2012 Second International Conference on Instrumentation & Measurement, Computer, Communication and Control

Overview of the Block Cipher

Hai Cheng, Qun Ding
Heilongjiang University
Key Laboratory of Electronic Engineering, College of Heilongjiang Province
Harbin, China
chengh@hlju.edu.cn, qunding@yahoo.cn

***Abstract*— Since the introduction of the Data Encryption Standard (DES) in the mid-1970s, block cipher is a wildly used algorithm in modern society. Along with the deep cryptanalysis, drawbacks of block cipher such as DES have been found which means improvement of cryptology should be done to face the challenge. Some block cipher algorithms such as SM4 are proposed to strong security. This paper describes the basic block cipher algorithm, design theory and structure, and cryptanalysis according to recent trend of development.**

Keywords-block cipher; cryptography; cryptanalysis

I. INTRODUCTION

For quite a long time, the word security plays a special role in our day-to-day lives. And there is no activity that does not depend on computers and network instead of face-to-face. Vast amount of personal data are maintained by Banks and credit card companies. Report of losing account and cipher can been seen in the news. Identity theft is well on its way to becoming a flourishing industry.

Cryptography now plays an important role in modern society, and it can solve problem that involve secrecy, authentication, integrity, and dishonest people. Cryptography is well-established science.

Modern information theory was first published in 1948 by Claude Elmwood Shannon. There are two basic types of encryption. One is symmetric (shared private key), the other is asymmetric (public key) encryption. Public key encryption means there are two keys, a public (shared) key, and a mathematical-related private key. Since the introduction of the data encryption standard (DES) in the mid-1970s, block ciphers have played an increasing role in cryptology. The growing numbers of practical applications rely on the security. Now block ciphers have received, and still receiving a lot of attention from academic cryptanalysts.

The reset of this paper is organized as follows. The Part two talks about symmetric-key cryptography, and part three talks about basic design theory and structure about block cipher, part four talks about cryptanalysis of block cipher.

II. INTRODUCTION OF BLOCK CIPHER ALGORITHM

A block cipher is a deterministic algorithm on fixed-length groups of bits, which is called blocks with an unvarying transformation that is called by a symmetric key. Practical symmetric encryption system processes plaintext messages unit by unit, and in the case of a block cipher a unit is called a block. Consequently, the block cipher maps plaintext message blocks of a special length into cipher text blocks of the same length.

A symmetric encryption system or cipher consists of the following five components:

- A plaintext message space M
- A ciphertext space C
- A key space K
- A family $E = \{E_k : k \in k\}$ of encryption functions $E_k : M \to C$
- A family $D = \{D_k : k \in k\}$ of decryption functions $D_k : C \to M$

In every practically relevant symmetric encryption system, equation is represented as follow

$$D_k(E_k(m)) = m \tag{1}$$

a) DES

The Data Encryption Standard (DES), known as Data Encryption Algorithm by ANSI, has been a worldwide algorithm more than thirty years. The DES was developed by IBM Corporation. And it was published in 1976. The most well-know and popular symmetric block cipher nowadays is DES. And the DES has been the most wildly used encryption algorithm until recently. It exhibits the classic Feistel structure.

DES has a block size of 64 bits and a key size of 56 bits. The key consists of eight groups, and each group has eight bits. There is one bit of eight which means a parity Chechnya bit that makes the overall parity in each block odd. So although the key size appears to be 64 bits, the effective key size is bits.

DES consists of 16 identical rounds. The 64 input bits are separated into 2 parts: the 32 leftmost bits part L and 32 rightmost parts R.

In each round, a new L and R are redefined by the (2) and (3) which is shown in Figure 1:

$$L_i = R_{i-1}, 1 \le i \le 16 \tag{2}$$

$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i), 1 \le i \le 16 \tag{3}$$

Here, K_i stands for a subsequence from the key K.

978-0-7695-4935-4/12 $26.00 © 2012 IEEE
DOI 10.1109/IMCCC.2012.379

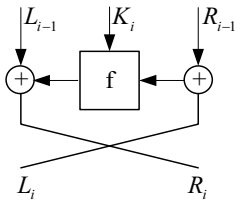

Figure 1. The Feistel structure of DES

But the DES has two main defects.

- The effective key size is only 56 bits, and amount of total key size is $2^{56} \approx 10^{17}$. An exhaustive key search is, at least in principle, possible.
- The most important module of DES is s-box. And it makes the nonlinear transformation. Statistical tests however show that there tables are not completely random. Maybe there is a hidden trapdoor in s-box.

During the first twenty years, nobody can crack the DES algorithm. However, in 1998, EFF cracks the DES within 56 hours by using a computer which costs 250 thousands dollars. In 1999 EFF breaks the challenge by a more brute-force attack just within 22.25 hours.

Even though the DES algorithm has security weaknesses, some alternatives have found based on DES algorithm. One alternative is tripe DES, often denoted as 3DES. 3DES consists of three subsequent DES encryptions shown in (4).

$$y = DES_{\mathbf{k}_3}(DES_{\mathbf{k}_2}(DES_{\mathbf{k}_1}(x))) \tag{4}$$

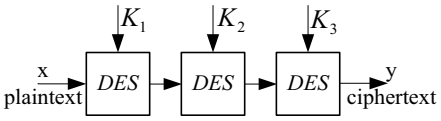

Figure 2. Triple DES (3DES)

Triple DES seems resistant to both exhausted key search and analytical attack at that moment. Another version triple DES is represented as (5)

$$y = DES_{\mathbf{k}_3}(DES^{-1}_{\mathbf{k}_2}(DES_{\mathbf{k}_1}(x))) \tag{5}$$

The advantage here is that this version only performs single DES encryption if $K_1 = K_2 = K_3$.

Triple DES is efficient in hardware rather than in software. It is not very efficient with regard to software implementations. And there is another disadvantage because of short block size of 64 bits, which is not supported for certain applications.

b) AES

The Advanced Encryption Standard (AES) is the most popular and widely used symmetric cipher nowadays. Because of the drawbacks of 3DES and brute-attacks with quantum computers, the US National Institute of Standard and Technology (NIST) decided to find new AES as a replacement for DES in 1997.

A few years later, after three subsequent AES evaluation rounds, in 2001, NIST declared the block cipher Rijndael as the new AES and published it as a final standard. Rijndael was designed by two young Belgian cryptographers.

The AES cipher is exactly like the block cipher Rijndael. The size of block and key can be 128,192 and 256. But AES standard only support 128 bits about a block size which is shown in Figure 3.

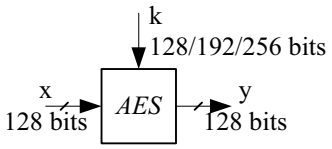

Figure 3. AES input and output structure

Unlike DES, AES was efficient in software implementation. And implementation of AES is suited for 8-bit processors, for example smart card. But it is not efficient on modern 32-bits or 64-bits processors. But the Rijndael designers proposed a workable method that is to merge round functions into one look-up table.

Compared with DES, AES needs more hardware resource than DES. With the development of modern integrated circuits, hardware resource can't be problems. Commercial AES ASIC can exceed throughputs to 10Gbit/sec.

c) SM4

Such as SM4 [1], it was published by China in 2006, at that time, named SMS4. SM4 is used in the Chinese National Standard for Wireless LAN WAPI (Wired Authentication and Privacy Infrastructure).

The block size and key size are 128 bits. They are spliced into four parts, and each part has 32 bits referred to as "words". SM4 consists of 32 identical rounds. Structure about encryption algorithm and decryption algorithm is same. The only operations used are XOR, circular shifts and S-box applications. Both hardware and software are easy to be realized. The keys which are used for decryption are same to encryption but in reversed order.

Assume that the input plain text is (X_0, X_1, X_2, X_3), the output cipher text is (Y_0, Y_1, Y_2, Y_3), and the round key is rk_i, i=0, 1, 2, … 31. Each of X, Y and rk_i is a block which the word length is 32 bits. The encryption transformation is shown in (6) and (7).

$$X_{i+4} = F(X_i, X_{i+1}, X_{i+2}, X_{i+3}, rk_i) \tag{6}$$

$$(Y_0, Y_1, Y_2, Y_3) = (X_{35}, X_{34}, X_{33}, X_{32}) \tag{7}$$

F function is shown in the Figure 4.

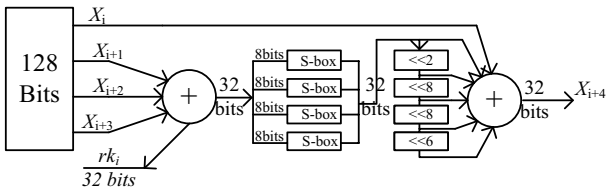

Figure 4. A round structure of SM4

d) Other block ciphers

Up to now, there are more than 100 block cipher algorithms, such as MISTY1, CAST-128, Camellia, SEED, ARIA [2], FOX [3], RC5, RC6, CLEFIA [4], A5/1, KASUMI [5] and SM4 etc. Design theory and application union are different about these block ciphers.

III. DESIGN THEORY AND STRUCTURE OF BLOCK CIPHER

A. Shannon's theory about cryptography

According to the famous information theorist Claude Shannon[6], two primitive operations are needed to build strong encryption algorithm which was identified by Shannon in his paper *Communication theory of secret systems*, published in 1949.

1. Confusion is one encryption operation. Through this way, the relationship between plaintext and ciphertext becomes complex. Substitution which could be found in both DES and AES is common element for achieving confusion.
2. Diffusion is the other encryption operation. Influence of one plaintext symbol is spread over many ciphertext symbols with the goal of hiding statistical properties of the plaintext. And influence of one cipher symbol is spread over many ciphertext symbols to protect encoding the cipher one by one. DES uses the bit permutation, and AES used the Mixcolumn transformation.

B. Design printciple for realization

Block cipher can been realize by hardware or software. The advantage of hardware is to reach the high speed, while the advantage of software is flexible and low cost.

1. Hardware: Encryption and decryption can realize through the same hardware, because of similarity between encryption and decryption. The only difference between them is mode of the key. And regular structure of cipher algorithm is fit for ASIC.
2. Software: Block size, such as 8, 16, 32, is suit for program through computer. Bit substitution should be avoided because of difficulty for software to realize.

C. Overall structure of block cipher

One of the most important properties of modern block ciphers is the overall structure. And it influences the choice of round number, software and hardware implantation performance and so on.

Block cipher can been realize by hardware software. The advantage of hardware is to reach the high speed, while the advantage of software is flexible and low cost.

The structure includes Feistel structure, SP structure, MISTY structure, L-M structure and Generalized Feistel structure.

1. Feistel structure

Horst Feistel introduced the Lucifer cipher about 40 years ago. And it can be considered to be the first modern block cipher. Now a lot of block ciphers employ the Feistel structure, such as Camellia, FEAL, GOST, LOKI, RC6 and so on.

The feature about Feistel structure is

- The plaintext is split into two halves;
- The round function is applied to one half;
- The output of the round function is xored with the other half.

Finally, the two halves are swapped.

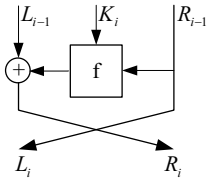

Figure 5. Feistel structure

2. SP-type structure

Another most used structure is the SP-type structure such as AES, Serpent, and ARIA. S means Substitution, and P means Permutation.

The feature about SP-type structure is

The round function is applied to the whole block

The output becomes the input of the next round

Substitution and permutation can alternate and iterate many rounds to strengthen the complexity between key and plaintext.

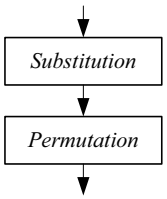

Figure 6. the structure of sp-type

3. SM4 and other Generalized Feistel Structure

Many block ciphers and hash functions are based on generalized Feistel structure. B.Schneier and J.Kelsey [7] published *Unbalanced Feistel Networks and Block Cipher Design* in 1996. There are many algorithms based on unbalanced Feistel structure such as CAST-256, CLEFIA, MARS, SM4 and so on [8].

SM4 is an unbalanced Feistel structure, and has been provable its security. The main feature about Generalized Feistel Structure is that leftmost bits and rightmost bits are not equal compare to Feistel structure.

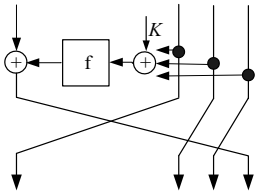

Figure 7. the structure of SM4

SM4 is resistant against many block cipher attacks such as different cryptanalysis, linear, boomerang, integral, impossible differential, higher order differential, interpolation, slide, XSL and related-key different attacks.

4. some others block cipher structure

There are many block cipher structures which are the combination of some typical structures such as Feistel-SP, SP-Feistel, GFN-SP, Feistel-SP, Feistel-MISTY, Lai-Massey [9] and so on.

IV. CRYPTANALYSIS ABOUT BLOCK CIPHER

The word cryptanalysis means to break codes and ciphers to find the key or the plaintext, and cryptanalysis is not only

the science but also sometimes art. Sometime perhaps the intelligence community, organized crime or military like code breaking. However, most cryptanalysis is done by researchers in academia nowadays. Cryptanalysis is most important for cryptosystems because without trying to break crypto methods, security of methods can not been known.

Without cryptanalysis, cryptosystems is not integrated. All crypto algorithms have withstood cryptanalysis using all kinds of method for a long time, in most case for several decades.

In cryptography, there is a Kerckhoff's assumption that a cryptosystem must be security even if everything about the system, except the key is known by public.

Three fundamental cryptanalytic techniques which are a dictionary attack, a codebook attack and an exhaustive key search attack are applied to any block cipher. An attack is commonly regarded as effective if it has lower time complexity as an exhaustive key search.

Recently a lot of cryptanalytic methods have been proposed. All these techniques are effective in data complexity, memory complexity or time complexity aspect compared with above three elementary cryptanalytic techniques.

Differential cryptanalysis [10] was introduced in 1990 and the first more effective method compared to exhaustive key search to be proposed for the full DES. Differential cryptanalysis is often a chosen plaintext attack. It means that encrypted ciphertext can be obtained according to some set of plaintexts. The attack relies primarily on the fact that a special difference in a pair of inputs makes difference in the pair of output of the cipher, where the pair of outputs are obtained through the same key. Several extensions to differential cryptanalysis have been proposed, including higher order derivatives and differential cryptanalysis, Boomerang and rectangle attacks, impossible differential cryptanalysis, and truncated differential cryptanalysis[11] and so on.

Linear cryptanalysis was introduced to attack on the full DES in 1993. Linear cryptanalysis is one of the two most widely used attacks on block cipher, where the other is differential cryptanalysis. It is often a plaintext attack. That means to construct linear equation relating plaintext, ciphertext, and key bits that have a high bias to derive some key bits with known plaintext and ciphertext pairs. Several extension to linear cryptanalysis have been proposed, including non-linear cryptanalysis, partitioning cryptanalysis, differential-linear cryptanalysis and so on.

Related key attack is different from differential cryptanalysis which is a chosen plaintext attack and linear cryptanalysis which is a known plaintext attack. Attacker is unknown the initially keys. But the operation of a cipher under several different keys and some mathematic relationship connecting the key can be observed.

Side channel attack [12] which is based on information gained from implementation of a cryptosystem is different from traditional cryptanalysis which is based on the theoretical weaknesses in the algorithm. Attackers can collect information of execution time, power consumption, and electromagnetic emanation to break the system. According to these information, there are many types of side channel attack, which are Timing attack, Simple and Differential Power analysis attack, Power attack, Electromagnetic attack, Fault attack and Cache attack.

V. CONCLUSION

In this paper, we described some block ciphers including algorithm theory and characteristics, introduced the main structures of block cipher, and presented the common cryptanalysis about block ciphers. With the development of cryptanalysis, some block ciphers which have been seemed security have been found weakness such as DES. Some block ciphers such as SM4 have been introduced to face the challenge and it is worthy for our further researches.

VI. ACKNOWLEDGEMENT

this work is supported by the National Science Foundation of China(no.61072072) and Scientific Research Fund of Heilongjiang Provincial Education Department(no.12521422).

VII. REFERENCE

[1] Office of State Commercial Cryptography Administration, P.R.China, Functionality and Interface Specification of Cryptographic Support Platform for Trusted Computing(in Chinese), http://www.oscca.gov.cn, 2012.

[2]Daesung Kwon, Jaesung Kim, Sangwoo Park et at. New Block Cipher: ARIA, In proc.Information Security and Cryptology-ICISC 2003, LNCS 2971, pp: 432-445, 2003.

[3]P.Junod, S.Vaudenay, FOX: a New Family of Block Cipher, Selected Areas in Cryptograph-SAC 2004, pp: 131-146, 2004.

[4]T. Shirai, K. Shibutani, T. Akishita, S. moriai, T. Iwata, The 128-bits block cipher CLEFIA, Fast Software Encrytion-fse 2007,pp:191-195,2007.

[5]ETSI, Universal Mobile Telecommunications System, Specification of the #GPP confidentiality and integrity algorithms, Document 2: Kasumi specification, 2007.

[6]C.E.Shannon, Communication Theory of Secrecy System, Bell System technology Journal, Vol.28, pp:656-715, 1949.

[7]B.Schneier, J.Kelsey, Unbalanced Feistel Networks and Block Cipher Design, Fast Software Encryption, pp:121-144,1996.

[8]K.Nyberg, Generalized Feistel Networks, Advances in Cryptology-ASIACRYPT'96, LNCS 1163, pp:91-104,1996.

[9]S.Vaudenay, On the Lai-Massey Scheme, Advances in Cryptology-ASIACRYPT'99, pp: 9-19, 2000.

[10]E. Biham, A. Shamir, Differential Cryptanalysis of the Data Encryption Standard, Berlin:springer-verlag, pp:388-397,1993.

[11]L.R.Knudsen, Truncated and Higher Order Differentials, Fast Software Encryption-FSE'94, pp:196-211,1995.

[12]M.S.Emam, S.Bulygin, Improved Algebraic Side-Channel Attack on AES, IEEE International Symposium on Hardware-Oriented Security and Trust, pp: 146-151, 2012.