Research on Application of Missile Blockchain Based on Nation Secret Algorithm

Yi Fang*, Linhu Cong, Jianqiu Deng, Weixin He and Yuliang Chen
Naval Aeronautical University, Yantai, Shandong, 264001, China
*Corresponding author’s e-mail: 395510796@qq.com

Abstract. Missile data has the characteristics of multiple data items, large data volume and high data value, which puts forward higher requirements for data storage security. The application of blockchain technology in missile business data storage can realize the safe, reliable and decentralized storage of data. The SM3 algorithm is a Hash function that supports the data structure and detects whether the data is tampered with in the blockchain. The SM3 algorithm is applied to the missile business blockchain to realize the localization of encryption, and the operation of SM3 algorithm is optimized under the condition that the missile business data contains a large number of documents, tables and pictures. Finally, the Go language was used for testing, and the results showed that the operation speed of SM3 algorithm could be improved by about 30% through optimization, and the optimization effect was obvious.

1. Introduction
The missile service data includes all kinds of data generated in the process of using, storing and maintaining the missile. By analyzing the missile service data, the state, performance and fault of the missile can be evaluated, which plays an important role in training and actual combat. However, at present, most of the data records still use paper records and centralized storage, which leads to low reliability of data and unclear data source, hidden dangers such as data tampering and loss, and great risks.

The technical features of blockchain such as tamper-proof, traceable and decentralized data [1] provide technical support for the safe storage of missile business data. Since the blockchain technology was proposed, especially in recent years, attention has been rising rapidly in China. It has been studied in the application of medical [2], energy [3], identity authentication [4], finance [5], notarization [6] and other fields. In terms of military, some scholars to blockchain in military application foreground is prospected [7], the blockchain on military data security are studied, put forward a kind of "active integrity protection" the data security of new scheme [8], but not for chain blocks in the application of a particular military scenarios were studied.

The core foundation of blockchain is cryptography, among which a kind of important algorithm is cryptographic Hash algorithm (Hash algorithm), which belongs to one of the three categories of cryptography algorithms [9]. Classical Hash algorithms include MD5, SHA, SM3, etc. SM3 algorithm is the national commercial password hashing algorithm issued by China's password authority. When using blockchain platforms such as hyperledger for application development, the commonly used Hash algorithm is sha-256 algorithm instead of SM3 algorithm.

Missiles often generate data in the form of pictures and documents when carrying out various businesses. The data stored in the traditional blockchain are generally in the form of messages and strings. It is not difficult to imagine that the Hash algorithm is slow in generating a fixed-length
summary of data in the form of pictures, documents and so on, and consumes a lot of hardware resources at the same time.

To solve above problems, this article will block chain technique is applied to missile business data recording, storage of military scenario, SM3 algorithm is chosen as the chain block application of Hash algorithm, at the same time, according to the characteristics of the missile business data form and SM3 algorithm, in the image data, documents and other forms of computing is improved, and make it more suitable for the actual situation of force to carry out the business of missile, but also achieve the "localization" of chain block encryption algorithm.

2. Blockchain and Hash functions

2.1 Structure of blockchain
From the perspective of structure, blockchain is a specific data structure that combines data blocks in the form of chains in a chronological order, and a decentralized public ledger that cannot be tampered with or falsified in a cryptographic way [10]. Blockchain can be regarded as a kind of linked list using hash values as Pointers. Each block contains data and a pointer to the previous block Hash value (the creation block does not include the previous block Hash value).

2.2 Hash function
Hash function is a kind of function which can construct arbitrary long message into fixed length data. Hash function generally has anti - bump and unidirectional, anti - bump is divided into weak anti - bump and strong anti - bump. Weak collision resistance means that it is difficult to find another message with the same hash value as this message; Strong collision resistance means that it is difficult to find two different messages with the same hash value. One-way means that the message cannot be derived from the hash value. Due to the characteristics of Hash function, it is widely used in data integrity detection, message authentication, digital signature, pseudo-random number generation, one-time password and other aspects [11].

Hash function is a general term for a class of functions that contain many specific algorithms, such as sha-1, sha-256, RIPEMD160, MD5, SM3, sha-3, etc. [12]. Among them, the strong collision resistance of MD5 algorithm and sha-1 algorithm has been broken, proving that it is not safe [13].

At present, the widely used Hash algorithms are all based on Merkle-Damgard (MD structure) iterative Hash algorithm, and there are also sponges, such as sha-3 function algorithm, wide-pipe structure, HAIFA structure and so on. MD structure is a special Hash algorithm to construct anti-collision based on iterative structure, that is, anti-collision password is constructed by anti-collision compression function to construct anti-collision Hash algorithm. The Hash function constructed in this way is anti-collision as long as the compression function satisfies the anti-collision property.

3. SM3 algorithm
SM3 algorithm is an iterative Hash algorithm proposed in China, and its input and output are bitstrings. The output length of SM3 algorithm is 256 bits, message grouping is 512 bits, using MD structure. For messages with a length less than \(2^n\) bit, the SM3 algorithm is populated and iteratively compressed to generate a hash value of 256 bits. The specific algorithm is described as follows.

3.1 The function definitions
Boolean functions \(FF_j(X,Y,Z)\), \(GG_j(X,Y,Z)\) and displacement function \(P_j(X,Y,Z)\), \(P_j(X,Y,Z)\) are defined in the SM3 algorithm:

\[
FF_j(X,Y,Z) = \begin{cases} 
X \oplus Y \oplus Z & 0 \leq j \leq 15 \\
(X \land Y) \lor (X \land Z) \lor (Y \land Z) & 16 \leq j \leq 63
\end{cases}
\]
\( GG_j(X, Y, Z) = \begin{cases} X \oplus Y \oplus Z & 0 \leq j \leq 15 \\ (X \land Y) \lor (\neg X \land Z) & 16 \leq j \leq 63 \end{cases} \)

- \( P_0(X) = X \oplus (X \lll 9) \oplus (X \lll 17) \)
- \( P_1(X) = X \oplus (X \lll 15) \oplus (X \lll 23) \)

Where, \( X, Y \) and \( Z \) are all bit strings with a length of 32.

### 3.2 Pad
For a message of bit length, first add bit "1" to the end of the message, and then add \( k \) "0", where \( k \) is the minimum non-negative integer that satisfies \( l + 1 + k \equiv 448 \mod 512 \), and then add a 64-bit length \( l \) binary bit string. The length of the filled message is a multiple of 512.

### 3.3 Iterative compression
The populated messages are grouped into groups of 512 bits in length, and the grouped messages are numbered: \( B^{(0)}B^{(1)} \ldots B^{(n-1)} \), and \( n = (l + k + 65) + 512 \). Iterate over the grouped populated messages as follows:

\[
\text{FOR } i = 0 \text{ TO } n - 1 \\
\quad V^{(i+1)} = CF \left( V^{(i)}, B^{(i)} \right) \\
\text{END FOR}
\]

Where \( CF \) is the compression function, \( V^{(0)} \) is the initial value, and the length is 256 bits. The result after the last iteration is \( V^{(n)} \).

### 3.4 Message extension
Grouped messages \( B^{(i)} \) for extension to generate words \( W_0, W_1, \ldots, W_{63}, W_0', W_1', \ldots, W_{63}' \), for the \( CF \) function. The message group is first divided into 16 words \( W_0, W_1, \ldots, W_{15} \). Expand according to the following methods:

\[
\text{FOR } j = 16 \text{ TO } 67 \\
\quad W_j = P \left( W_{j-16} \oplus W_{j-1} \oplus \left( W_{j-3} \lll 15 \right) \oplus \left( W_{j-15} \lll 7 \right) \oplus W_{j-6} \right) \\
\text{END FOR}
\]

\[
\text{FOR } j = 0 \text{ TO } 63 \\
\quad W'_j = W_j \oplus W_{j+4} \\
\text{END FOR}
\]

### 3.5 Compression function
The calculation process of the compression function is as follows:

\[
\begin{align*}
ABCDEFGHI & \leftarrow V^{(i)} \\
\text{FOR } j = 0 \text{ TO } 63 \\
\quad SS1 & \leftarrow \left( (A \lll 12) + E + (T_j \lll j) \right) \lll 7 \\
\quad SS2 & \leftarrow SS1 \oplus (A \lll 12) \\
\quad TT1 & \leftarrow FF_j(A, B, C) + D + SS2 + W'_j \\
\quad TT2 & \leftarrow GG_j(E, F, G) + H + SS1 + W'_j \\
\quad D & \leftarrow C \\
\quad C & \leftarrow B \lll 9
\end{align*}
\]
Where, A, B, C, D, E, F, G, H is the intermediate variable and SS1, SS2, TT1, TT2 is the word register. And the storage mode of the word is big-end storage. The final output hash value of 256 bits is y = ABCDEFGH.

4. Improvement of SM3 algorithm

4.1 SM3 algorithm performance test

The platform and environment used in the performance test of SM3 algorithm are as follows: Intel Core i7-6700hq CPU @2.60Ghz, 8G ddr4-2133mhz, Windows 7 x64, Go v1.21.1, JetBrains GoLand 2017.3.3x64.

Some scholars have analyzed the security of SM3 algorithm in their research, and used collision attack, preimage attack, discriminator attack and other methods to verify the high security of SM3 cryptographic hashing algorithm. SM3 algorithm is implemented with Go language, and its performance is tested with the testing tool in the testing package provided by Go language.

Performance analysis of stress tests is performed using the pprof performance analysis tool built into the Go language. At the end of the test, the top command is used to obtain the top ten time-consuming and resource-consuming functions, as shown in figure 1.

![Fig.1 Operating time](image)

As can be seen from the figure, the compression function takes up more than 65% of the time, so the focus is on the improvement and optimization of the compression function.

4.2 Improvement strategy

According to the above description of SM3 algorithm, the main process of the compression function is the assignment of intermediate variables, shift operation and data reading and writing in the register, and the use of multiple intermediate variables and multiple registers, reading and writing the data in the register occupies a lot of operation time. Thus by optimizing the intermediate variable to read and write data in a register, reduce the number of ways to achieve the purpose of reducing operation time compression function, use this method to improve at the same time also does not destroy the original compression function structure, ensure the result is still reliable. Intermediate variables SS1, SS2, TT1, TT2 are all in the compression function, so you need to reduce the use of these intermediate variables. At the same time, combined with the optimization scheme of the message extension part, on the basis of the above description of SM3 algorithm, the optimization improvement
scheme mainly focuses on the first four steps of the compression function loop body, and the remaining identical parts are not given anymore. The description of the compression function after optimization and improvement is as follows:

\[
\begin{align*}
TT1 & \leftarrow FF_j(A,B,C)+D+\left((A \lll 12)+E+(T_j \lll j)\right) \lll 7 \oplus (A \lll 12) + W_j \oplus W_{j+4} \\
if \ j \geq 16 \\
TT2 & \leftarrow GG_j(E,F,G)+H+\left((A \lll 12)+E+(T_j \lll j)\right) \lll 7 + P(W_{j+6} \oplus W_{j+9} \oplus W_{j+15}) \oplus (W_{j+13} \lll 7) \oplus W_{j+6} \\
else \\
TT2 & \leftarrow GG_j(E,F,G)+H+\left((A \lll 12)+E+(T_j \lll j)\right) \lll 7 \oplus W_j \\
D & \leftarrow C \\
C & \leftarrow B \lll 9 \\
\end{align*}
\]

\[\ldots\]

4.3 Performance comparison

The running time and resource share of the optimized improvement scheme proposed in this paper are shown in figure 2. Compared with the running situation of the original SM3 algorithm, the total running time is reduced by about 25%, among which the efficiency of the compression function is significantly improved by about 30%, which proves that the optimized improvement scheme can effectively improve the running efficiency of SM3 algorithm.

\[\text{Fig.2 Operating time after improved}\]

5. Conclusion

Hash function plays an important role in the blockchain data structure. It can generate a fixed-length summary of any message through calculation, providing technical support for tamper-proof and traceability of blockchain data. The SM3 algorithm is a commercial cipher hashing algorithm published by China's cryptographic administration. It uses many other techniques not used by hashing algorithms in its design, and has better performance than the traditional sha-256 and RIPEMD160 algorithms used in the blockchain. This paper mainly studies the application of SM3 algorithm in blockchain, and improves the SM3 algorithm according to the characteristics of a large number of documents, pictures and other types of data stored in missile business data storage. The test results show that the improved strategy proposed in this paper increases the execution speed by about 30% compared with the original SM3 algorithm. The conclusion proves that this scheme can effectively improve the operation speed of SM3 algorithm input as document, picture, table and other types of data, so that the SM3 algorithm is more suitable for missile service Blockchain application system.

References

[1] Yuan Y, Wang F.Y. Blockchain: The State of the Art and Future Trends [J]. ACTA Automatica Sinica, 2016(04):481-494.
[2] Xue T.F., Fu Q.C., Wang C, et al. A Medical Data Sharing Model via Blockchain [J]. ACTA Automatica Sinica, 2017(09):1555-1562.
[3] She W, Hu Y, Yang X.Y., et al. Virtual Power Plant Operation and Scheduling Model Based on Energy Blockchain Network[J]. Proceedings of the CSEE, 2017(13):3729-3736.
[4] Tang L.T., Xu M, Jin Y.R. [J/OL]. 2019, 36(10). [2018-06-19]. http://www.arocmag.com/article/02-2019-10-20.html.

[5] Xu W.H., Zhou F. Application of the Theory of Blockchain in Finance[J]. Informatization Research, 2018(02):74-78.

[6] Zhou Z.C., Li L.X., Li Z.H. Efficient Cross-domain Authentication Scheme Based on Blockchain Technology [J]. Journal of Computer Applications, 2018(02):316-320+326.

[7] Sun Y, Lei Z, Cui P.Z. Blockchain Technology and Its Application in Military Field [J]. China Computer and Communication, 2017(19):136-138.

[8] Sun Y, Lei Z, Zhan G.Y. Security of Military Data Based on Blockchain [J]. Journal of Command and Control, 2018(03):189-194.

[9] Zhao J, Zeng X.W., Guo Z.C. Comparison and Analysis of Domestic and International Common Hash Algorithms[J]. Journal of Network New Media, 2018(05):58-62

[10] Cai W.D., Yu L, Wang R, et al. Blockchain Application Development Techniques[J]. Journal of Software, 2017(06):1474-1487.

[11] Wang X.Y., Yu H.B. SM3 Cryptographic Hash Algorithm [J]. Journal of Information Security Research, 2016(11):983-994.

[12] Xu J, Wen Q.Y., Wang D.Y. A New Message Authentication Code Based on Hash Function and Block Cipher[J]. Chinese Journal of Computers, 2015(04):793-803.

[13] Wang X.Y., Yu H.B. How to break MD5 and other hash functions.[C]// Advances in Cryptology EUROCRYPT 2005. Heidelberg: Springer Berlin, 2005:19-35.