers) of this mechanism can immediately verify and stop actions even if they encounter forgery in the rest of the process, thereby maintaining overall network security.

(2) Reduced Transaction Costs

The Fail-Stop Scheme (FSS) mechanism enhances security verification and control within blockchain networks, effectively reducing costs for users and businesses over time.

(3) Efficiency

Blockchain technology accelerates transaction processing by simplifying and automating operations. Additionally, participants in the network are not required to manage multiple documents, as trust is reinforced when all parties share a unified digital ledger. The Fail-Stop Scheme (FSS) mechanism plays a crucial role in maintaining security and preventing counterfeiting within this framework.

(4) Traceability

Blockchain enhances traceability by allowing the ledger to be tracked along the chain from its point of origin. This capability helps verify the provenance of a product and facilitates the identification and resolution of issues within its distribution path. The Fail-Stop Scheme (FSS) mechanism further strengthens security by detecting and exposing counterfeiters during the fail-stop process, ensuring a safer and more reliable system.

(5) Security

Blockchain technology ensures that all transactions are added to the ledger only after undergoing rigorous trust verification. Each participant in the network is assigned a unique identity key linked to their account, in accordance with the Fail-Stop Scheme (FSS) mechanism. If authentication fails, access is immediately revoked to prevent unauthorized activity.

Additionally, the blockchain ledger is secured through cryptographic techniques, relying on adjacent blocks to reinforce the encryption process. Transactions are recorded sequentially, creating a time-stamped structure that enhances integrity and makes it significantly more difficult for hackers to manipulate or compromise the chain.

(6) Faster Processing

Blockchain operates continuously-24 hours a day, 7 days a week-enabling faster transaction processing. Additionally, advancements in information systems and improvements in computing speed further accelerate processing efficiency and enhance security verification. These developments contribute significantly to strengthening security control mechanisms and ensuring a more resilient digital infrastructure.

8. Conclusions And Future Research

There is a direct causal relationship between information security management and the research and development of encryption technologies. To ensure security measures remain ahead of emerging threats—rather than merely reacting to breaches after vulnerabilities are exploited—it is crucial to adopt a proactive approach. Continuous advancements in encryption technology, particularly within the Fail-Stop Scheme (FSS) mechanism, represent a vital direction for the future of information security management.

Blockchain is defined by several key characteristics, including decentralization, anonymity, immutability, consensus mechanisms, and encryption. Over time, its applications have expanded across various domains, including proof of existence, smart contracts, the Internet of Things (IoT), identity verification, prediction markets, asset transactions, e-commerce, social communication, file storage, and data APIs (application programming interfaces).

Each of these applications inherently faces security challenges related to digital signatures, reinforcing the importance of robust cryptographic mechanisms. Given the critical role blockchain plays in securing digital interactions, maintaining and enhancing security remains a top priority.

This paper introduces a feasible and secure fail-stop signature strategy based on discrete logarithm and factorization complexity. This approach ensures that confidential information remains protected during blockchain transactions, establishes proof of innocence in cases of alleged forgery, and mitigates the risk of malicious rejection caused by an attacker's actions.

Under this mechanism, all operations can be immediately halted upon detection of an attack or counterfeiting attempt, providing a robust security framework for blockchain applications.

Improving existing protection mechanisms and establishing a secure, stable market order is the ultimate goal we actively pursue. Therefore, ongoing research and development of secure blockchain applications will remain a key priority. In particular, ensuring the security of smart contract signing within blockchain systems will be the focus of our next research endeavor.

References

Bari'c, N. and Pfitzmann, B. (1997). Collision-free accumulators and fail-stop signatures without trees.advances in Cryptology – Eurocrypt '97, Lecture Notes in Computer Science 1233, 480-494. doi:10.1007/3-540-69053-0_33

Bleumer, G., Pfitzmann, B. and Waidner, M. (1991). A remark on signature scheme where forgery can be proved. In Advances in Cryptology - EUROCRYPT 90, volume 473 of Lecture Notes in Computer Science, 441 – 445, Berlin. doi:10.1007/3-540-46877-3_39

Boneh, D., Durfee, G. and Howgrave-Graham, N. (1999). Factoring $N = p^r q$ for large r. In Advances in Cryptology - CRYPTO 99, volume 1666 of Lecture Notes in Computer Science, 326–337, Berlin. doi:10.1007/3-540-48405-1_21

Brickell, E. F. and McCurley, K. S. (1991). An Interactive Identification Scheme based on Discrete Logarithms and Factoring. Advances in Cryptology – Eurocrypt '90, Lecture Notes in Computer Science 437, 63-71. doi:10.1007/3-540-46877-3_6

Chain, K., Chen, J. J. R., Yang, J. F. and Chang, K. H. (2014). An improved Fail-Stop Signature Scheme Based on Dual Complexities, International Journal of Innovative Computing, Information and Control, Vol. 10, Number 2, 535-544.

Chen, J. J. R. and Liu, Y. (2000). A Traceable Group Signature Scheme, Mathematical and Computer Modelling 31, 147-160. doi:10.1016/S0895-7177(99)00229-0

Chen, J. J. R., Chiang, Y. Y., Hsu, W. H., and Lin, W. Y. (2021). Fail Stop Group Signature Scheme. Security and Communication Networks, vol. 2021, Article ID 6693726, 1-6. doi:10.1155/2021/6693726

Chen, X. F., Zhang, F. G., Susilo, W. and Mu, Y. (2007). Efficient generic on-line/off-line signatures without key exposure, Lecture Notes in Computer Science, Vol. 4521, 18-30. doi:10.1007/978-3-540-72738-5_2

Chen, Y. R., Chen, H., Zhang, Y., Han, M., Siddula, M. and Cai, Z. P. (2022). A survey on blockchain systems: Attacks, defenses, and privacy preservation, High-Confidence Computing, Elsevier, Vol. 2, Issue 2. doi: 10.1016/j.hcc.2021.100048

Cornelius C. Agbo and Qusay H. Mahmoud. (2020). Blockchain in Healthcare: Opportunities, Challenges, and Possible Solutions. International Journal Of Healthcare Information Systems And Informatics 15(3):82-97. doi:10.4018/IJHISI.2020070105

Diffie, W. and Hellman, M. (1976). New directions in cryptography. IEEE IT, 22, 644-654. doi:10.1109/TIT.1976.1055638

ELGamal, T. (1985). A public-key cryptosystem and a signature scheme based on discrete logarithms, IEEE Trans. On Information Theory II-31 (4), 469-472. doi:10.1109/TIT.1985.1057074

Hu, X. and Huang, S. (2006). Comment fail-stop blind signature scheme design based on pairings, Wuhan University Journal of Natural Sciences, Vol. 6, 1545-1548. doi:10.1007/BF02831817

Kashif Khan, Junaid Arshad and Muhammad Khan. (2018). Secure digital voting system based on blockchain technology. Core. 1-12. IGI Global. doi:10.4018/IJEGR.2018010103

Kuo, C. C. and Shyu, J. Z. (2021). A Cross-National Comparative Policy Analysis of the Blockchain Technology between the USA and China, Sustainability 2021, 13(12):6893. doi:10.3390/su13126893

Laih, C. S. and kuo, W. C. (1997). New signature schemes based on factoring and discrete logarithms, IEICE Trans. Fundamentals E80-A, 46-53.

L. Lingareddy and P. Krishnamoorthy (2020). Blockchain Technology and Its Applications. Impact of Digital Transformation on Security Policies and Standards. IGI Global. doi: 10.4018/978-1-7998-2367-4.ch007

Lenstra, A. K. and Lenstra, H. W. Jr. (1993). The Development of the Number Field Sieve, Vol. 1554 of Lecture Notes in Mathematics. Springer-Verlag.

N. Kitajima, N. Yanai, T. Nishide, G. Hanaoka, and E. Okamoto, (2015). Constructions of fail-stop signatures for multi-signer setting. 2015 10th Asia Joint Conference on Information Security, 112-123, doi: 10.1109/AsiaJCIS.2015.26.

Niven, I., Zuckerman, H. S. and Montgomery, H. L. (1991). An Introduction to the Theory of Numbers, John Wiley and Sons.

Okamoto, T. and Uchiyama, S. (1998). A new public-key cryptosystem as secure as factoring. In Advances in Cryptology - EUROCRYPT 98, volume 1403 of Lecture Notes in Computer Science, 308–317, Berlin. doi:10.1007/BFb0054135

Padmavathi U. and N. Rajagopalan (2021). Concept of Blockchain Technology and Its Emergence. Blockchain Applications in IoT Security. IGI Global. 1-17.doi: 10.4018/978-1-7998-2414-5.ch001

Pfitzmann, B,. Waidner, M. (1990). Formal Aspects of Fail-stop Signatures; Interner Bericht 22/90 der Fakultät für Informatik, Universität Karlsruhe, Dezember.

Pfitzmann, B. (1991). Fail-stop Signatures: Principles and Applications; Proc. Compsec '91, 8th world conference on computer security, audit and control, Elsevier, Oxford, 125-134.

Priti Sharma and Ritesh Chandra. (2022). Significance of Blockchain in Banking and Insurance. Applications, Challenges, and Opportunities of Blockchain Technology in Banking and Insurance. IGI Global. 99-127. doi: 10.4018/978-1-6684-4133-6.ch006

Rabin, M. O. (1979). Digitalized signatures and public-key functions as intractable as factorization, Technical Report LCS/TR 212, MIT, Cambridge, MA.

Rivest, R. L., Shamir, A. and Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. Comm. Of the ACM, Vol. 21, Issue 2:120-126. doi:10.1145/359340.359342

Schmidt-Samoa, K. (2004). Factorization-based Fail-Stop Signatures Revisited. In: Information and Communications Security (ICICS 2004), LNCS 3269, 118-131. Springer-Verlag. doi:10.1007/978-3-540-30191-2_10

Susilo, W. and Mu, Y. (2005). Provably secure fail-stop signature schemes based on RSA, International Journal of Wireless and Mobile Computing, Vol.1, No.1, 53-60. doi:10.1504/IJWMC.2005.008055

Susilo, W., Safavi-Naini, R., Gysin, M. and Seberry, J. (2000). A new and efficient fail-stop signature scheme. The Computer Journal, 43(5):430–437. doi: 10.1093/comjnl/43.5.430

Takagi, T. (2004). A fast RSA-type public-key primitive modulo $p^k q$ using hensel lifting. IEICE Transactions, Vol. E87-A(1):94–101.

Van Heijst, E., Pedersen, T. P., and Tzmann, B. P. (1993). New constructions of fail-stop signatures and lower bounds, Lecture Notes in Computer Science, Vol. 740, 15-30.

Van Heyst, E. and Pedersen, T. P. (1993). How to make efficient fail-stop signatures, Lecture Notes in Computer Science, Vol. 658, 366-377. doi:10.1007/3-540-47555-9_30

Wagstaff, S. S. Jr. (1979). Greatest of the least primes in arithmetic progression having a given modulus. Mathematics of computation, 33(147), 1073-1080.

W. Susilo, R. Safavi-Naini, M. Gysin and J. Seberry (2000). A new and efficient fail-stop signature scheme, Computer Journal, Vol. 43, No. 5, 430-437.

