A New Algorithm for Key and Improved Feistel Rounds in Blowfish Algorithm

Mahesh Patil
School of Information Technology and Engineering
VIT University Vellore, Tamil Nadu

Rahul Kolhe
School of Information Technology and Engineering
VIT University Vellore, Tamil Nadu

ABSTRACT
The main feature of Blowfish algorithm is its variable key size (ranges from 32 to 448 bit). The blowfish algorithm is 16 round feistel network and it uses large s-boxes which are key dependant. Blowfish algorithm use value of π (=3.14159….) to calculate the sub key values, but in cryptanalysis it is claimed that if attacker knows the value of hexadecimal digits of π those we used for generation of sub keys, then it is easy for attacker to break key. In this paper random number generator (RNG) is introduced to create a set of values instead of π value. Seed value is kept private so that no one can guess the value of sub keys and the random number generator (RNG) function is declared public. Also the 16 rounds of blowfish are replaced by 17 complex rounds of IDEA (International data encryption standard) to enhance the security. This paper focuses on enhancing security of Blowfish algorithm for digital content delivery.

Keywords
Feistel network, cryptanalysis, random number generator.

1. INTRODUCTION

1.1 Blowfish
Blowfish was designed in 1993 by Bruce Schnenier. Nowadays blowfish has good encryption rate. It has two parts viz. key expansion and data encryption. When key is expanded, the key is converted into sub key arrays i.e.18-entry P-array and four 256-entry S-boxes. The S box consumes 8 bits and produces 32 bit output. The input is again split into four 8 bits b and used as the input for the S boxes. Decryption and encryption are somewhat similar. While encrypting 64 bit, all zero blocks are encrypted after that data is encrypted by XORing P1 with P2, then P2 XORing with P3 and so on. While decryption same procedure is followed in reverse order i.e. first XORing P17 and P18, then P16 and P17 and so on. As far as the Blow Fish key is concerned, it starts by assigning the P-array and S-boxes along with hexadecimal digits of the π.

1.2 Random number generator (RNG)
Random number generator is a computational machine or formula that generates a sequence of numbers randomly. Random number generator has many applications in computer sampling, computer security (cryptography) and gambling. These numbers are generated from seed value which is fixed for all numbers. The RNG function recursively calculates numbers using seed value. Here one RNG function is introduced to get the values of sub keys such that seed value is hidden and the function is public.

2. LITERATURE REVIEW
Need of data encryption is increased now-a-days due to online services. Everyone wants fast as well as a reliable lifestyle of internet but there are some disadvantages like security of data. That's why there is more demand for security algorithms and new encryption techniques.

From many years there are many algorithms available for encryption and decryption of data. Main classification of these types of algorithms is symmetric algorithm and asymmetric algorithm. Blowfish, AES, DES, and IDEA are the examples of symmetric algorithms while diffe-hellman and RSA are the examples of asymmetric algorithms.

The whole cryptography science is divided in two types:

- Secrete key cryptography (symmetric key cryptography)
- Public key cryptography (asymmetric key cryptography)

In symmetric key cryptography same keys are used to encrypt plaintext and to decrypt of cipher text. This key can be shared between two parties for exchanging information. In public key cryptography two different keys are used i.e. one is private key which is not shared by two parties and another one is public key which is shared by two parties to exchange information. Blowfish is one of the algorithms that falls under symmetric key cryptography. Blowfish algorithm is published in 1993 by Bruce schnenier. Variable key size is the main feature of this algorithm. This algorithm is proposed for enhancing level of security on transfer of data.

3. DETAILED PROBLEM DEFINATION
Main objective of this paper is to increase the security of blowfish algorithm. Sub keys are sequences of original key which is of variable size (32 to 448 bit). In old algorithm these sub keys are initialized by taking some series of hexadecimal digits of value π (=3.14129....). But this paper introduces random number generator (RNG) to calculate the sub key values. For this calculation a random number generator function is introduced with private seed value to generate a number in the range of 32 to 448. As seed value is private it reduces the probabilities of attacks. Feistel rounds of Blowfish algorithm (16 rounds) are also changed and replaced with IDEA (International Data Encryption Algorithm) rounds. IDEA has 17 rounds with 2 different types i.e. even round and odd round. In even round there is use of same mangler function as IDEA for generation of cipher text and plaintext (i.e. X_a ,X_b,X_c,X_d). So the IDEA encryption algorithm is merged with Blowfish algorithm to enhance the security of Blowfish.

4. METHODOLOGY

4.1 Sub Key and S-box Generation

Blowfish algorithm has a variable key size of range 32 to 448 bits (1 word of size 32 i.e. 14 words). That chosen key is used to generate the 52 sub keys i.e. P_1, P_2 .....P_{52} and four 8×32 s-boxes. A K-array is declared to store the keys k1, k2, k3…...k14. P-array is declared to store sub keys P1, P2.....P52 and 4 s-boxes with 256 entries are declared.

S1, 0, S1, 1..... S1, 256.
S2, 0, S2, 1..... S2, 256.
……..
.....
S256, 1.....S256, 256

4.2 Algorithm: Generate P-array and S-boxes

Step 1: Declare a seed value for random generator as private.
Step 2: Use following random number generator function to generate sub keys.
$P_{i+1} = S_{i+1} = X_{i+1} = (X_i + i) \bmod 448$
Where P is sub key and S is s-box values.
Step 3: Perform a bitwise XORing of P array and K-array. Here that k word is used again if needed.
Step 4: Run Encryption algorithm (Explained later.) to generate a cipher text.

Step 5: Continue this process for all P array and S-box values.
Step 6: Stop.

4.3 Algorithm: Encryption

Step 1: Blowfish uses two primitive operations:

- Addition: Addition of words ,denoted by +
- Bitwise Exclusive OR: This is nothing but simple OR operation.

Above two operations are non-commutative in nature which makes cryptanalysis difficult.
Step 2: Divide the plaintext into 4 parts, let's say X_a, X_b, X_c and X_d are the 4 variables as shown in fig 4.2.
Step 3: Use variable key of size Y bits, use same size for single 64 bit block for encryption and decryption but can be changed for next 64 bit plaintext block. This key expansion is explained in detail later.

Step 4: All these parts are taken as input for round 1. Rounds are of two types, even round and odd round.
Even round needs 2 sub keys while odd round needs 4 sub keys.
Step 5: Above process repeats for 17 alternative rounds and after 17 rounds cipher text is generated.
Step 6: stop.

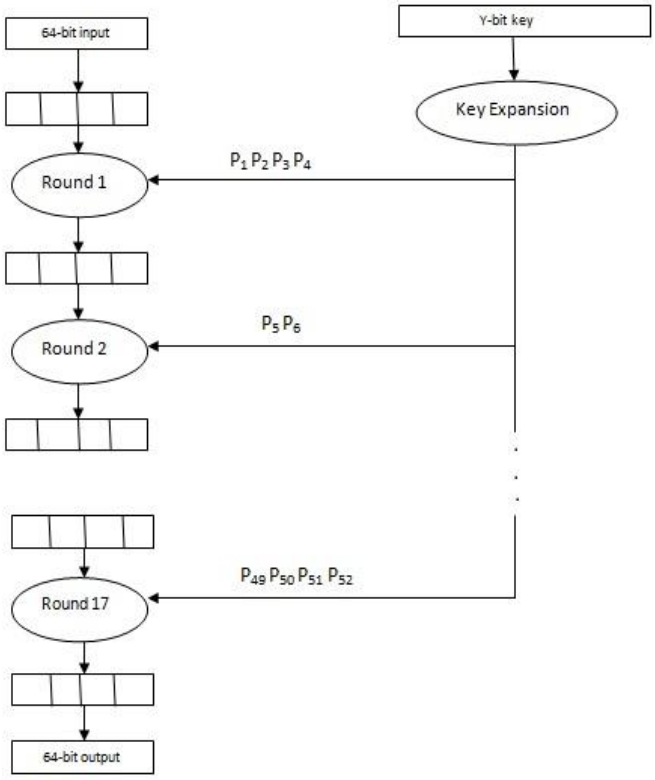

Fig 4.1: Feistel rounds

4.3.1 Odd Round

This round is very simple as compared to even round. How the actual replacement takes place is as follows:

$X_a = X_a \otimes P_a$;
$X_b = X_b \otimes P_b$;
$X_c = X_c \otimes P_c$;
$X_d = X_d \otimes P_d$;

This round operation is properly explained in figure given below.

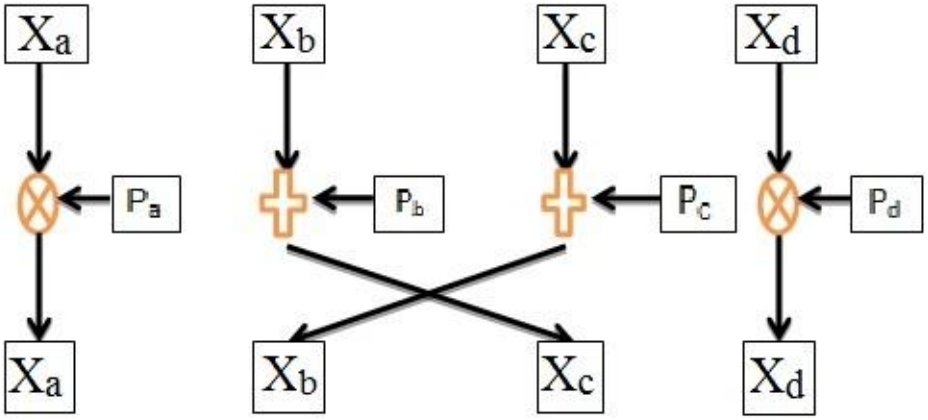

Fig 4.2: Odd round

4.3.2 Even Round:

This is more complex than odd round. It uses
Mangler Function as shown in figure given below.

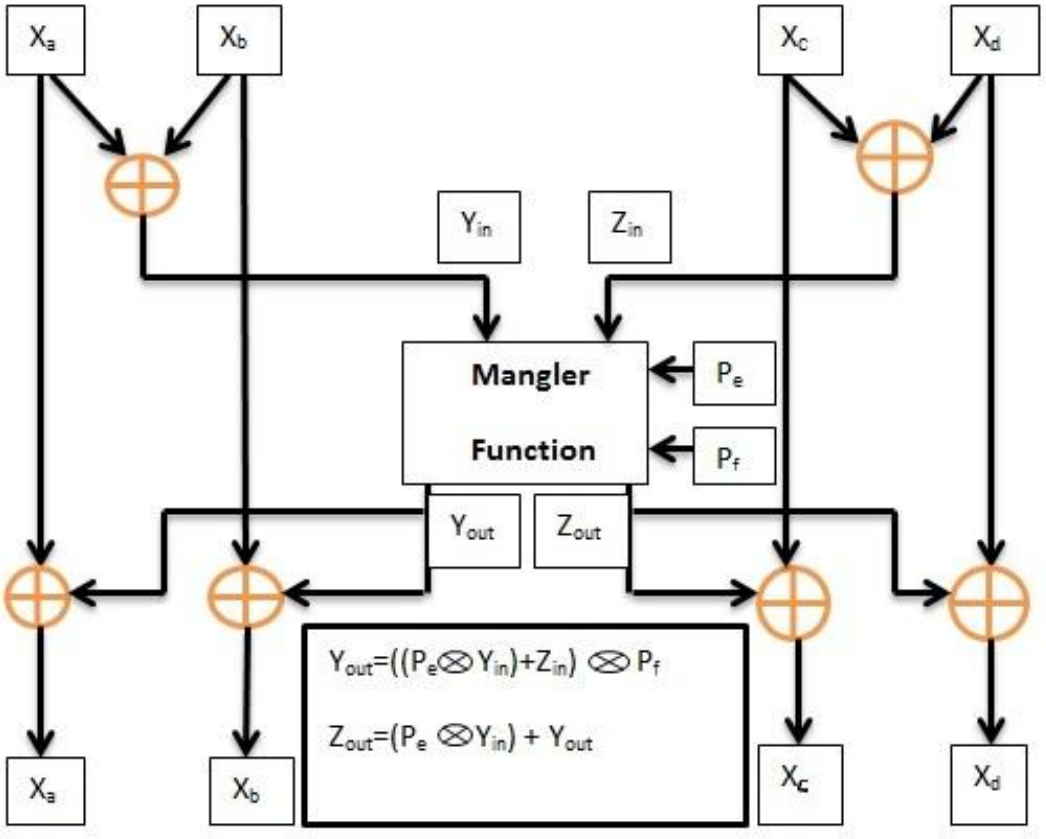

Fig 4.3: Even Round

4.4 Decryption process

As the IDEA round is used for encryption which uses same keys (inverse in case of decryption). There is need to compute inverse keys such that encryption process will work as decryption process without any modification. For encryption

52 different keys are used from P1 to P52. Here four of them are used for odd round and 2 for even round. Similarly while inversing; same order should be followed so that no conflicts occur. Care should be taken while odd round, in even round no special attention is required.

5. RESULTS AND ANALYSIS

The attacker can break the key of Blowfish algorithm by easily guessing the hexadecimal digits of value π. In Proposed Blowfish algorithm Random Number Generator is introduced to generate the sub key values.

Random Number Generator:

$P_{i+1} = S_{i+1} = X_{i+1} = (X_i + i) \bmod 448$

Here 432 is the maximum number generated by function. If a value less than 448 is chosen then collision of two values may occur and if a value greater than 448 is selected then some non possible values it may take. Value of 'i' increases as iterations goes on. P is key value; S is s-box values. X's initial value is the seed value which is kept private. Here the value of seed should be greater than 32.

Let consider i=1 and X=34

$P_{i+1} = (34+1) \bmod 448 = 35$

Now X=35 and i=2;

$P_{i+1} = (35+2) \bmod 448$

$P_{i+1} = 37$ and so on...

Thus no one predict the next value of sub key by being unknown to the seed value.

6. CONCLUSION

The proposed mechanism of Blowfish algorithm is not only enhancing the security by introducing the random number generator and IDEA complex feistel rounds but also provides open path to researchers. Rounds in encryption algorithm are used to make it too hard for cryptanalysis. Also for decryption there is provision of a simple inverse function. Here an easy but hard to break RNG method is implemented in proposed blowfish algorithm.

7. FUTURE WORK

In multipath routing an attempt is made to find an optimal (not necessarily shortest. i.e. if shortest path lose some data over link then avoid that link) path from source to sink. To deliver data from one node to another node proposed encryption algorithm can be used to enhance the security over a link. This secured multipath routing can be applied for digital library in cloud computing.

8. REFERENCES

[1] S.Bruce, "Description of a new variable-length key, 64-bit block cipher (Blowfish),"In Fast Software Encryption Second International Workshop, Leuven, Belgium,

December 1993, Proceedings, Springer-Verlag, ISBN: 3-540-58108-1, pp.191-204, 1994.

[2] M.Allam,"Data encryption performance based on Blowfish," 47th International Symposium ELMAR, Zadar, Croatia, 2005,pp. 131-134.

[3] K.Russell Meyers, and H.Ahmed Desoky, "An implementation of the Blowfish cryptosystem," Proceedings of the IEEE International Symposium on Signal Processing and Information Technology, Sarajevo, Bosnia and Herzegovina, pp. 346-351, December 16-19, 2008.

[4] William Stallings, "Cryptography and Network Security", Third Edition, Pearson Education, 2003.

[5] G.N. Krishnamurthy, Ramaswamy, V, M.E. Ashalatha, "Performance Enhancement of Blowfish and CAST-128 Algorithms and Security of Improved Blowfish Algorithms Using Avelanche Effect",International Journal of Computer Science and Network Security,Vol.8 No.3, 2008.

[6] Bruce Schneier. The Blowfish Encryption Algorithm Retrieved October 25, 2008, http://www.schneier.com/blowfish.html

[7] S. Vaudenay, "On the Weak Keys in Blowfish," Fast Software Encryption, Third International Workshop Proceedings, Springer-Verlag, 1996, pp. 27-32.