ABC - A Block Cipher

Dieter Schmidt
Denkmalstrasse 16
D-57567 Daaden
Germany

May 27, 2002

Abstract

The author proposes a block cipher which is easy to implement in software on modern 32 bit microprocessors. It has a block size of 256 bit and key length of 512 bit. The building blocks of the cipher are from the block ciphers MMB and SAFER. The cipher may be expanded for use with future 64 bit processors. Also a new diffusion layer, developed from the SAFER diffusion layer, is proposed. It has complexity $\mathcal{O}(n\ log\ n)$ and the author conjectures that it is MDS. Diffusion layers currently known to be MDS are based on matrices and thus have complexity $\mathcal{O}(n^2)$.

1 Introduction

State of the art in block cipher design is a block size of 128 bit. Expanding that size will give additional security, especially against codebook attacks. Today, a typical microprocessor in a PC has a register length of 32 bit. Future processors like Intel's Itanium or AMD's Opteron will have a register size of 64 bit. It seems therefore prudent, to build cipher systems from building blocks using that size. The backdraw of that approach is that such a cipher is not as universal as let's say AES, because it will be hard to implement it on computers with limited resources like smart cards. Nevertheless, this article is an attempt to build a block cipher primarily for PC's which utilizes typical instructions like multiplication, addition, XOR, rotation and shifts, which can be easily programmed in assembler or a language like C and also give a high performance. Those familiar with block cipher design will find little new in this article. The cipher design is done by "recycling" old ideas, like the use of incompatible arithmetic operations (IDEA) [5], a diffusion layer where the complexity is of $\mathcal{O}(n\ log\ n)$ (SAFER, [6]) and the use of multiplication modulo $2^{32}-1$ [2, 3]. The cipher itself resembles a Substitution-Permutation-Network (SPN). The author assumes that the expanded SAFER diffusion layer is MDS (Maximum Distance Separable) which, if proven, would be the only new thing in this paper.

2 Notation

A word of 32 bit is the natural unit of calculus in this paper. If not stated otherwise, all calculations refer to a 32 bit word.$\lll l$ denotes o rotation of a word by l positions to the left, $+$ denotes addition modulo 2^{32}, $\bigoplus$ denotes XOR and $\bigotimes$ denotes multiplication modulo $2^{32}-1$.

3 Description of the cipher

Consider a bit string of size 256 which is divided into substrings of length 32. These substrings constitue on array $A_0, \dots, A_7$. The division is done in little endian manner, i.e. the memory mapping is Intel style.

The cipher consists of eight primary rounds, a middle transformation and eight secondary rounds. A primary round consists of an XORing the data with the first round key, multiplication modulo $2^{32}-1$ with constants given in [3] and XORing the data again with the second round key. This followed by a diffusion layer essentially made up of an extended and modified SAFER layer [6]. Then the next primary round is used until eight rounds have been taken.

The S-boxes are made up of multiplication modulo $2^{32}-1$ by given constants. These constants are taken from [3] and are used the following way: $\gamma_0 = 0x025F1CDB$ is the constant for the leftmost S-boxes which are entered by A_0, A_1 after XORing, $\gamma_1 = 2 \bigotimes \gamma_0$ is the constant for next two S-boxes which are entered by A_2, A_3 after XORing, $\gamma_2 = 2^3 \bigotimes \gamma_0$ is used for S-boxes entered by A_4, A_5 and $\gamma_3 = 2^7 \bigotimes \gamma_0$ is used for the rightmost S-boxes entered by A_6, A_7

after XORing. If the data entering the S-box is equal to $2^{32} - 1$ no multiplication will take place. They choice of the constants is according to [3], the ordering was chosen to avoid rotational symmetry. Note that the S-boxes have a complementation property, i.e. if one complements the input, the output is complemented too [4].

The middle tarnsformation consists of XORing the data with the first middle round key, multiplication modulo $2^{32} - 1$ with given constants and XORing the data with the second middle round key.

The secondary rounds are comprised of an inverse diffusion layer, XORing the data with the first round key, multiplication modulo $2^{32} - 1$ with given constants and XORing the data with the second round key. This is repeated eight times.

In the diffusion layer and the Pseudo-Hadamard-Transform (PHT) from [6] and its inverse (IT) are used, but extended to 32 bit words instead of bytes. The PHT can be described as follows, if one uses a_1, a_2 for inputs and b_1, b_2 for the outputs:

$$b_1 = 2 \cdot a_1 + a_2 \quad b_2 = a_1 + a_2 \tag{1}$$

The IT can formulated the following way:

$$a_1 = b_1 - b_2 \quad a_2 = -b_1 + 2 \cdot b_2 \tag{2}$$

Every right output of the PHT in the diffusion layer (the b_2) is rotated by a specified amount to the left before being fed into the next PHT. This is done to ensure better diffusion. The amount of the rotation can be seen in the figures. Note that complexity of the diffusion layer is $\mathcal{O}(n\ log\ n)$ when n denotes the number of blocks. For large block numbers this is clearly better the the $\mathcal{O}(n^2)$ complexity which is achieved by matrix multiplication.

For decryption the cipher is used the same way, except that constants for multiplication have to be replaced by their inverse modulo $2^{32} - 1$, which can be done using the extended Euclidian algorithm. Also the round keys have to be swapped for decryption. This will be explained in the next section. Thus the cipher is selfinverse, if the change in the constants and the round keys is taken into account.

4 Key Schedule

The user supplies a key of size 512 bits. This key is taken to form the round key of the first primary round, i.e. the first 256 bits of the key are used for XORing before the multiplication and the second 256 bits afterwards. Then the user supplied key ist shifted by 101 positions to the left and used in the same manner as before to form the round key of the second primary round. This is repeated until all primary rounds, the middle transformation and the secondary rounds have received their respective round keys.

For decryption the key expansion is done same way but after that the last round key of the last secondary round is swapped with the first round key of the first primary round. The first round key of the last secondary round is swapped with the last round key of the first primary round and so on. This is repeated until the first and the last round keys of the middle transformation have been swapped.

5 Security Considerations

The source [2] gives the probability for the critical characteristics $p_c = 2^{-9}$. If one assumes that the diffussion layer is MDS, i.e. it has the maximal branch number of $\mathcal{B} = 9$, then then maximum differential characteristic probalitity (MDCP) is upper bounded [8] by

$$MDCP \leq p_c^{\mathcal{B}T/2} \tag{3}$$

where T denotes an even number of rounds. If $T = 16$, $\mathcal{B} = 9$ and $p_k = 2^{-9}$ are given, then the maximum differential characteristic probability is $MDCP \leq 2^{-648}$, which means that the proposed cipher should be immune from ordinary differential cryptanalysis.

It should also be immune from the slide attack [1] due to its design and the boomerang attack [9] due to its low MDCP.

Crucial to the above estimate is the branch number $\mathcal{B}$. If the diffusion layer has really the maximal branch number of nine, the estimate holds. The author has found no indication to the contrary, but this remains an open problem.

6 Intellectual Property

James Massey stated in [7]: “SAFER K-64 has not been patented and, to the best of our knowledge, is free for use by anyone...”. The inventors of MMB claim no intellectual property, neither does the author of ABC. Thus the algorithm can be used freely by anyone around the world, although it seems prudent to wait with implementation until some cryptanalysis has been done.

7 Conclusion

The author proposes a block cipher with 256 bit block size and 512 bit key length. If the assumption holds that the diffusion layer has maximal branch number, then the cipher is immune from ordinary differential cryptanalysis. Resistance to linear cryptanalysis was not investigated, but is strongly encouraged.

A reference implementation in C of ABC is available from the author on request. It works with the gcc compiler under Linux and the Cygwin B20.1 compiler under Windows 9x. With minor modifications it should work with other compilers as well.

8 Acknowlegdements

The author is grateful to his parents Robert and Johanna Schmidt for making his crypto studies possible through financial and moral support. He also thanks his wife Maria for continued support.

References

[1] Biryukov, Alex and David Wagner: Slide Attacks, in Knudsen, Lars R. (Ed.): *Fast Software Encryption - Proceedings of 6th International Workshop*, Springer Verlag, 1999, Berlin

[2] Daemen, Joan; Van Linden, Luc; Govaerts, René and Joos Vandewalle: *Propagation Properties of Multiplication Modulo* $2^n - 1$, available from `http://www.esat.kuleuven.ac.be/~cosicart/pub92.html`

[3] Daemen, Joan; Govaerts, René and Joos Vandewalle: *Block Ciphers Based on Modular Arithmetic*, available from `http://www.esat.kuleuven.ac.be/~cosicart/pub93.html`

[4] Daemen, Joan: *personal communication*

[5] Lai, Xuejia: *On the Design and Security of Block Ciphers*, ETH Series in Information Processing, Volume 1, Hartung-Gorre Verlag, Konstanz, Germany, 1992

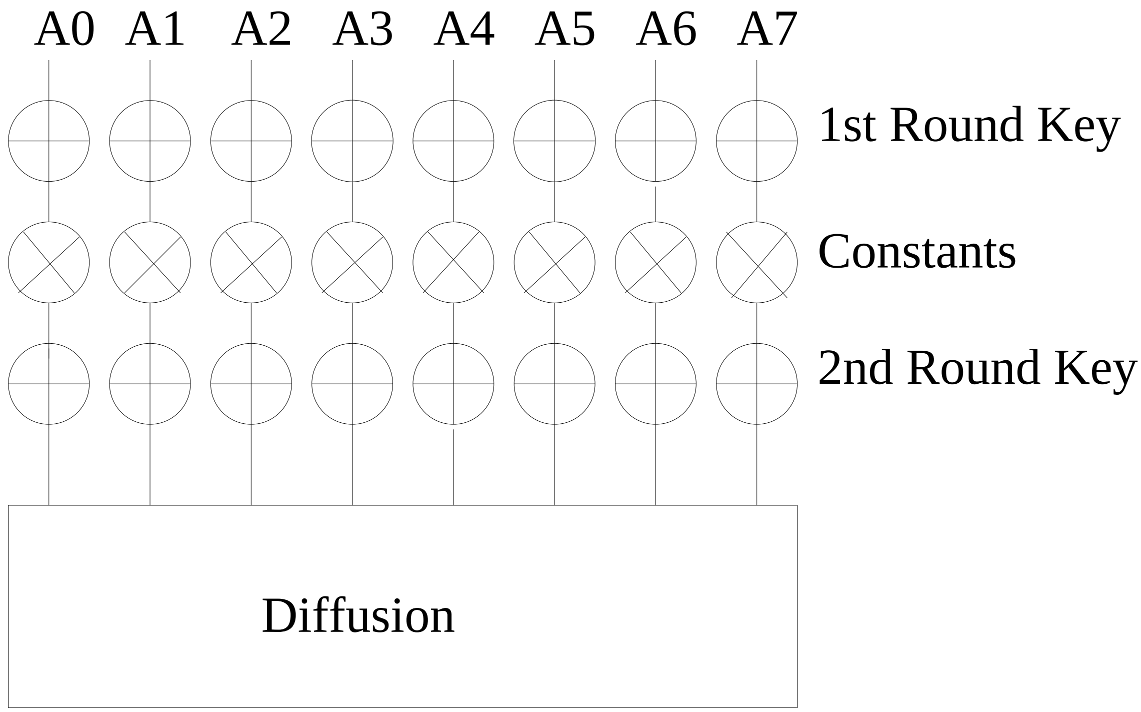

Figure 1: Diagram of one primary round

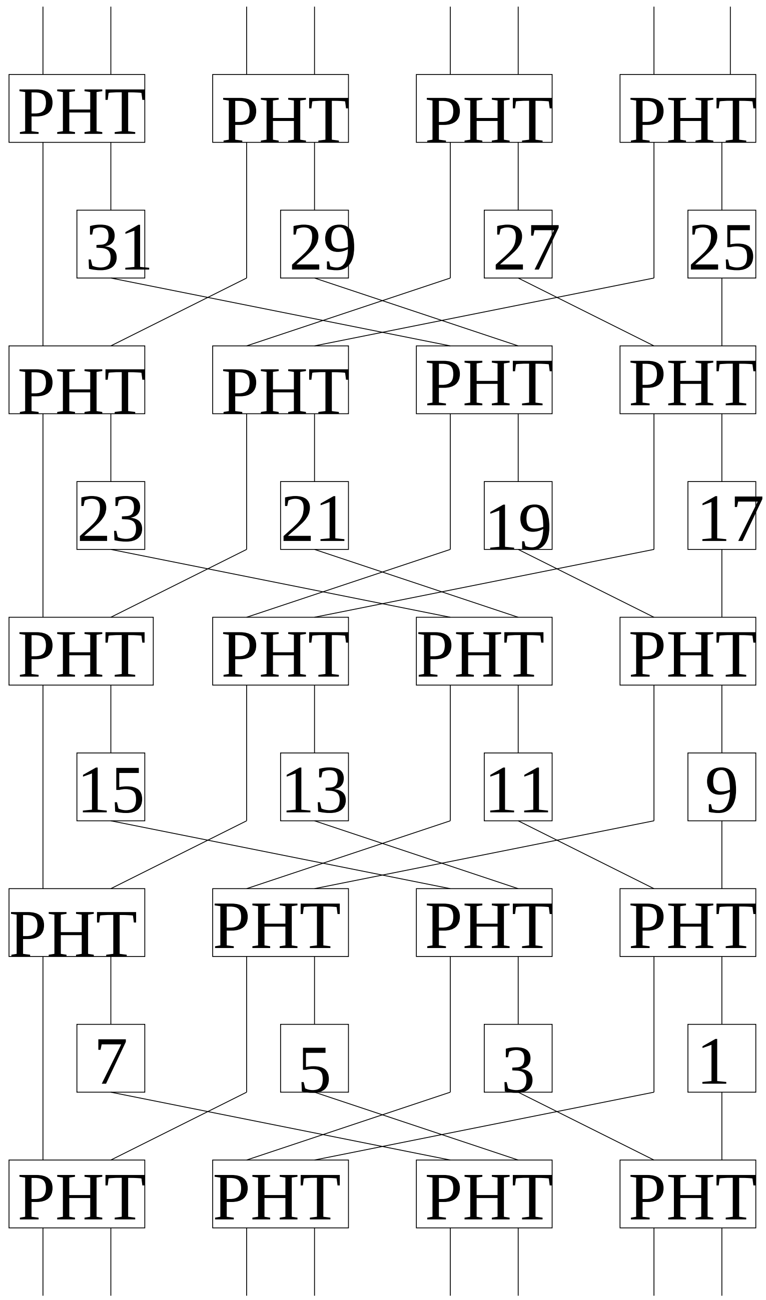

Figure 2: Diagram of the diffusion layer. The numbers in the small boxes indicate by how much a word is rotated to the left

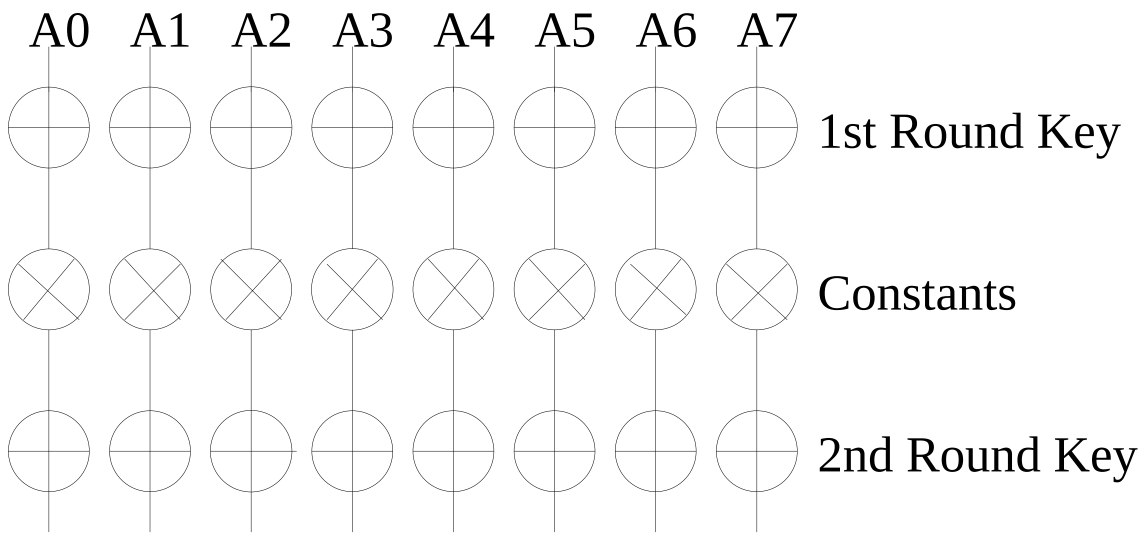

Figure 3: Diagram of the middle transformation

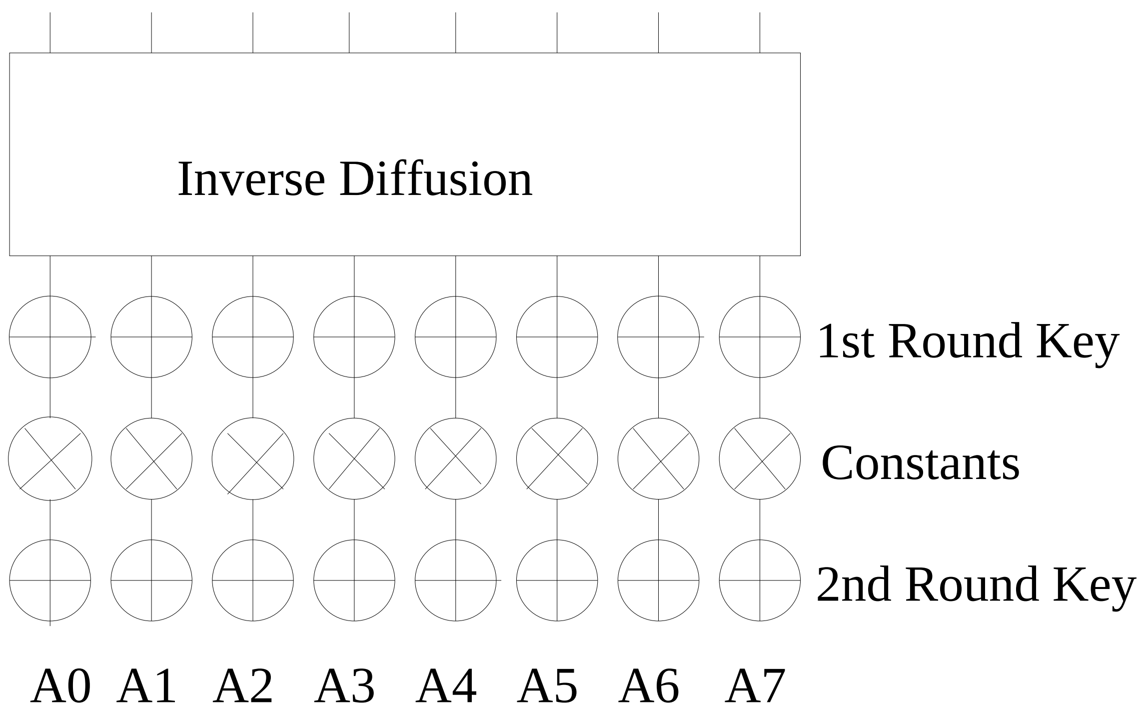

Figure 4: Diagram of one secondary round

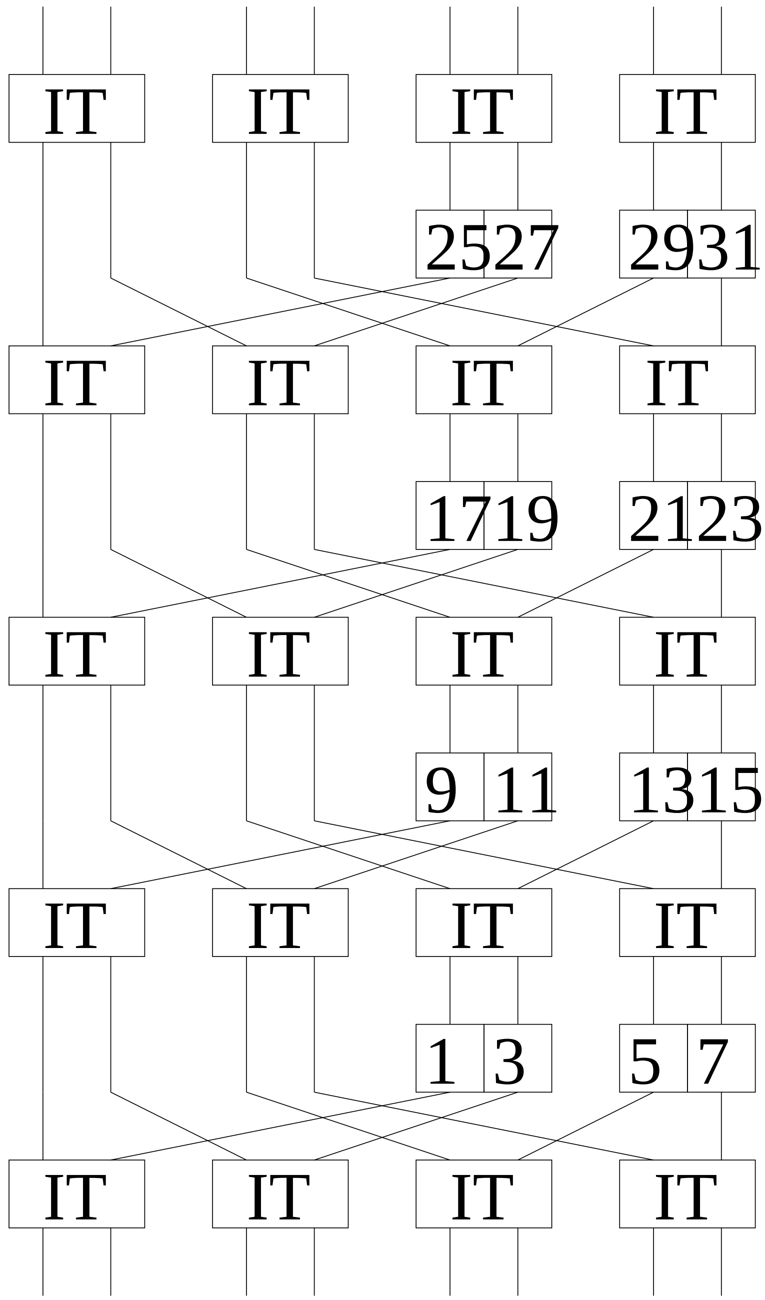

Figure 5: Diagram of the inverse diffusion layer. The numbers in the small boxes indicates by how much a word is rotated to the left

[6] Massey, James L.: SAFER K-64: A Byte Oriented Block-Ciphering Algorithm, in Anderson, Ross (Ed.): *Fast Software Encryption, Cambrigde Security Workshop Proceedings*, Springer Verlag, Berlin, 1994

[7] Massey, James L.: SAFER K-64: One year later, in Preneel, Bart (Ed.): *Fast Software Encryption - Proceedings of Second International Workshop*, Springer Verlag, Berlin, 1995

[8] Ohkuma, Kenji; Shimizu, Hideo; Sano, Fumihiko and Shinichi Kawamura: *Security assessment of Hierocrypt and Rijndael against Differential and Linear Cryptanalysis*, available from `http://eprint.iacr.org/2001/070.ps`

[9] Wagner, David: The Boomerang Attack, in Knudsen, Lars R. (Ed.): *Fast Software Encryption - Proceedings of 6th International Workshop*, Springer Verlag, Berlin, 1999