




Security Monitoring Method of Accounting Computerized Software with Artificial Intelligence Integration under Digital Marketing

Yang Jin^{1*} 

¹Henan Polytechnic Institute, NanYang, 473000, China,
yangjin_hnpi@outlook.com

Corresponding author: Yang Jin, yangjin_hnpi@outlook.com

Abstract. In order to improve the security monitoring effect of computerized accounting software, this paper combines artificial intelligence technology to build a security monitoring system for computerized accounting software. Moreover, this paper makes full use of the specific structure and characteristics of the nonlinear components of the cryptographic algorithm, and uses the high probability differential path to reduce the number of required failures and increase the number of rounds to induce failures. In the differential fault analysis of the SHACAL-2 algorithm and the MD5 encryption mode, the properties of the differential equation formed by the round function are analyzed. In this process, algebraic analysis technology is mainly used, and after the differential characteristic of the round function is introduced into the differential fault attack, the probability analysis technology is mainly used to solve the required number of faults, and the security monitoring model of the accounting computerized software is constructed. The research shows that the security monitoring effect of the computerized accounting software proposed in this paper has a good effect, which can effectively improve the security of the computerized accounting software.

Keywords: artificial intelligence; computerization of accounting; software security; monitoring; Digital Marketing Security

DOI: <https://doi.org/10.14733/cadaps.2024.S4.150-173>

1 INTRODUCTION

At this stage, there are still some problems in the process of applying accounting computerized software, that is, the confidentiality and security of the company's financial information system are relatively poor. However, for an enterprise, financial data is very important. If the financial data is leaked, it will have a great negative impact on the survival and development of an enterprise [1]. In the process of applying accounting computerized software, accounting information is recorded on

the magnetic storage medium by means of various data files. In this case, the information is relatively easy to be copied and changed. In addition, the database technology is relatively centralized. Although some personnel are not authorized, they can also use computers and networks to browse files, increasing the danger of software [2].

The human factor is an important factor that increases the security risk of computerized accounting software, because when operating the computerized accounting software, if the user does not perform the correct operation, it will be prone to hardware failure, power interruption, etc. It is easy to increase the risk of software security [3]. In addition, because there is no relatively perfect management system, and no perfect operation management mechanism has been established, this causes the computerized accounting personnel to operate the software arbitrarily, and there is no management mechanism to refer to. In this case, the It will affect the security of computerized software, and it is prone to problems such as the transfer of funds in the deposit account [4].

In the process of applying accounting computerized software, if the software application is unreasonable, it is easy to cause software security problems. At this stage, many companies' financial institutions buy some advanced software products when purchasing computerized software, and do not combine the actual situation of the current company. In this case, it is not conducive to the function of accounting computerized software. It is also prone to waste of resources. In addition, accounting computerized software generally needs to have a high operating environment. At this time, if the software is improperly applied, it is easy to induce software security problems [5].

In the process of applying accounting computerized software, if the software itself has problems, it will also have an impact on the company's financial activities. Therefore, it is necessary to improve the security of computerized accounting software itself. For companies, it is necessary to use genuine system software, because compared with general system software, genuine software has a greater defense capability against viruses, and also has a higher analysis capability for external data [16]. For pirated system software, there may be problems such as lack of important files and unsafe decryption. In this case, it is easy to cause computerized accounting software to crash, and it will affect the performance of computerized accounting software. safety.

The computerized accounting system is a man-machine system, and personnel are a very important factor. Only when the personnel have a high comprehensive quality, can the normal operation of the computerized accounting software be guaranteed. Therefore, it is necessary to improve the quality of accounting computerized personnel, and should establish a multi-form, multi-level, multi-channel idea, and actively learn advanced ideas. For relevant institutions, it is possible to strengthen the training of accounting computerization talents, and invite some celebrities and experts to give lectures, so as to cultivate accounting computerization personnel to understand the latest knowledge and ideas. For enterprises, it is also necessary to cultivate the learning ability of practitioners to learn accounting computerized software, so as to maintain the normal operation of accounting computerized software and better ensure the security of the software [6].

In order to ensure the security of accounting computerized software, it is necessary to establish a sound accounting computerized management system, so as to provide a good environment for accounting and the transmission of important accounting information. First of all, a relatively complete computer operation system should be established, and the function authorization, operation process, category authorization, etc. should be clarified [7]. Secondly, a relatively clear post division system should be established, and the responsibilities and division of labor of each post should be clarified. Thirdly, an archives management system should be established to specify the number of archives, archive location, archive time, etc. Finally, a complete confidentiality system should be established to clarify the responsibilities of relevant personnel, so as to better protect the

security of information. Only by improving from these four aspects, can the security of software be guaranteed to a certain extent [9].

Risk of failure of accounting computerized systems. Computer accounting information system is mainly composed of hardware and software, hardware is the body of the system, software is the soul of the system. Due to mechanical failure, damage to spare parts, sudden power failure, operator error, etc., the hardware system may fail, and the software system will be damaged due to illegal calls and modifications. In the network environment, the openness, dynamism and virtuality of the network lead to the reduction of the consistency and controllability of the system. Once it encounters system blockage, virus intrusion or hacker attack, the system will be chaotic or even paralyzed [8].

Accounting information is a comprehensive reflection of the production and operation activities of an enterprise, which meets the needs of the internal management of the enterprise and the needs of relevant external departments and individuals[10]. The authenticity, integrity and accuracy of accounting information are the basic requirements for accounting information. Once the security of the accounting information system is compromised, the most direct is the error of accounting data, loss of data or tampering, resulting in information distortion. The unsafe factor here is The performance is as follows [11]: First, hardware defects, such as computer hard disk damage and data loss without data backup. The second is human misoperation and intentional destruction, resulting in data loss and tampering. The third is the external environment such as power outage during operation or the magnetic disk is magnetized to cause data loss. In addition, in the computerized network environment, the intrusion of some illegal users or the interception and tampering of data during the transmission of the network will also cause the information to be insecure.

Under computerized conditions, accounting data comes from original vouchers or bookkeeping vouchers, if there is no effective control. Once the wrong data is entered, the computer will accept this part of the data and process it automatically, which will lead to the continuity and repetition of errors, resulting in errors in the output of accounting books and accounting statements and other information. It is difficult to guarantee the authenticity and integrity of accounting data. In the network environment, accounting data is transmitted through communication lines, and the wide range of data sources makes it face illegal interception or modification by unauthorized personnel, and the security and reliability of accounting data are difficult to guarantee [12].

In the e-commerce environment of the network economy, business operations are increasingly dependent on customers, and online financial activities are increasing, such as online ordering, online sales, online settlement, online financial management, online securities investment and foreign exchange trading, etc. All of them are exchanges of information without face-to-face, and transactions are carried out entirely on the basis of the reputation of both parties. In this way, enterprises are faced with the security problem of financial settlement. Some illegal users invade other people's computer systems, illegally transfer electronic funds through network transmission, and steal passwords from banks. Deposits, causing corporate funds to face security risks [13].

In the process of implementing computerized accounting, due to insufficient understanding of ideological concepts and factors such as funds, computerized accounting has no professional guidance and systematic research, no excellent professional software and hardware equipment, and the implementation is blind to a certain extent. It is not solid and the operation is not standardized, which brings the phenomenon of data loss, system error analysis, and abnormal operation of the accounting information system to the scientific and standardized computer data processing [14]. The security deficiencies of the computerized information system have even affected the development of the network, informatization and financial management specialization of the computerized accounting of the unit. The hardware and software of the accounting information system itself are relatively high-tech, and the development is changing with each passing day.

Moreover, due to the fact that accounting computerization has many interdisciplinary disciplines, their respective development is also very rapid, which increases the difficulty of integration between other disciplines and accounting. The improvement of accounting computerized security control brings many uncertain factors [15]. Digital marketing channels provide a platform for accounting professionals, consultants, and experts to share their insights and thought leadership on computerized accounting security. Through blog posts, whitepapers, and social media engagement, these individuals can establish themselves as trusted authorities in the field, offering guidance and advice on implementing robust security controls and best practices.

In order to improve the security monitoring effect of computerized accounting software, this paper combines artificial intelligence technology to build a security monitoring system for computerized accounting software to improve the security monitoring effect of computerized accounting software.

2 THE SAFE PROCESSING ALGORITHM OF ACCOUNTING COMPUTERIZED SOFTWARE INFORMATION

2.1 Fundamentals of Differential Fault Attacks

For symmetric cipher algorithms, differential fault attacks can be divided into attacks on block cipher algorithms and attacks on stream cipher algorithms according to the object of the attack. Differential fault attacks can be classified into attacks based on statistical analysis techniques and attacks based on algebraic analysis techniques.

The model of differential fault attack is shown in Figure 1.

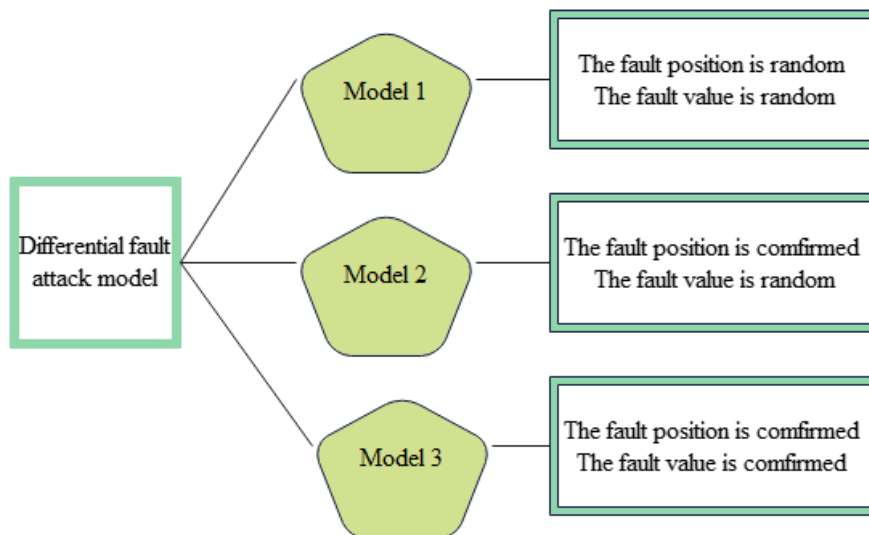


Figure 1: Differential fault attack model.

Among the three types of hypothetical models, model 1 has the weakest hypothesis, which is the closest to the actual cryptographic model, and model 2 has the next worst hypothesis. Model 3 has the strongest assumptions and it is the farthest from the actual cryptographic assumptions.

Hash function is a very important part in the field of cryptography. It has a very wide range of applications in the fields of information security such as data integrity detection, digital signature, and message authentication. The iterative structures of the MD series and SHA series Hash functions are based on the classic Merkle-Damgard (MD) iterative structure.

The definition of the MD iterative structure is: the message m after filling is divided into t message blocks m_0, \dots, m_{t-1} , and the length of each message block is k bits. We set $h_0 = iv$ to be an n -bit initial chain variable, $f: \{0,1\}^n \times \{0,1\}^k$ to be a compression function, and define $h_{i+1} = f(h_i, m_i) = E_{m_i}(h_i) + h_i, i = 0, 1, 2, \dots, t-1$, then the hash value of message m is $H(m) = h_t$, as shown in Figure 2. Among them, h_i is the intermediate chain variable, m_i is the message block, and E_{m_i} is the encryption algorithm with m_i as the key, which is referred to as the encryption mode of the Hash function.

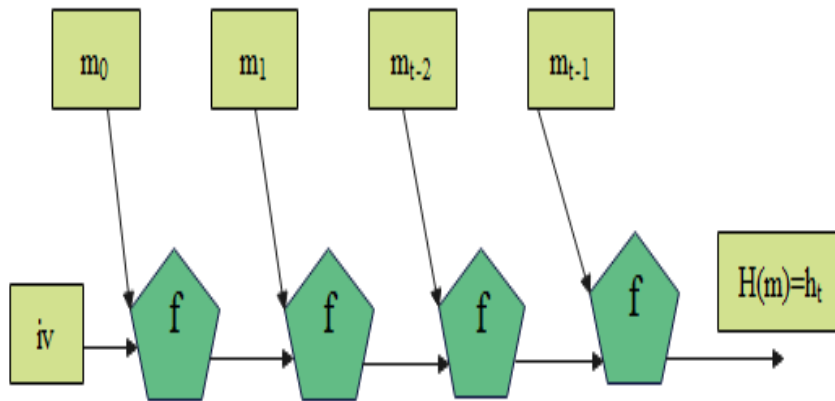


Figure 2: MD iteration structure of Hash function.

The iterative structure of the SIMON32/64 algorithm is shown in Figure 3. The iteration function is as follows:

$$\begin{cases} X_L^r = F(X_L^{r-1}) \oplus X_R^{r-1} \oplus K^r \\ X_R^r = X_L^{r-1} \end{cases}$$

Among them, the round function is $F(X) = (X \lll 2) \oplus ((X \lll 1) \wedge (X \lll 8))$. Here, X_L, X_R represents the left half and right half of the variable X , respectively, and K^r represents the $r+1$ th round key.

The key expansion scheme of SIMON32/64 is:

$$K^i = K^{i-2} \oplus (K^{i-1} \ggg) \oplus (K^{i-1} \gggg 4) \oplus c \oplus (Z_j)_i,$$

Among them, $i \leq r-1, K^0, K^1$ is the seed key, and there is $c = (2^n - 1) \oplus 3 = 0xFF \dots FF$, and the value of the constant $Z_j (j = 0, 1, 2, 3, 4)$ is shown in the literature.

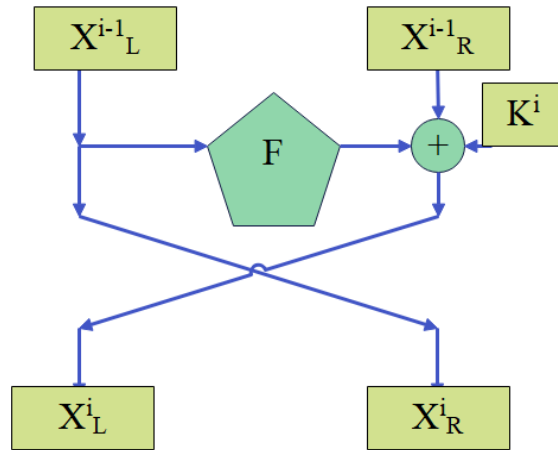


Figure 3: One-round iteration structure of SIMON algorithm.

This section adopts a byte-oriented fault-induction model whose basic assumptions are:

(1) An attacker can induce a fault on a selected byte in the left half of the intermediate variable, but we do not know the specific fault value.

(2) For the same plaintext P , the attacker can obtain the correct ciphertext C and the wrong ciphertext C^* under the action of the same seed key K .

According to the assumption of differential fault attack, after a plaintext P is selected to be encrypted, the corresponding correct ciphertext can be obtained. We encrypt the same plaintext with the same key, and after inducing a failure at some selected byte position of the intermediate variable, we can get the wrong ciphertext.

The plaintext $P = X_L^0 // X_R^0$ is selected, and the correct ciphertext obtained after encryption is $C = X_L^{r-1} // X_R^{r-1}$. We consider the last round, according to the structure of the iteration function, there is $C_L = X_R^{r-2} \oplus F(X_L^{r-2}) \oplus K^{r-1}, C_R = X_L^{r-2}$, so there is $K^{r-1} = X_R^{r-2} \oplus F(X_L^{r-2}) \oplus C_L = X_R^{r-2} \oplus F(C_R) \oplus C_L$. Since C_L and C_R are known, if we want to recover K^{r-1} , we only need to find X_R^{r-2} , which in turn has $X_L^{r-3} = X_R^{r-2}$ according to the structure

of the iterative function. This enlightens us from the penultimate round of import failures. Figure 4 shows the differential fault attack of the last two rounds of the SIMON algorithm.

According to the iterative function, there is $X_L^{r-2} = X_R^{r-3} \oplus F(X_L^{r-3}) \oplus K^{r-2}$, the fault δ is injected at X_L^{r-3} , and $(X_L^{r-2})^* = X_R^{r-3} \oplus F(X_L^{r-3} \oplus \delta) \oplus K^{r-2}$ can be obtained, then there is:

$$F(X_L^{r-3} \oplus \delta) \oplus F(X_L^{r-3}) = X_L^{r-2} \oplus (X_L^{r-2})^* \quad (1)$$

At the same time, there is $X_L^{r-2} = C_R$, so there is $X_L^{r-2} \oplus (X_L^{r-2})^* = C_R \oplus C_R^*$. We also notice $\delta = x_L^{r-3} \oplus (x_L^{r-3})^* = x_R^{r-2} \oplus (x_R^{r-2})^* = (C_L \oplus C_L^*) \oplus (F(C_R) \oplus F(C_R^*))$, then formula (1) can be transformed into:

$$F(X_L^{r-3} \oplus \delta) \oplus F(X_L^{r-3}) = C_R \oplus C_R^* \quad (2)$$

If we set $x = X_L^{r-3}$, $\Delta = C_R \oplus C_R^*$, $\delta = (C_L \oplus C_L^*) \oplus (F(C_R) \oplus F(C_R^*))$, it can be reduced to the situation of equation $F(x \oplus \delta) \oplus F(x) = \Delta$.

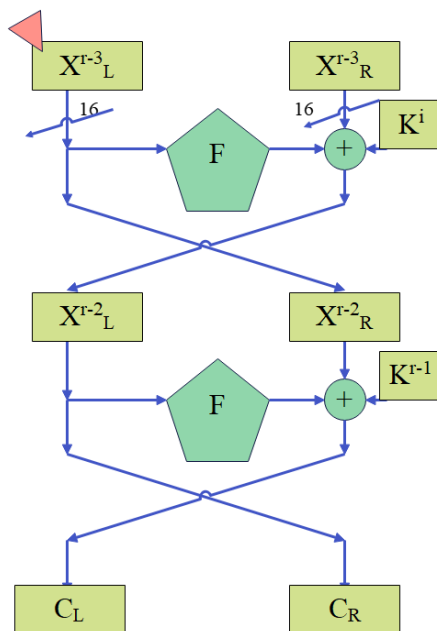


Figure 4: Differential fault attack of SIMON algorithm importing faults from the penultimate round.

For the difference equation $F(x \oplus \delta) \oplus F(x) = \Delta$, since both δ and Δ are known, the difference equation can be solved to obtain X_L^{r-3} , and then K^{r-1} can be obtained. When K^{r-1} is obtained, the values of X_L^{r-2} and X_R^{r-2} can be obtained by inverse solution one round, and then the fault is introduced in the penultimate third round, and the value of K^{r-2} can be obtained by similar analysis. In this way, the seed key can be obtained according to the key expansion scheme.

2.2 Differential Fault Attack of Shacal-2 Algorithm

The block length of SHACAL-2 algorithm is 256 bits, the key space is 512 bits, and the number of iteration rounds is 64 rounds. Its basic functions have the following 4, which are defined as follows. Among them, Ch and Maj are called the selection function and the majority function, respectively.

$$\begin{aligned}\Sigma_0(X) &= S_2(X) \oplus S_{13}(X) \oplus S_{22}(X); \\ \Sigma_1(X) &= S_6(X) \oplus S_{11}(X) \oplus S_{25}(X); \\ Ch(X, Y, Z) &= (X \wedge Y) \oplus (\bar{X} \wedge Z); \\ Maj(X, Y, Z) &= (X \wedge Y) \oplus (X \wedge Z) \oplus (Y \wedge Z)\end{aligned}$$

During the encryption process, the plaintext P is divided into eight 32-bit variables $A_0, B_0, C_0, D_0, E_0, F_0, G_0$ and H_0 . After 64 iterations, the corresponding ciphertext C consists of $A_{64}, B_{64}, C_{64}, D_{64}, E_{64}, F_{64}, G_{64}$ and H_{64} concatenated. The update process of one round of encryption function is shown in Figure 5.

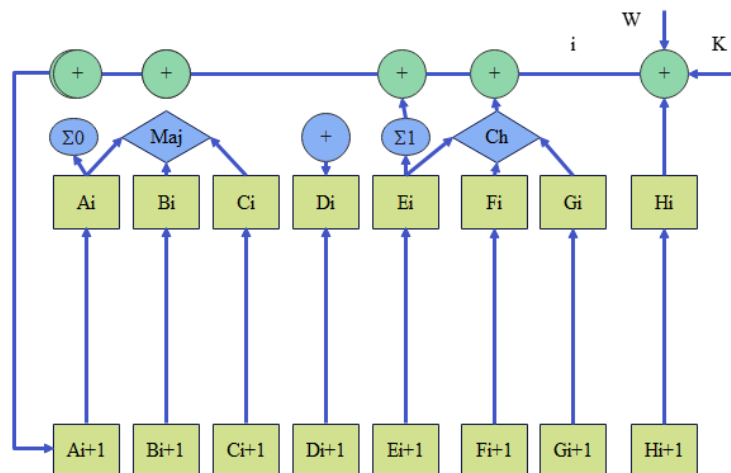


Figure 5: One-round encryption structure of SHACAL-2 algorithm.

There is:

$$\begin{aligned}
 T1_{i+1} &= H_i \boxplus \Sigma_1(E_i) \boxplus Ch(E_i, F_i, G_i) \boxplus K_i \boxplus W_i \\
 T2_{i+1} &= \Sigma_0(A_i) \boxplus Maj(A_i, B_i, C_i) \\
 H_{i+1} &= G_i; G_{i+1} = F_i; F_{i+1} = E_i; E_{i+1} = D_i \boxplus T1_{i+1} \\
 D_{i+1} &= C_i; C_{i+1} = B_i; B_{i+1} = A_i; A_{i+1} = T1_{i+1} \boxplus T2_{i+1}
 \end{aligned}$$

The seed key K of the SHACAL-2 algorithm is divided into 16 32-bit key words K_0, K_1, \dots, K_{15} , and the key arrangement algorithm expands these 16 seed keys into 64 round keys ($i = 16, 17, \dots, 63$)

$$K_i = \sigma_1(K_{i-2}) \boxplus K_{i-7} \boxplus \sigma_0(K_{i-15}) \boxplus K_{i-16}$$

Among them, there is:

$$\begin{aligned}
 \sigma_0(X) &= S_7(X) \oplus S_{18}(X) \oplus R_3(X) \\
 \sigma_1(X) &= S_{17}(X) \oplus S_{19}(X) \oplus R_{10}(X)
 \end{aligned}$$

In the SHACAL-2 algorithm, the selection function is defined as $Ch(x, y, z) = x \cdot y \oplus \bar{x} \cdot z$, and the majority function is defined as $Maj(x, y, z) = x \cdot y \oplus x \cdot z \oplus y \cdot z$.

In order to analyze the difference characteristics of the selection function and the majority function, the following Lemma 1 is given first:

Lemma 1: Equation $(z \oplus \delta) \boxplus z = \Delta$ is given, among them, z, δ, Δ is a 32-bit word. If it is assumed that δ, Δ is known and z is unknown, the following conclusions hold:

$$z_i = \begin{cases} 0 \text{ or } 1, i = 31 \\ 0 \text{ or } 1, \delta_i = 0, 0 \leq i \leq 30 \\ \delta_{i+1} \oplus \Delta_{i+1}, \delta_i = 1, 0 \leq i \leq 30 \end{cases}$$

For the selection function $Ch(x, y, z) = x \cdot y \oplus \bar{x} \cdot z$, the difference is induced at x , y and z , respectively, and the difference equations of the following three cases are obtained:

Scenario I: $Ch(x \oplus \delta, y, z) \boxplus Ch(x, y, z) = \Delta$

Scenario II: $Ch(x, y \oplus \delta, z) \boxplus Ch(x, y, z) = \Delta$

Scenario III: $Ch(x, y, z \oplus \delta) \boxplus Ch(x, y, z) = \Delta$

In the following discussion, according to the characteristics of the difference equations in the above three cases, the relationship between the number of values of the last known quantity z and the input difference δ will be deduced respectively. The main results are as follows:

Theorem 1: The selection function in the SHACAL-2 algorithm has the following differential characteristics: if the weight of the input differential δ is k , the number of unknowns that satisfy the equation of case I is 2^{32-k} . The number of unknowns that satisfy the equation of Case III cannot be determined by k alone.

Proof: First, according to the definition of the choice function, the difference equation for case I is

$$[(x \oplus \delta) \cdot y \oplus \overline{(x \oplus \delta)} \cdot z] \boxminus (x \cdot y \oplus \bar{x} \cdot z) = \Delta$$

$\overline{x \oplus \delta} = \bar{x} \oplus \delta$ is noticed. The difference equation above can be transformed into

$$\begin{aligned} \Delta &= (xy \oplus \delta y \oplus \bar{x}z \oplus \delta z) \boxminus (xy \oplus \bar{x}z) \\ &= ((xy \oplus \bar{x}z) \oplus \delta(y \oplus z)) \boxminus (xy \oplus \bar{x}z) \end{aligned}$$

We set $w = xy \oplus \bar{x}z$, then there is

$$\begin{aligned} (w \oplus \delta(y \oplus z)) \boxminus w &= \Delta \\ (w \oplus \delta(y \oplus z)) &= \Delta \boxplus w \end{aligned}$$

It expands by bit

$$\begin{cases} (w \oplus \delta(y \oplus z))_i = (\Delta \boxplus w)_i, 0 \leq i \leq 31 \\ w_i \oplus \delta_i(y_i \oplus z_i) = \Delta_i \oplus w_i \oplus c_i, 0 \leq i \leq 31 \end{cases} \quad (3)$$

Among them, there is

$$\begin{cases} c_i = w_{i-1} \Delta_{i-1} \oplus (w_{i-1} \oplus \Delta_{i-1}) c_{i-1} = w_{i-1} (\Delta_{i-1} \oplus c_{i-1}) \oplus \Delta_{i-1} c_{i-1}, 1 \leq i \leq 31 \\ c_0 = 0 \end{cases} \quad (4)$$

Formula (3) is simplified to

$$\delta_i(y_i \oplus z_i) = \Delta_i \oplus c_i, 0 \leq i \leq 31 \quad (5)$$

In formula (5), when there is $i=0$, there is $\delta_0(y_0 \oplus z_0) \oplus \Delta_0 = c_0 = 0$, so there is $\delta_0 z_0 = \Delta_0 \oplus \delta_0 y_0$. When there is $\delta_0 = 1$, z_0 can be uniquely determined. When there is $\delta_0 = 0$, z_0 can take the value 0 or 1.

When there is $1 \leq i \leq 3l$, there is

(1) If there is $\Delta_{i-1} \oplus c_{i-1} = 1$, there is $\Delta_{i-1}c_{i-1} = 0$, and $1 = \Delta_{i-1} \oplus c_{i-1} = \delta_{i-1}(y_{i-1} \oplus z_{i-1})$ is known from formula (5),

Therefore, there is

$$\begin{cases} y_{i-1} \oplus z_{i-1} = 1 \\ \delta_{i-1} = 1 \end{cases} \Rightarrow \begin{cases} z_{i-1} = \overline{y_{i-1}} \\ \delta_{i-1} = 1 \end{cases}$$

At this time, formula (4) becomes $c_i = w_{i-1}$, which is substituted into formula (5), there is

$$\begin{cases} \delta_i(y_i \oplus z_i) = \Delta_i \oplus w_{i-1} \\ \delta_i(y_i \oplus z_i) = \Delta_i \oplus x_{i-1}y_{i-1} \oplus \overline{x_{i-1}z_{i-1}} \\ \delta_i z_i = \Delta_i \oplus x_{i-1}y_{i-1} \oplus \overline{x_{i-1}z_{i-1}} \oplus \delta_i y_i = \Delta_i \oplus x_{i-1}y_{i-1} \oplus \overline{x_{i-1}y_{i-1}} \oplus \delta_i y_i, 1 \leq i \leq 3l \end{cases} \quad (6)$$

In formula (6), the right side is the known quantity. When there is $\delta_i = 1$, z_i can be uniquely determined. When there is $\delta_i = 0$, z_i can take the value 0 or 1;

(2) If there is $\Delta_{i-1} \oplus c_{i-1} = 0$, since Δ_{i-1} is given, c_{i-1} that satisfies this condition is determined, and there is $c_{i-1} = \Delta_{i-1}, c_{i-1}\Delta_{i-1} = \Delta_{i-1}^2 = \Delta_{i-1}$. At this time, formula (4) is $c_i = \Delta_{i-1}$, which is substituted into formula (5) to have

$$\begin{cases} \delta_i(y_i \oplus z_i) = \Delta_i \oplus c_i = \Delta_i \oplus \Delta_{i-1} \\ \delta_i z_i = \delta_i y_i \oplus \Delta_i \oplus \Delta_{i-1} \end{cases} \quad (7)$$

In formula (7), the right side is the known quantity. Therefore, when there is $\delta_i = 1$, z_i can be uniquely determined, and when there is $\delta_i = 0$, z_i can take the value 0 or 1.

(3) When there is $\Delta_i \oplus c_i = 1$, $\delta_i (y_i \oplus z_i) = 1$ is known from formula (5), then there are $\delta_i = 1$ and $z_i = y_i \oplus 1 = \bar{y}_i$, so z_i can be uniquely determined.

Therefore, when there is $\delta_i = 1 (1 \leq i \leq 31)$, from conditions (1) and (2), z_i can be uniquely determined. When there is $\delta_i = 0 (1 \leq i \leq 31)$, conditions (1) (2) (3) cannot uniquely determine z_i , and z_i can take 0 or 1. The case of $i=0$ has been given before. To sum up, the only equivalence condition for z_i is $\delta_i = 1$. Therefore, when the weight of δ is k , there are k components that are 1. At this time, the bit component z_i of z at the position corresponding to δ can be uniquely determined, and the remaining components can be 0 or 1. Therefore, in this case, the number of unknown quantities z that satisfy the difference equation is 2^{32-k} .

Therefore, for the case I, the following conclusions can be drawn: the relationship between the input difference δ that satisfies the difference equation and the final knowledge z is: when there is $W(\delta) = k$, there is $N(z) = 2^{32-k}$.

Second, according to the definition of the selection function, the equation for case II is

$$[x(y \oplus \delta) \oplus \bar{x}z] \boxminus (xy \oplus \bar{x}z) = \Delta$$

It can be further transformed into $((xy \oplus \bar{x}z) \oplus x\delta) \boxminus (xy \oplus \bar{x}z) = \Delta$, we set $w = xy \oplus \bar{x}z$, it can be simplified to:

$$(w \oplus x\delta) \boxminus w = \Delta \quad (8)$$

For formula (8), since x, δ is given, w is a function of the unknown quantity z . From Lemma 1, except for the highest bit, if we want to determine that $z_i (0 \leq i \leq 30)$ needs to have $(x\delta)_i = x_i \delta_i = 1$, that is, $x_i = 1$ and $\delta_i = 1$, there is $w_i = y_i$, so the value of z cannot be determined, and each bit of it can take 0 or 1. Therefore, the number $N(z)$ of the last known quantity satisfying the difference equation has nothing to do with δ , so there is $N(z) = 2^{32}$.

Finally, the equation for case III is $(x \cdot y \oplus \bar{x} \cdot (z \oplus \delta)) \boxminus (x \cdot y \oplus \bar{x} \cdot z) = \Delta$, which can be further transformed into

$$by((xy \oplus \overline{xz}) \oplus \overline{x\delta}) \boxminus (x \cdot y \oplus \overline{x} \cdot z) = \Delta$$

We set $w = xy \oplus \overline{xz}$, then the equation can be simplified to

$$(w \oplus \overline{x\delta}) \boxminus w = \Delta \quad (9)$$

For formula (9), since x, δ is given, w is a function of the unknown quantity z . From Lemma 1, it can be known that except for the highest bit, in order to determine $z_i (0 \leq i \leq 30)$, we need to have $(\overline{x\delta})_i = \overline{x_i} \delta_i = 1$, that is, $\overline{x_i} = 1$ and $\delta_i = 1$. At this time, there is $z_i = w_i = \overline{x_{i+1}} \delta_{i+1} \oplus \Delta_{i+1}$, so there is

$$z_i = \begin{cases} 0 \text{ or } 1, i = 31 \\ 0 \text{ or } 1, \delta_i = 0 \text{ or } x_i = 1, 0 \leq i \leq 30 \\ \overline{x_{i+1}} \delta_{i+1} \oplus \Delta_{i+1}, \delta_i = 1 \text{ and } x_i = 0, 0 \leq i \leq 30 \end{cases}$$

This shows that whether any bit of the final quantity z except the highest bit can be determined is not only related to the corresponding δ component, but also related to the corresponding x component. Therefore, the number of unknowns that satisfy the difference equation cannot be determined by δ alone. The proof is complete.

For the difference characteristic of the majority function $Maj(x, y, z) = x \cdot y \oplus xz \oplus y \cdot z$, the difference is induced at x , y , and z respectively, and the difference equations of the following three cases are obtained:

$$\text{Scenario IV: } Maj(x \oplus \delta, y, z) \boxminus Maj(x, y, z) = \Delta$$

$$\text{Scenario V: } Maj(x, y \oplus \delta, z) \boxminus Maj(x, y, z) = \Delta$$

$$\text{Scenario VI: } Maj(x, y, z \oplus \delta) \boxminus Maj(x, y, z) = \Delta$$

According to the characteristics of the difference equations in the above three cases, the relationship between the number of values of the last known quantity z and the input difference δ is inferred, and the results are as follows:

Theorem 2: The majority function in the SHACAL-2 algorithm has the following differential characteristics: if the weight of the input differential δ is k , the number of unknown quantities satisfying the equation of case **IV** is 2^{32-k} . The number of unknowns that satisfy the equation of

case V is 2^{32-k} . Moreover, the number of unknowns that satisfy the equation of case VI cannot be determined by k alone.

Proof: According to the definition of the majority function, the difference equation of case IV can be transformed into:

$$[(xy \oplus xz \oplus yz) \oplus \delta(y \oplus z)] \boxminus (xy \oplus xz \oplus yz) = \Delta$$

We set $w = xy \oplus xz \oplus yz$, then there is $[w \oplus \delta(y \oplus z)] \boxminus w = \Delta$, which is exactly similar to the structure of case I. Therefore, it is proved by the same method that the same result can be obtained.

That is, the relationship between the input difference δ and the final knowledge z that satisfies the difference equation is: when there is $W(\delta) = k$, there is $N(z) = 2^{32-k}$.

The equation for case V can be reduced to $[x(y \oplus \delta) \oplus xz \oplus (y \oplus \delta)z] \boxminus (xy \oplus xz \oplus yz) = \Delta$.

Since x and y in the majority function are symmetric, from the case V , the relationship between the input difference δ that satisfies the difference equation and the final known quantity z is: when there is $W(\delta) = k$, there is $N(z) = 2^{32-k}$.

Finally, the difference equation for Case VI is $[xy \oplus x(z \oplus \delta) \oplus y(z \oplus \delta)] \boxminus (xy \oplus xz \oplus yz) = \Delta$. With simple variable substitution, the above equation is transformed into:

$$[(xy \oplus xz \oplus yz) \oplus \delta(x \oplus y)] \boxminus (xy \oplus xz \oplus yz) = \Delta,$$

We set $w = xy \oplus xz \oplus yz$, then there is $[w \oplus \delta(x \oplus y)] \boxminus w = \Delta$. From Lemma 1, when there is $\delta_i(x_i \oplus y_i) = 1$, that is, $\delta_i = 1$ and $(x_i \oplus y_i) = 1$, w_i can be uniquely determined except for the highest bit. At this time, there is $w_i = x_i y_i \oplus x_i z_i \oplus y_i z_i = x_i y_i \oplus (x_i \oplus y_i) z_i = z_i$, so there is

$$z_i = \begin{cases} 0 \text{ or } 1, i = 31 \\ 0 \text{ or } 1, \delta_i = 0 \text{ or } x_i \oplus y_i = 0, 0 \leq i \leq 30 \\ \delta_{i+1}(x_{i+1} \oplus y_{i+1}) \oplus \Delta_{i+1}, \delta_i = 1 \text{ and } x_i \oplus y_i = 1, 0 \leq i \leq 30 \end{cases}$$

This shows that whether a certain bit of the final unknown quantity z except the highest bit can be determined is not only related to the corresponding δ component, but also related to the

corresponding x , y components. Therefore, the number of unknowns that satisfy the difference equation cannot be determined by δ alone.

The theorem is proved.

A plaintext $P = (A_0, B_0, C_0, D_0, E_0, F_0, G_0, H_0)$ is randomly selected, and the correct ciphertext $Y = (A_{64}, B_{64}, C_{64}, D_{64}, E_{64}, F_{64}, G_{64}, H_{64})$ can be obtained after encryption. If we assume that a random failure based on a 32-bit word is introduced somewhere in the intermediate state, and the corresponding error ciphertext is obtained:

$$Y^* = (A_{64}^*, B_{64}^*, C_{64}^*, D_{64}^*, E_{64}^*, F_{64}^*, G_{64}^*, H_{64}^*)$$

Since, there is

$$\begin{aligned} A_{64} &= T1_{64} \boxplus T2_{64} \\ &= H_{63} \boxplus \Sigma_1(E_{63}) \boxplus Ch(E_{63}, F_{63}, G_{63}) \boxplus K_{63} \boxplus W_{63} \boxplus \Sigma_0(A_{63}) \boxplus Maj(A_{63}, B_{63}, C_{63}) \\ &= H_{63} \boxplus \Sigma_1(F_{64}) \boxplus Ch(F_{64}, G_{64}, H_{64}) \boxplus K_{63} \boxplus W_{63} \boxplus \Sigma_0(B_{64}) \boxplus Maj(B_{64}, C_{64}, D_{64}) \end{aligned}$$

Therefore, in the above equation, except that H_{63} and K_{63} are known, in order to solve K_{63} , we only need to know H_{63} . At the same time, there is $H_{63} = G_{62}$, so there is an option to enter a fault in the penultimate round. The update process by the encryption function is:

$$\begin{aligned} A_{63} &= T1_{63} \boxplus T2_{63} = H_{62} \boxplus \Sigma_1(E_{62}) \boxplus Ch(E_{62}, F_{62}, G_{62}) \boxplus K_{62} \\ &\boxplus W_{62} \boxplus \Sigma_0(A_{62}) \boxplus Maj(A_{62}, B_{62}, C_{62}) \end{aligned} \quad (10)$$

In formula (10), in order to obtain the value of G_{62} , it is necessary to select a position to induce a fault in the penultimate round. The literature mentions that only E_{62} is a valid differential fault location, but no theoretical explanation is given. According to the differential characteristics of the selection function, that is, from Theorem 1, it can be seen that only when the first position of the selection function, that is, the input fault at E_{62} , the effective information of G_{62} can be obtained, and the effective information of G_{62} cannot be obtained when F_{62}, G_{62} is selected. Therefore, E_{62} is a valid differential fault location.

As shown in Figure 6, when the input fault is at E_{62} , according to the update process of the iterative function, A_{63}, E_{63}, F_{63} has a difference in the output value of the second last round, $A_{64}, B_{64}, E_{64}, F_{64}, G_{64}$ has a difference in the output value of the last round, and there is no difference in the rest of the positions. When fault δ is entered at E_{62} , we get:

$$A_{63}^* = H_{62} \boxplus \Sigma_1(F_{63} \oplus \delta) \boxplus Ch(F_{63} \oplus \delta, G_{63}, H_{63}) \boxplus K_{62} \boxplus W_{62} \boxplus \Sigma_0(B_{63}) \boxplus Maj(B_{63}, C_{63}, D_{63})$$

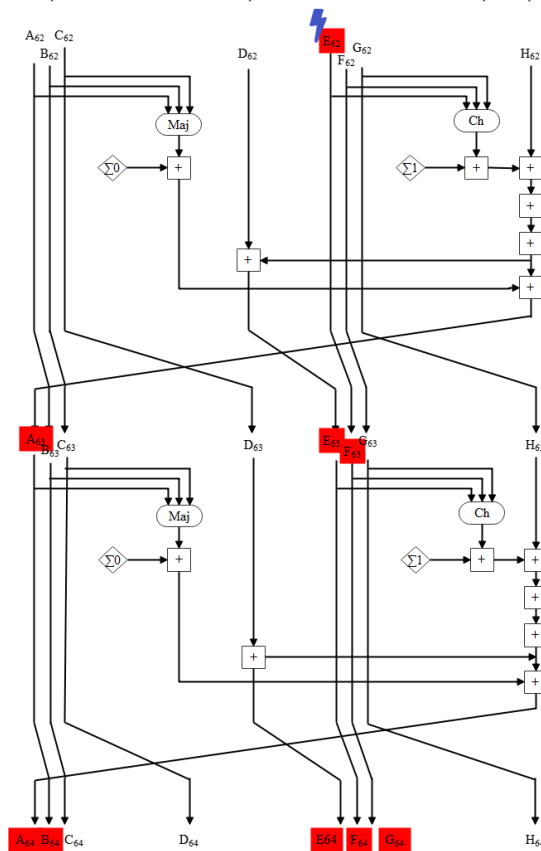


Figure 6: Differential fault attack on the last two rounds of SHACAL-2 algorithm.

According to the encryption process, it can be known that:

$$\begin{aligned} B_{64}^* &= H_{62} \boxplus \Sigma_1(G_{64} \oplus \delta) \boxplus Ch(G_{64} \oplus \delta, H_{64}, H_{63}) \\ &\boxplus K_{62} \boxplus W_{62} \boxplus \Sigma_0(C_{64}) \boxplus Maj(B_{63}, C_{63}, D_{63}) \end{aligned} \quad (11)$$

Similarly, according to the encryption process, formula (10) can be transformed into:

$$\begin{aligned}
B_{64} &= H_{62} \boxplus \Sigma_1(G_{64}) \boxplus Ch(G_{64}, H_{64}, H_{63}) \boxplus K_{62} \\
&\boxplus W_{62} \boxplus \Sigma_0(C_{64}) \boxplus Maj(B_{63}, C_{63}, D_{63})
\end{aligned} \tag{12}$$

The formula (11) and formula (12) are modulo-subtracted and sorted out:

$$\Delta' = Ch(G_{64} \oplus \delta, H_{64}, H_{63}) \boxminus Ch(G_{64}, H_{64}, H_{63}) \boxplus (\Sigma_1(G_{64} \oplus \delta) \boxminus \Sigma_1(G_{64})) \tag{13}$$

Among them, there is $\Delta' = B_{64}^* \boxminus B_{64}$, and formula (13) is the difference equation for solving H_{63} in the literature.

The algebraic solution of formula (13) can be given directly by using the differential characteristic of the selection function. Next, the relationship between the successful probability of differential fault attack and the number of induced faults in SHACAL-2 algorithm is given by theoretical derivation.

We set $\Delta = \Delta' \boxminus (\Sigma_1(G_{64} \oplus \delta) \boxminus \Sigma_1(G_{64}))$, $x = G_{64}$, $y = H_{64}$, $z = H_{63}$, then formula (13) can be changed to:

$$Ch(x \oplus \delta, y, z) \boxminus Ch(x, y, z) = \Delta$$

This corresponds to Case I. Therefore, the differential fault attack on the SHACAL-2 algorithm can be attributed to the differential properties of the selection function.

The difference equation of case I is denoted as $(z; x, y, \delta, \Delta)$, then the following conclusion holds:

Theorem 3: For m difference equations $(z; x, y, \delta^{(j)}, \Delta^{(j)})(1 \leq j \leq m)$, among them, $\delta^{(j)}(1 \leq j \leq m)$ is a randomly selected 32-bit word, the probability that the final unknown quantity z can be uniquely determined is $P_l = [1 - (1/2)^m]^{32}$.

Proof: According to the proof process of Theorem 1, the value of each bit of the unknown variable z only depends on the value of the corresponding δ component. When there is $\delta_i = 1(0 \leq i \leq 31)$, z_i can be uniquely determined. We set A_i to denote that there exists at least some integer j such that $\delta_i^j = 1, 1 \leq j \leq m$. We note that each δ_i^j is chosen independently and randomly. Therefore, there is $P(A_i) = 1 - (1/2)^m$, and since each A_i is independent of each other, the probability that the unknown quantity z can be uniquely determined is

$$P_1 = \prod_{i=0}^{31} P(A_i) = \left[1 - (1/2)^m\right]^{32}$$

Proof is complete

The attacker can obtain m difference equations $(z; x, y, \delta^{(j)}, \Delta^{(j)}), 1 \leq j \leq m$, by inducing m faults in appropriate positions. At this time, the probability that the unknown z can be uniquely solved through

the difference equation is $\left[1 - (1/2)^m\right]^{32}$, and the corresponding round key can be determined through the solution of the difference equation. According to the key expansion scheme, if the round

key $(K_{48}, K_{49}, \dots, K_{63})$ of the last 16 rounds is recovered, the seed key can be completely recovered. If it is assumed that the number of faults induced in 16 consecutive rounds is

m_1, m_2, \dots, m_{16} , the number of differential faults required at this time is $n = \sum_{i=1}^{16} m_i$, and the

$$P_2 = \prod_{i=1}^{16} \left[1 - (1/2)^{m_i}\right]^{32}$$

probability of recovering the unique seed key is , the following conclusions are established.

Theorem 4: If a unique seed key is recovered with a given success probability ρ , that is, there is

$P_2 = \prod_{i=1}^{16} \left[1 - (1/2)^{m_i}\right]^{32} = \rho$, when there is $m_1 = m_2 = \dots = m_{16} = m$, the required total number of

$$n = \sum_{i=1}^{16} m_i = 16m$$

failures n is the smallest. At this point, there is

Proof: Since there is $\prod_{i=1}^{16} \left[1 - \left(\frac{1}{2^{m_i}}\right)\right]^{32} = \rho$, there is $\prod_{i=1}^{16} \left[1 - \left(\frac{1}{2^{m_i}}\right)\right] = \rho^{\frac{1}{32}}$, and $\rho_0 = \rho^{\frac{1}{32}}$ is logged, we set:

$$f(m_1, m_2, \dots, m_{16}) = \prod_{i=1}^{16} \left[1 - \left(\frac{1}{2^{m_i}}\right)\right] - \rho_0, g(m_1, m_2, \dots, m_{16}) = \sum_{i=1}^{16} m_i$$

Then, from the method of finding the conditional extreme value of multivariate functions in mathematical analysis, the constraints are:

$$f(m_1, m_2, \dots, m_{16}) = 0,$$

The objective function is:

$$g(m_1, m_2, \dots, m_{16})$$

We set

$$h(m_1, m_2, \dots, m_{16}, \lambda) = g(m_1, m_2, \dots, m_{16}) + \lambda f(m_1, m_2, \dots, m_{16}),$$

Then, the set of equations satisfied when reaching the extreme condition is:

$$\begin{cases} \frac{\partial h}{\partial m_j} = 1 + \lambda \prod_{i=1, i \neq j}^{16} \left(1 - \frac{1}{2^{m_i}}\right) 2^{-m_j} \ln 2 = 0, j = 1, 2, \dots, 16 \\ \prod_{i=1}^{16} \left(1 - \left(\frac{1}{2^{m_i}}\right)\right) - \rho_0 = 0 \end{cases} \quad (14)$$

We set $1 \leq j_k, j_l \leq 16, j_k \neq j_l$, and from formula (14), we get:

$$\begin{cases} \frac{\partial h}{\partial m_{j_k}} = 1 + \lambda \prod_{i=1, i \neq j_k}^{16} \left(1 - \frac{1}{2^{m_i}}\right) 2^{-m_{j_k}} \ln 2 = 0 \\ \frac{\partial h}{\partial m_{j_l}} = 1 + \lambda \prod_{i=1, i \neq j_l}^{16} \left(1 - \frac{1}{2^{m_i}}\right) 2^{-m_{j_l}} \ln 2 = 0 \end{cases}$$

The two equations are subtracted to get:

$$\lambda \left(2^{-m_{j_k}} - 2^{-m_{j_l}}\right) \prod_{i=1, i \neq j, i \neq j_k}^{16} \left(1 - \frac{1}{2^{m_i}}\right) \ln 2 = 0$$

At the same time, there is $1 - \frac{1}{2^{m_i}} \neq 0, i = 1, 2, \dots, 16$, and there is $\lambda \neq 0$, so there is $2^{-m_{j_k}} - 2^{-m_{j_l}} = 0$. Therefore, $m_{j_k} = m_{j_l}$ can be obtained.

From the arbitrariness of the value of j_k, j_l , it can be known that $m_1 = m_2 = \dots = m_{16} = m$ is substituted into formula (14) to obtain $m = -\log_2 \left(1 - \rho^{1/(32 \times 16)}\right)$. At this point, the objective function achieves the minimum value, that is, there is

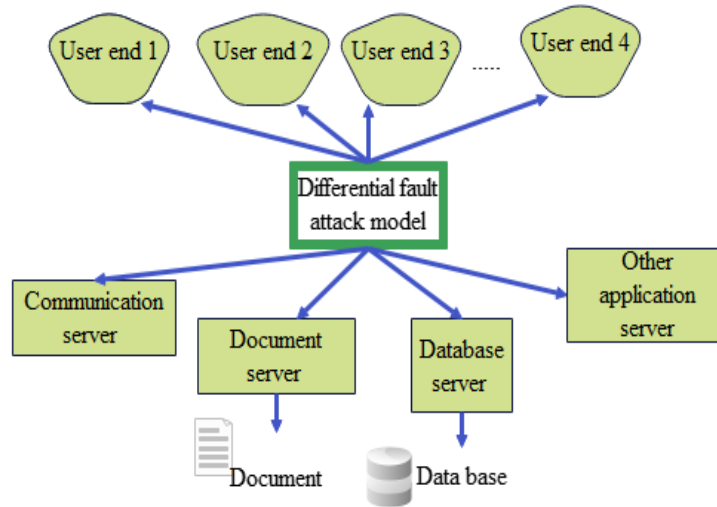
$$n = \sum_{i=1}^{16} m_i = 16m = -16 \log_2 \left(1 - \rho^{1/(32 \times 16)}\right)$$

The proof is complete.

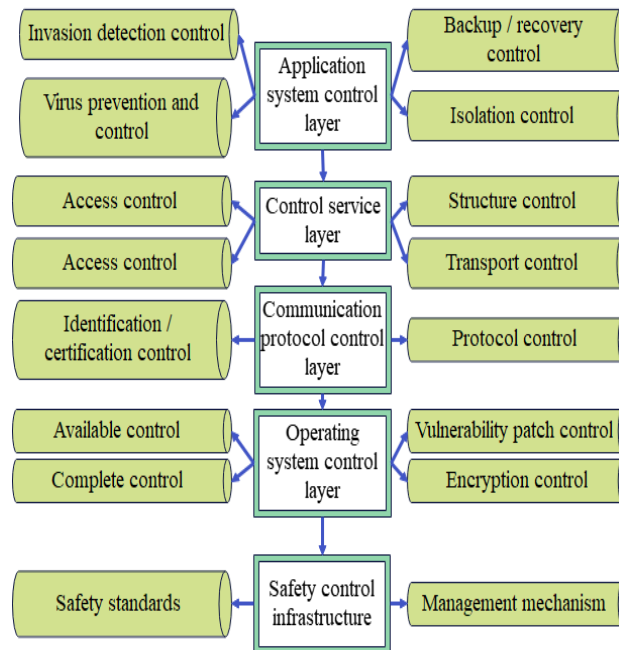
From Theorem 4, when the success probability ρ is given, in order to minimize the total number of faults, the number of faults $m_i (1 \leq i \leq 16)$ injected in each round needs to be equal, that is, $m_1 = m_2 = \dots = m_{16} = m$. At this point, there is $P_2 = \left(1 - (1/2)^m\right)^{32 \times 16}$.

3 ACCOUNTING COMPUTERIZED SOFTWARE SECURITY MONITORING SYSTEM

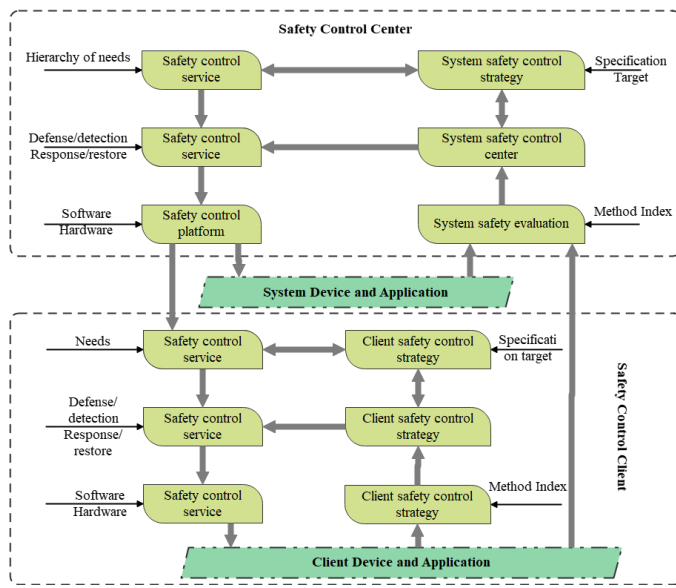
According to the concept of client/server, an accounting computerized system is established. The architecture of the client/server model is shown in Figure 7(a).



(a) Architecture of the schema



(b) Security control system



(c) Safe control principle model of C/S mode

Figure 7: Accounting computerized software safety monitoring system.

As can be seen from the hierarchical structure in the figure, the lower layer is the foundation of the upper layer and provides technical support for the upper layer; the upper layer is the extension and progression of the lower layer. Moreover, all levels are interdependent and interrelated to form a unified whole. Therefore, in order to realize the safety and controllability of the whole system, it is necessary to realize the advancement of safety control technology at all levels. According to the research on the security technology and control principle of the computerized accounting system, the corresponding security control system is shown in Figure 7(b). According to the architecture of the C/S mode and the security control principle model of the accounting computerized system, the security control principle model of the C/S mode is constructed, as shown in Figure 7(c).

After the above system model is constructed, the security monitoring effect of the model is evaluated, and it is verified by multiple groups of simulated attacks, and the experimental verification results shown in Table 1 are obtained.

<i>Number</i>	<i>Safety</i>	<i>Number</i>	<i>Safety</i>	<i>Number</i>	<i>Safety</i>
1	89.736	21	94.702	41	94.002
2	89.045	22	93.672	42	91.082
3	88.738	23	87.559	43	93.419
4	87.020	24	92.286	44	92.339

5	87.771	25	93.923	45	90.314
6	91.423	26	91.256	46	87.829
7	94.295	27	93.580	47	92.191
8	94.686	28	89.099	48	92.575
9	90.918	29	87.035	49	90.724
10	95.005	30	87.265	50	94.085
11	91.803	31	87.550	51	88.839
12	92.194	32	90.263	52	95.176
13	90.067	33	93.166	53	88.611
14	88.036	34	94.647	54	93.502
15	95.891	35	88.827	55	89.188
16	91.729	36	90.608	56	89.946
17	94.883	37	90.119	57	91.535
18	94.824	38	93.099	58	89.779
19	94.923	39	89.937	59	88.806
20	87.078	40	94.672	60	95.302

Table 1: Evaluation of the security monitoring effect of computerized accounting software.

Through the above research, it can be seen that the security monitoring effect of the computerized accounting software proposed in this paper has a good effect, and can effectively improve the security of the computerized accounting software.

4 CONCLUSION

Information technology has developed rapidly, and the application of computer technology has become more and more extensive. Under this premise, computerized accounting has been produced. Accounting computerization is the abbreviation for the application of modern electronic and information technology in traditional accounting work, and is the basis for accounting to enter informationization. It is the process of using electronic computers to replace manual accounting, accounting and reporting, and partially replacing the human brain to complete the analysis, prediction and decision-making of accounting information. It changes the manual bookkeeping

method of traditional accounting, enables accountants to spend time and energy on the analysis and synthesis of capital data, and ensures the accuracy and timeliness of accounting information. It has strengthened financial management and capital monitoring, improved the efficiency of capital use, and reduced capital risks, thus promoting the management of enterprises, and computerized accounting has become a requirement of the development of the times. However, at the same time, when applying accounting computerized software, there will be some risks, and even financial information may be leaked. Therefore, in order to reduce the occurrence of risks, it is necessary to pay attention to the security of computerized accounting software. In order to improve the security monitoring effect of computerized accounting software, this paper combines artificial intelligence technology to build a security monitoring system for computerized accounting software. The research shows that the security monitoring effect of the computerized accounting software proposed in this paper has a good effect, which can effectively improve the security of the computerized accounting software.

Yang Jin, <https://orcid.org/0009-0003-6518-7996>

REFERENCES

- [1] Aaron, A. P.; Kohlstrand, M. L.; Welborn, L. V.; Curvey, S. T.: Maintaining medical record confidentiality and client privacy in the era of big data: ethical and legal responsibilities, *Journal of the American Veterinary Medical Association*, 255(3), 2019, 282-288. <https://doi.org/10.2460/javma.255.3.282>
- [2] Abdualgalil, B.; Abraham, S.: Efficient Machine Learning Algorithms for Knowledge Discovery in Big data: A literature Review, *Database*, 29(5), 2020, 3880-3889.
- [3] Al Natour, J. R. A. Q.: The Impact of Information Technology on The Quality of Accounting Information, *Turkish Journal of Computer and Mathematics Education*, 12(13), 2021, 885-903.
- [4] Ali, B. J.; Oudat, M. S.: Accounting Information System And Financial Sustainability Of Commercial And Islamic Banks: A Review Of The Literature, *Journal of Management Information and Decision Sciences*, 24(5), 2021, 1-17.
- [5] Almutairi, B.L.S: Impact Of Covid19 On Accounting Profession From The Perspective Of A Sample Of Head Of Accounting Departments Within Kuwaiti Manufacturing Sector, *Psychology and Education Journal*, 58(2), 2021, 4758-4768. <https://doi.org/10.17762/pae.v58i2.2867>
- [6] Brock, V.; Khan, H. U.: Big data analytics: does organizational factor matters impact technology acceptance?, *Journal of Big Data*, 4(1), 2017, 1-28. <https://doi.org/10.1186/s40537-017-0081-8>
- [7] Chessell, D.; Neguriță, O.: Smart industrial value creation, cyber-physical production networks, and real-time big data analytics in sustainable Internet of Things-based manufacturing systems, *Journal of Self-Governance and Management Economics*, 8(4), 2020, 49-58. <https://doi.org/10.22381/JSME8420205>
- [8] De Laat, P. B.: Algorithmic decision-making based on machine learning from Big Data: Can transparency restore accountability?, *Philosophy & Technology*, 31(4), 2018, 525-541. <https://doi.org/10.1007/s13347-017-0293-z>
- [9] de Laat, P.B.: Big data and algorithmic decision-making: can transparency restore accountability?, *Acm Sigcas Computers and Society*, 47(3), 2017, 39-53. <https://doi.org/10.1145/3144592.3144597>
- [10] Handoko, B. L.; Mulyawan, A. N.; Tanuwijaya, J.; Tanciady, F.: Big Data in Auditing for the Future of Data Driven Fraud Detection, *International Journal of Innovative Technology and Exploring Engineering*, 9(3), 2020, 2902-2907. <https://doi.org/10.35940/ijitee.B7568.019320>

- [11] Huerta, E.; Jensen, S.: An accounting information systems perspective on data analytics and Big Data, *Journal of Information Systems*, 31(3), 2017, 101-114. <https://doi.org/10.2308/isys-51799>
- [12] Kumar, K. S.: Factors affecting the adoption of computerized accounting system (CAS) among smes in Jaffna District, *SAARJ Journal on Banking & Insurance Research*, 8(6), 2019, 11-15. <https://doi.org/10.5958/2319-1422.2019.00022.5>
- [13] Lanlan, Z.; Ahmi, A.; Popoola, O. M. J.: Perceived ease of use, perceived usefulness and the usage of computerized accounting systems: A performance of micro and small enterprises (mses) in china, *International Journal of Recent Technology and Engineering*, 8(2), 2019, 324-331. <https://doi.org/10.35940/ijrte.B1056.0782S219>
- [14] Loku, L.; Fetaji, B.; Krstev, A.: Automated medical data analyses of diseases using big data, *Knowledge-International Journal, Scientific Papers*, 28(5), 2018, 1719-1724. <https://doi.org/10.35120/kij28051719L>
- [15] Marshall, T. E.; Lambert, S. L.: Cloud-based intelligent accounting applications: accounting task automation using IBM watson cognitive computing, *Journal of Emerging Technologies in Accounting*, 15(1), 2018, 199-215. <https://doi.org/10.2308/jeta-52095>
- [16] Zhao, H.; Liu, Z.; Yao, X.; Yang, Q.: A machine learning-based sentiment analysis of online product reviews with a novel term weighting and feature selection approach, *Information Processing & Management*, 58(5), 2021, 102656. <https://doi.org/10.1016/j.ipm.2021.102656>