Twin Concept for stream cipher algorithms

Dr. Abdulkareem O.Ibadi
Baghdad College For Economic Sciences

Abstract

Twin algorithm is a new concept of designing stream cipher algorithm using well-known pre-tested algorithms to immune the known plaintext attack and the correlation attack. In this paper, simple twin, ternary, and quaternary variants algorithms are discussed with periods 2P, 3P, 4P respectively, where P is the period of the base algorithm. The complexity and randomness properties are the same as the base algorithm.

1. Introduction

The conversion of data into a secret code for transmission over a public network is called cryptography. Today, most cryptography is digital, and the original text ("plaintext") is turned into a coded equivalent called "ciphertext" via an encryption algorithm. The ciphertext is decrypted at the receiving end and turned back into plaintext [1].

Encryption algorithm, or cipher, is a mathematical function used in the encryption and decryption process - series of steps that mathematically transforms plaintext or other readable information into unintelligible ciphertext. A cryptographic algorithm works in combination with a key (a number, word, or phrase) to encrypt and decrypt data. To encrypt, the algorithm mathematically combines the information to be protected with a supplied key. The result of this combination is the encrypted data. To decrypt, the algorithm performs a calculation combining the encrypted data with a supplied key. The result of this combination is the decrypted data. If either the key or the data is modified, the algorithm produces a different result. The goal of every encryption algorithm is to make it as difficult as possible to decrypt the generated ciphertext without using the key.

If we look at the types of cryptographic algorithms that exist in a little bit more detail, we see that the symmetric ciphers can be divided into stream ciphers and block ciphers, as shown in Fig. 1.

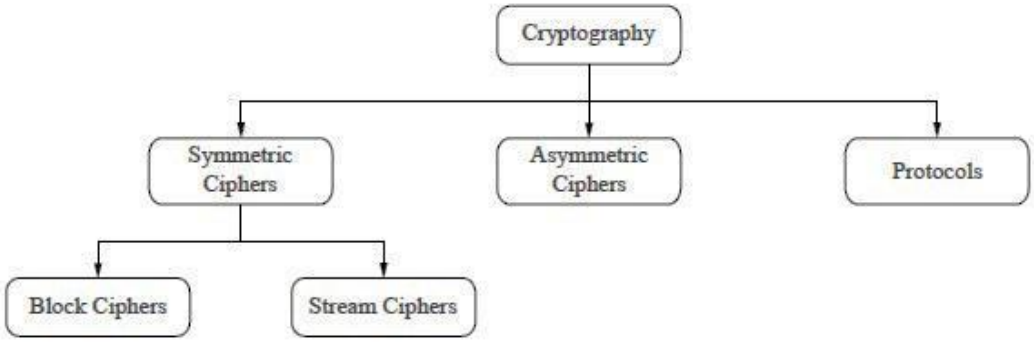

Fig. 1 Main areas within cryptography

A stream cipher is a cipher that makes use of an algorithmic procedure to produce an unending sequence of binary digits which is then combined either with plaintext to produce ciphertext or with ciphertext to recover plaintext as shown in fig. 2 [2].

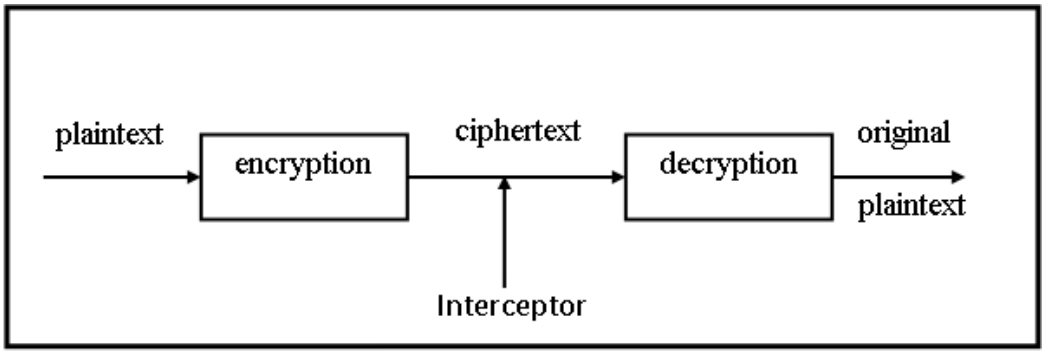

Figure 1: encryption and decryption

Binary stream ciphers are often constructed using linear feedback shift registers (LFSRs) because they can be easily implemented in hardware and can be readily analyzed mathematically. A stream cipher algorithms that consist LFSR's are called LFSR's stream ciphers. The use of LFSRs on their own, however, is insufficient to provide good security. Various schemes have been proposed to increase the security of LFSR [1].

2. Unbreakable ciphers

Unbreakable ciphers are possible. But the key must be randomly selected and used only once, and its length must be equal to or greater than that of the plaintext to be enciphered. Therefore such long keys, called one-time tapes, are not practical in data-processing applications. To work well, a key must be of fixed length, relatively short, and capable of being repeatedly used without compromising security [3]. In theory, any algorithm that uses such a finite key can be analyzed; in practice, the effort and resources necessary to break the algorithm would be unjustified.

3. Strong algorithms

Fortunately, to achieve effective data security, construction of an unbreakable algorithm is not necessary. However, the work factors (a measure, under a given set of assumptions, of the requirements necessary for a specific analysis or attack against a cryptographic algorithm) required to break the algorithm must be sufficiently great. Included in the set of assumptions is the type of information expected to be available for cryptanalysis. For example, this could be ciphertext only; plaintext (not chosen) and corresponding ciphertext; chosen plaintext and corresponding ciphertext; or chosen ciphertext and corresponding recovered plaintext [4].

A strong cryptographic algorithm must satisfy the following conditions[5]:

(1) The algorithm's mathematical complexity prevents, for all practical purposes, solution through analytical methods.

(2) The cost or time necessary to unravel the message or key is too great when mathematically less complicated methods are used, because either too many computational steps are involved (for example, in trying one key after another) or because too much storage space is required (for example, in an analysis requiring data accumulations such as dictionaries and statistical tables).

To be strong, the algorithm must satisfy the above conditions even when the analyst has the following advantages [6]:

(1) Relatively large amounts of plaintext (specified by the analyst, if so desired) and corresponding ciphertext are available.
(2) Relatively large amounts of ciphertext (specified by the analyst, if so desired) and corresponding recovered plaintext are available.

(3) All details of the algorithm are available to the analyst; that is, cryptographic strength cannot depend on the algorithm remaining secret.

(4) Large high-speed computers are available for cryptanalysis.

4. The twin concept

Fig. 3 shows the main components of the twin generator concept. Key generator algorithm is one of the well-known stream cipher algorithms which is used twice but with different initializations to construct the twin algorithm.

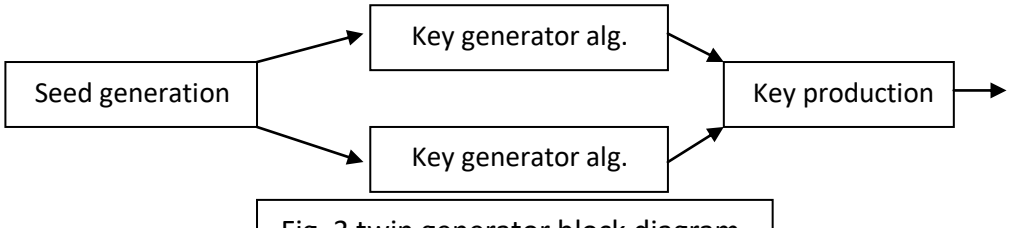

Fig. 3 twin generator block diagram.

The seed generation is the procedure of generating a seed for each of the twin algorithm from an input seed key. Key production is a two inputs function (a generated bit from each algorithm) and has one output bit as produced key bit.

5. Seed Key Generation

The input seed key of the twin generator is used to produce the initializations of both of the twin algorithm which must be **different**. There are several proposed procedures of generation some of them are:

a) Doubling the size of the seed key: by input seed key with length of double the size of the length of seed key of the used key generator algorithm or by double permutated the input seed key as shown in fig. 4.

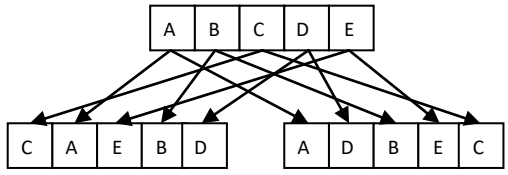

Fig. 4 Seed key permutation

b) Using one way function: the input of the function is the seed key and the output has a length of the double of the size of the seed key or greater which divided into two parts one for each algorithm.

c) Using stream cipher algorithm to generate initial state for each of the twin algorithm. This algorithm may be the same of the used algorithm in the twin fashion.

d) Using Initial Vector (IV) of the same length of the seed key and used as a part of the initial state of each algorithm.

6. Key Production

A function is used to produce the output key sequence and may have the following alternatives:

a) Linear function: simple XOR function its input are the output of each of the twin algorithm.

b) Nonlinear procedure: using the outputs of the twin algorithm in additional to extra bits from both of them.

c) Stream cipher algorithm with warm-up stage used the addition of the twin outputs as initialization state. This algorithm may be the same of the used algorithm in the twin fashion.

7. Simple twin algorithm

A simple twin algorithm may consist of an LFSR of length N and a permutation seed key generation and Xor production key sequence. For example, if n=5 then the simple twin algorithm will be as shown in fig. 5.

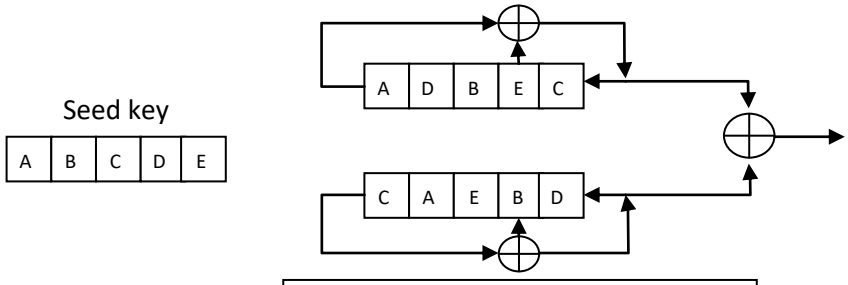

Fig. 5 Simple twin Algorithm

As shown in fig. 5, the tapping stages of the LFSR are 5 and 2. The simple twin algorithm will be used to evaluate the features of the twin concept algorithm.

8. Twin concept Features

The features of the stream cipher twin algorithm are the period, the complexity, and the randomness properties. All of these features are depending on the key production function. For the twin algorithm depicted in fig. 5, the features can be evaluated as:

a) The period = P, where P is the period of single LFSR (for N=5, P=31).

b) The complexity of the simple twin algorithm is the same as the single LFSR if the seed permutation is fixed and known (for N=5, the complexity equal 2^5).

c) The simple twin algorithm can be approved to have randomness properties because the output of an LFSR has randomness properties besides it has been proven that the xoring of two random sequences will yield a random sequence.

9. Analysis study

In an analysis study the conclusion is that the simple twin algorithm has the same feature as a single LFSR, which is not a good throughput for using such concept.

To enhance the throughput of the simple twin algorithm its period must be greater than single LFSR, this can be done by changing the output sequence of each LFSR. For example, by feeding the output of one LFSR to the feedback function of the second LFSR the period will be 2P. The output key sequence produced from a simple twin algorithm of LFSR of length 4 with tapping stages (4, 2), initialized by (0111) will be 010001000101000001000000010101 repeatedly. The period equal 30 which is equal to $2*(2^4-1) = 2P$.

The complexity of the twin algorithm can be increased by using IV or by using stream cipher algorithm in the seed key generation as discussed in the previous section. In the simple twin algorithm if IV is used in the seed key generation the complexity will be 2^{n+m}, where n is the length of the LFSR, m is the length of IV.

According to the above required modifications the proposed simple twin algorithm depicted in fig. 6.

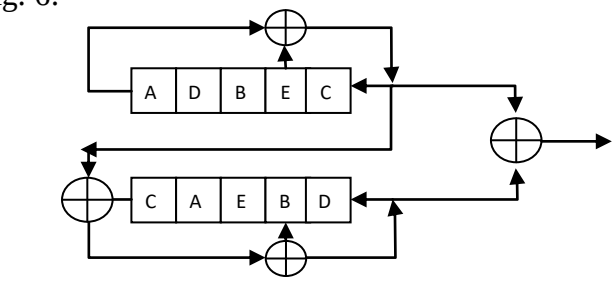

Fig. 6 Proposed Simple twin Algorithm

10. Twin algorithm variants

Fig. 7 shows one of the most important twin algorithm design. This design consists of three stages; they are the seed key generation feed up stage, the twining stage, and the initialization stage of key production.

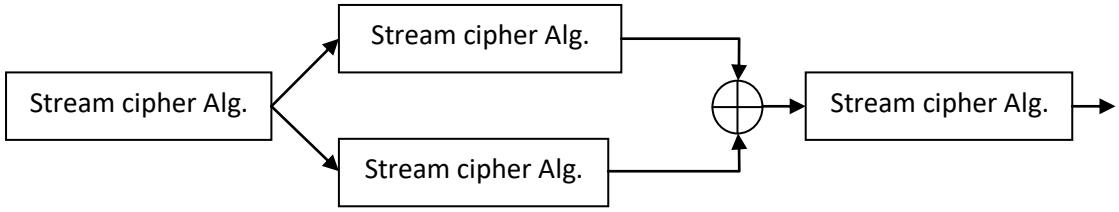

Fig. 7. Quaternary Twin algorithm

The stream cipher algorithm used in the Quaternary Twin algorithm must be equivalent in the twining parts only, the others can be different. The period of the quaternary algorithm will be 4P.

The quaternary simple twin algorithm (as shown in fig.8) has four equivalent LFSR's.

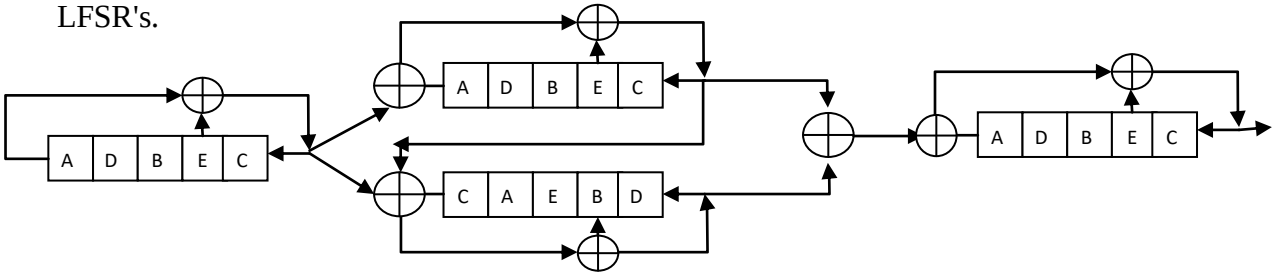

Fig. 8 Quaternary Simple twin Algorithm

The seed key generation feeding one LFSR at a time. After filling the second LFSR the seed key generation stage is stopped and then the second stage is started to fill the key production stage. The last two stages are working together to produce the key sequence that will be used for encryption or decryption. The ternary twin algorithm is other twin algorithm variants where the twining stage and the key production stage have the same base algorithm only.

Any known well tested stream cipher algorithm can be used in quaternary twin algorithm like Geffe, bless, trivium, and others. Fig. 9 shows Geffe quaternary twin algorithm.

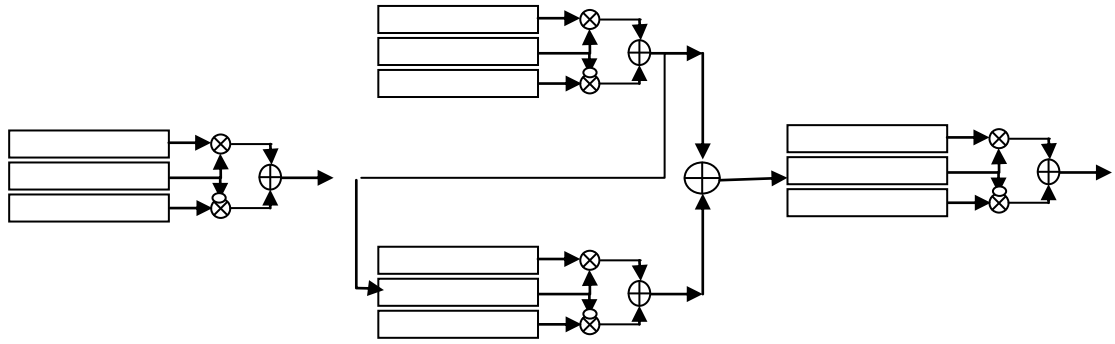

Fig. 9, Geffe quaternary twin algorithm

11. Conclusions

One of the most important benefits of the twin concept is to generate period equal to 2P, 3P, 4P from a well-tested known algorithm of period equal to P by designing ternary and quaternary forms of the twin algorithm.

The second benefit of designing the twin algorithm is the economical benefit; a single hardware chip set of the base algorithm will be used to build the twin hardware with extra memory. This benefit is necessary to reduce the gap between the high processor speed and the relatively low transmission speed.

The computational complexity and randomness features of the twin algorithm are equivalent to or depending on the selected base algorithm.

Crypanalyticaly, The twin concept design has a good immunity for known plaintext attack and the correlation attack.

12. References

[1] C. Paar, J. Pelzl, *Understanding Cryptography*, Springer-Verlag Berlin Heidelberg, 2010.

[2] Christof Paar, Jan Pelzl, "Understanding Cryptography, A Textbook for Students and Practitioners". (Companion web site contains online cryptography course that covers stream ciphers and LFSR), Springer, 2009.

[3] Matt J. B. Robshaw, Stream Ciphers Technical Report TR-701, version 2.0, RSA Laboratories, 1995.

[4] Khaled Merit, Abdelazziz Ouamri, "Securing Speech in GSM Networks using DES with Random Permutation and Inversion Algorithm", International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.4, July 2012

[5] Ashraf D. Elbayoumy and Simon J. Shepherd," Stream or Block Cipher for Securing VoIP?", International Journal of Network Security, Vol.5, No.2, PP.128–133, Sept. 2007.

[6] Tin Lai Win, and Nant Christina Kyaw, "Speech Encryption and Decryption Using Linear Feedback Shift Register (LFSR)", World Academy of Science, Engineering and Technology 48 2008.