A Study of Twofish Algorithm

Aparna. K, Jyothy Solomon, Harini . M, Indhumathi . V
B.E (final year)
Department of Computer Science and Engineering
United Institute of Technology, Coimbatore, India

Abstract - **Twofish is a well known encryption algorithm commonly used in cryptography and steganography. Twofish algorithm is derived from Blowfish algorithm. Twofish is a 128-bit block cipher that accepts a variable length key up to 256 bits. The cipher is a 16-round Feistel network with a bijective function made up of four key dependent 8-by-8 bit S-boxes, a fixed 4-by-4 maximum distance seperable matrix, a pseudo Hadamard transform, bitwise rotations, and a carefully designed key schedule. A fully optimized implementation encrypts on a Intel core i5 at 17.8 clock cycles per byte, and an8-bit smart card implementation encrypts at 1660 clock cycle per byte. The design of both the round function and the key schedule permits a wide variety of tradeoffs between speed, software size, key setup time, gate count and memory.**

Keywords - **Twofish, Cryptography, Steganography, block cipher, AES, Feistel network**

I. INTRODUCTION

Twofish is a 128 bit blocker cipher that accepts variable key up to 256 bits. Generally Twofish algorithm is used for encryption process, that means hiding information within one information. Following are some parameters which need to be taken care always for a safe and secure data encryption process i.e.

Imperceptibility: Imperceptibility is the property in which a person should be unable to distinguish the original and the embedded data.

Robustness: refers to the degree of difficulty required to destroy embedded information without destroying the cover data.

Embedding Capacity: Refers to the amount of secret information that can be embedded without degradation to the quality of the data.

II. TWOFISH DESIGN GOALS

A 128-bit symmetric block cipher. Key length of 128 bits, 192 bits, and 256 bits. No weak keys. Efficiency both on the Intel Pentium pro and other software and hardware platforms. Accept additional key length be implementable on a wide variety of platforms and applications and be suitable for a stream cipher, hash function and MAC. Simple design both to facilities ease of analysis and ease of implementation.

III. TWOFISH BUILDING BLOCKS

3.1 Feistel Network

Feistel Network is a general method of transforming any function (usually called F function) into a permutation. It was invented by Horst Feistel in the designer of Lucifer, and popularized by DES (Data Encryption Standard), The fundamental building block of a feistel network is the F function: a key dependent mapping of an input string on to an output string. An F function is always non linear and possibly non subjective,

F: {0,1}^n/2 x {0,1}^N→ {0,1}^n

Where n is the block size of the feistel network, and F is a function taking n/2 bits of the block and N length n/2 bits. In each round the "Source block" is the input to F, and the output of F is XOR ed with the "target block", after which these two blocks swap places for the next round.

3.2 S-BOXES:

An s-box is a table driven non linear substitution operation used in most block ciphers. S-boxes vary in both input size and output size, can be created either randomly or algorithmically. S-boxes were first used in Lucifer, then DES, and afterwards in most encryption algorithm. These s-boxes are built using two fixed 8-by-8 bit permutations and key material.

3.3 MDS MATRICES

Maximum Distance Separable (MDS) is a code over a field is a linear mapping from a field elements to be field elements, producing a composite vector of a + b elements, with the property that the minimum number of non zero elements in any non zero vector is less b + 1. The distance between two distinct vectors produced by MDS mapping is at least b + 1. It can easily be shown that no mapping can have larger minimum distance between two distinct vectors, hence the term maximum distance seperable. MDS mapping can be represented by an MDS matrix consist of a x b elements.

2.4 WHITENING

Whitening, the technique of XOR – ing key material before the first round and after the last round, was used by merkle, and independently invented it was shown that whitening substantially increases the difficulty of key search attacks against the remainder of the cipher. In our attack on reduced round twofish variants.

2.5 KEY SCHEDULE

The key schedule is the means by which the key bits are turned into round keys that the cipher can use. Twofish needs a lot of key material, and has a complicated key schedule. To facilitate analysis, the key schedule uses the same primitive as the round function.

2.6 PSEUDO – HADAMARD TRANSFORMS

A pseudo – hadamard transform (PHT) is a simple mixing operation that runs quickly in software give two inputs, a and b. this PHT can be execute in two opcodes on most modern microprocessors, including the Pentium family

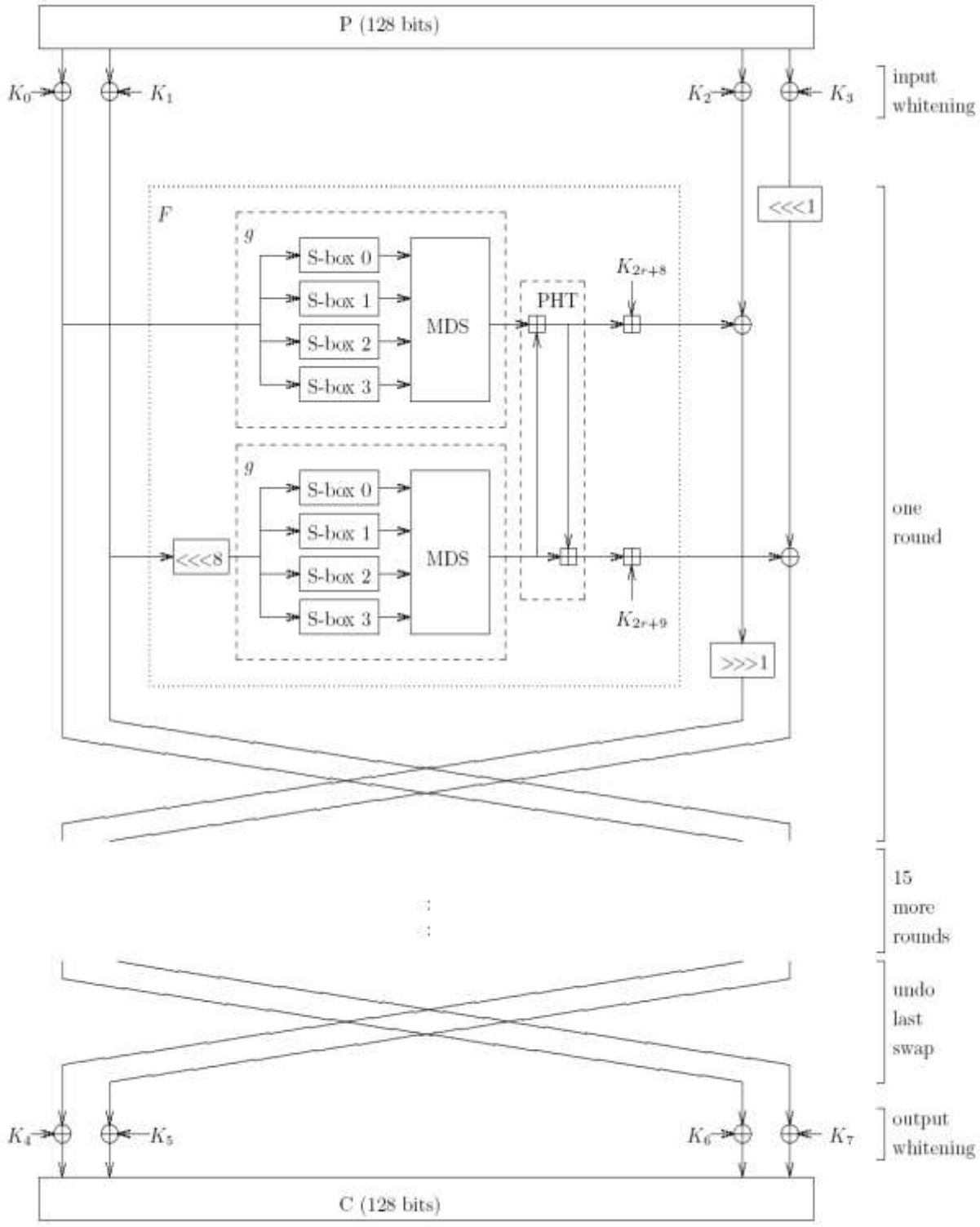

Figure 1: Twofish

Block Diagram of Twofish

Given two inputs, a and b, the 32- bit PHT is defined as:

$$a' = a + b \bmod 2^{32}$$
$$b' = a + 2b \bmod 2^{32}$$

IV. OVERVIEW OF THE TWOFISH ALGORITHM

The two words on the left are used as input to the g functions after the rotation by 8 bits of one of them. The g function consist of four byte wide key dependent s-boxes, followed by a linear mixing step based on the MDS matrix. The result of the two g functions are combined using pseudo hadamard transform (PHT), and two keywords are added. One of the words on the right is rotated by bit and then both of them are XOR ed in to the result on the left. The left and right halves are then swapped for the next round. After 16 rounds, the swap of the last round is reserved, and the four words are XOR ed with four more key words to procedure the cipher text.

V. CONCLUSION

Twofish, the rationale behind its design, and the results of our initial cryptanalysis. The encryption algorithm and key schedule must be designed in tandem. There is no such thing as a key dependent s-box only a complicated multi stage nonlinear function that is implemented as a key dependent s-box for efficiency. Key should be a short as possible. It is much harder to design an algorithm with a long key than an algorithm with a secret key.

VI. FUTURE WORK

Twofish algorithm generally used for embedding process. Mainly used for text encryption. There are some for audio, image , but this is still an area, which lags behind image steganography. Future work can be done to minimize the key and security transmits it to the receiver. In future Twofish can be used for other digital media files like image, audio, and video.

VII. REFERENCES

[1] R.anderson and E. Bihan, “Two practical and provably secure block cipher BEAR and LION”, fast software encryption, third international workshop proceedings, springer – verlag, 1996, pp. 113-120

[2] U. Blumenthal and S. Bellovin, “A Better Key Schedule for DES like ciphers” pragocrypt “96 proceedings, 1996, pp.42-54.