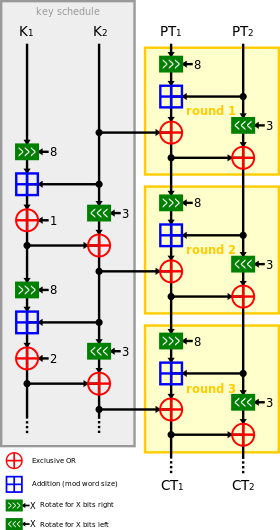
# speck

Beaulieu, Ray, et al. "The SIMON and SPECK Families of Lightweight Block Ciphers." *IACR Cryptology ePrint Archive* 2013 (2013): 404.

维基百科：<https://en.wikipedia.org/wiki/Speck_(cipher)>

NSA新发布的轻量级分组密码，被用在嵌入式，物联网等安全中

|  |  |
| --- | --- |
| Designers | Ray Beaulieu, Douglas Shors, Jason Smith, Stefan Treatman-Clark, Bryan Weeks, Louis Wingers[NSA](https://en.wikipedia.org/wiki/National_Security_Agency) |
| First published | 2013 |
| Related to | [Simon](https://en.wikipedia.org/wiki/Simon_(cipher)), [Threefish](https://en.wikipedia.org/wiki/Threefish" \o "Threefish) |
| Cipher detail | |
| [Key sizes](https://en.wikipedia.org/wiki/Key_size) | 64, 72, 96, 128, 144, 192 or 256 bits |
| [Block sizes](https://en.wikipedia.org/wiki/Block_size_(cryptography)) | 32, 48, 64, 96 or 128 bits |
| Structure | ARX |
| Rounds | 22–34 (depending on block and key size) |
| Speed | 2.6 [cpb](https://en.wikipedia.org/wiki/Cycles_per_byte" \o "Cycles per byte) (5.7 without [SSE](https://en.wikipedia.org/wiki/Streaming_SIMD_Extensions)) on Intel Xeon 5640 (Speck128/128) |



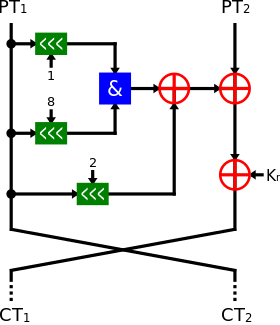
# Simon

Beaulieu, Ray, et al. "The SIMON and SPECK Families of Lightweight Block Ciphers." *IACR Cryptology ePrint Archive* 2013 (2013): 404.

维基百科：<https://en.wikipedia.org/wiki/Simon_(cipher)>

与speck一起提出

|  |  |
| --- | --- |
| General | |
| Designers | Ray Beaulieu, Douglas Shors, Jason Smith, Stefan Treatman-Clark, Bryan Weeks, Louis Wingers[NSA](https://en.wikipedia.org/wiki/National_Security_Agency) |
| First published | 2013 |
| Related to | [Speck](https://en.wikipedia.org/wiki/Speck_(cipher)) |
| Cipher detail | |
| [Key sizes](https://en.wikipedia.org/wiki/Key_size) | 64, 72, 96, 128, 144, 192 or 256 bits |
| [Block sizes](https://en.wikipedia.org/wiki/Block_size_(cryptography)) | 32, 48, 64, 96 or 128 bits |
| Structure | Balanced [Feistel network](https://en.wikipedia.org/wiki/Feistel_network" \o "Feistel network) |
| Rounds | 32, 36, 42, 44, 52, 54, 68, 69 or 72 (depending on block and key size) |



# Lucifer

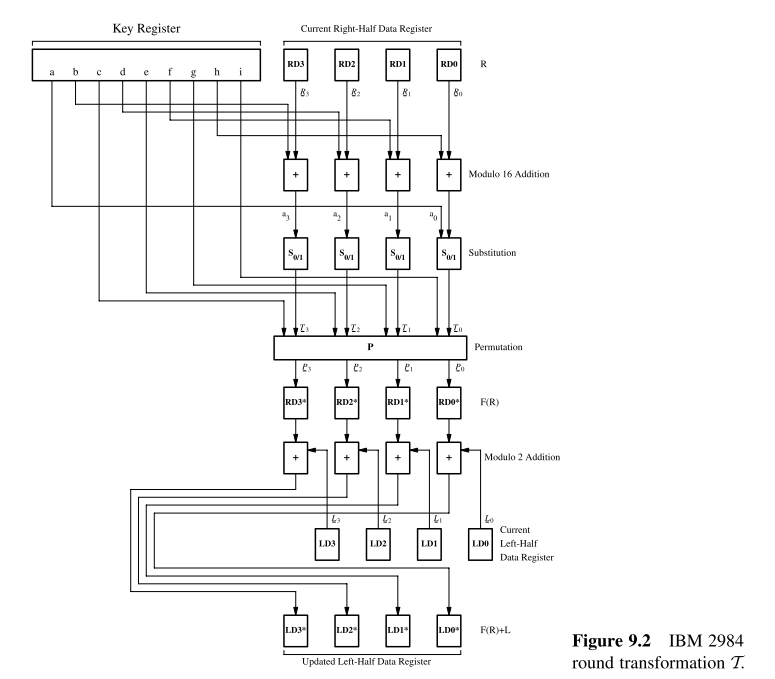
Sorkin, Arthur. "Lucifer, a cryptographic algorithm." Cryptologia 8.1 (1984): 22-42.

维基：<https://en.wikipedia.org/wiki/Lucifer_(cipher)>

 a candidate for the [Data Encryption Standard](https://en.wikipedia.org/wiki/Data_Encryption_Standard)

|  |  |
| --- | --- |
| Designers | [Horst Feistel](https://en.wikipedia.org/wiki/Horst_Feistel) et al. |
| First published | 1971 |
| Successors | [DES](https://en.wikipedia.org/wiki/Data_Encryption_Standard) |
| Cipher detail | |
| [Key sizes](https://en.wikipedia.org/wiki/Key_size) | 48, 64 or 128 bits |
| [Block sizes](https://en.wikipedia.org/wiki/Block_size_(cryptography)) | 48, 32 or 128 bits |
| Structure | [Substitution-permutation network](https://en.wikipedia.org/wiki/Substitution-permutation_network), [Feistel network](https://en.wikipedia.org/wiki/Feistel_network" \o "Feistel network) |
| Rounds | 16 |





# CLEFIA

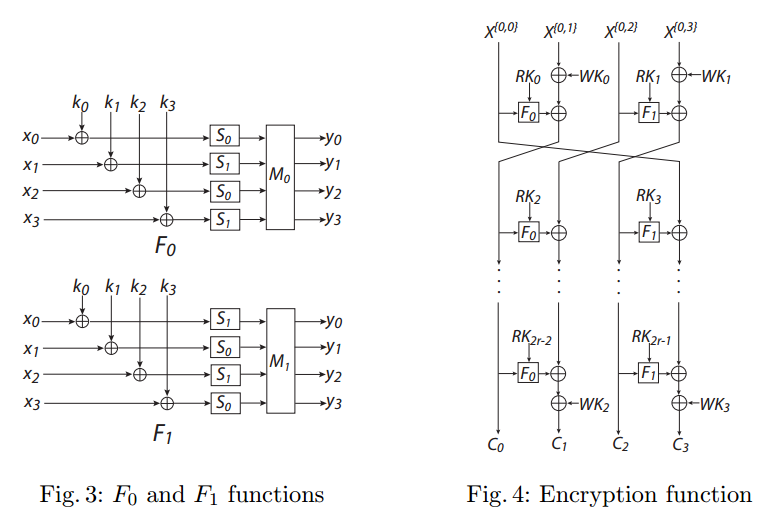
Tezcan, Cihangir. "The improbable differential attack: Cryptanalysis of reduced round CLEFIA." *Progress in Cryptology-INDOCRYPT 2010*. Springer Berlin Heidelberg, 2010. 197-209.

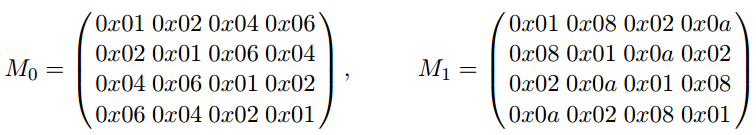
Shirai, Taizo, et al. "The 128-bit blockcipher CLEFIA." *Fast software encryption*. Springer Berlin Heidelberg, 2007.

维基：<https://en.wikipedia.org/wiki/CLEFIA>

索尼提出，网站：http://www.sony.net/Products/cryptography/clefia/?j-short=clefia

|  |  |
| --- | --- |
| Designers | Sony |
| First published | 2007 |
| Certification | [CRYPTREC](https://en.wikipedia.org/wiki/CRYPTREC) (Candidate) |
| Cipher detail | |
| [Key sizes](https://en.wikipedia.org/wiki/Key_size) | 128, 192, or 256 bits |
| [Block sizes](https://en.wikipedia.org/wiki/Block_size_(cryptography)) | 128 bits |
| Structure | [Feistel network](https://en.wikipedia.org/wiki/Feistel_network) |
| Rounds | 18, 22, or 26 |





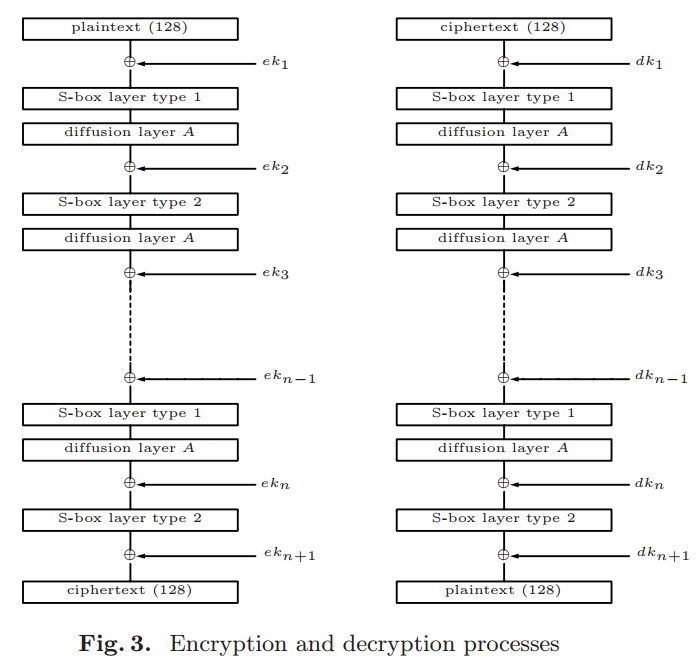
# ARIA

Kwon, Daesung, et al. "New block cipher: ARIA." *Information Security and Cryptology-ICISC 2003*. Springer Berlin Heidelberg, 2004. 432-445.

韩国提出

维基：https://en.wikipedia.org/wiki/ARIA\_(cipher)

|  |  |
| --- | --- |
| First published | 2003 |
| Derived from | [AES](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard) |
| Certification | [South Korean](https://en.wikipedia.org/wiki/South_Korea) standard |
| Cipher detail | |
| [Key sizes](https://en.wikipedia.org/wiki/Key_size) | 128, 192, or 256 bits |
| [Block sizes](https://en.wikipedia.org/wiki/Block_size_(cryptography)) | 128 bits |
| Structure | [Substitution-permutation network](https://en.wikipedia.org/wiki/Substitution-permutation_network) |
| Rounds | 12, 14, or 16 |

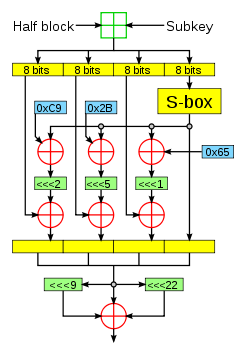
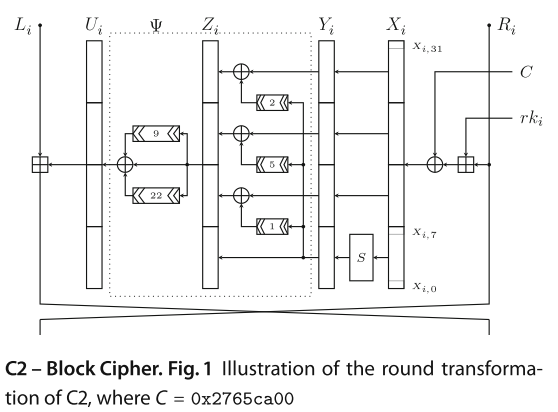


# Cryptomeria/C2

Knudsen, Lars R., and Gregor Leander. "C2–Block Cipher." *Encyclopedia of Cryptography and Security*. Springer US, 2011. 179-180.

维基:https://en.wikipedia.org/wiki/Cryptomeria\_cipher

|  |  |
| --- | --- |
| Designers | [4C Entity](https://en.wikipedia.org/wiki/4C_Entity) |
| First published | 2003 |
| Derived from | [DES](https://en.wikipedia.org/wiki/Data_Encryption_Standard) |
| Related to | [CSS](https://en.wikipedia.org/wiki/Content_Scramble_System) |
| Cipher detail | |
| [Key sizes](https://en.wikipedia.org/wiki/Key_size) | 56 bits |
| [Block sizes](https://en.wikipedia.org/wiki/Block_size_(cryptography)) | 64 bits |
| Structure | [Feistel network](https://en.wikipedia.org/wiki/Feistel_network) |
| Rounds | 10 |

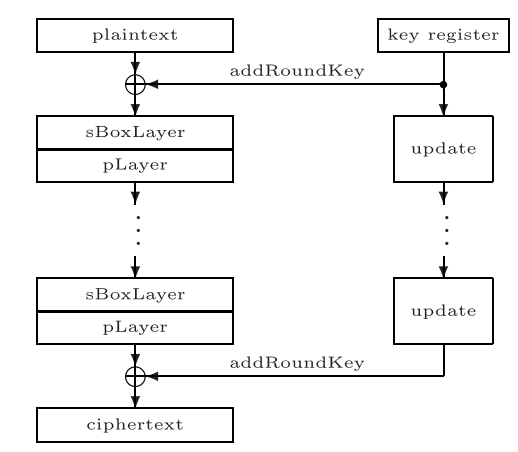
 

# PRESENT

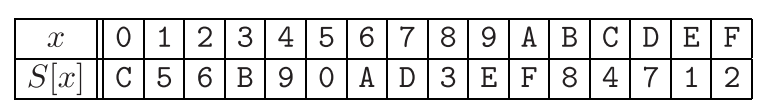
Bogdanov, Andrey, et al. *PRESENT: An ultra-lightweight block cipher*. Springer Berlin Heidelberg, 2007.

维基：<https://en.wikipedia.org/wiki/PRESENT_(cipher)>

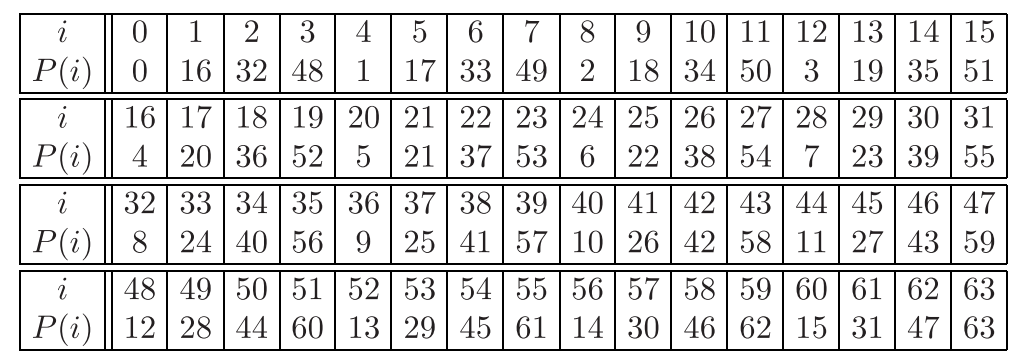
|  |  |
| --- | --- |
| Designers | [Orange Labs](https://en.wikipedia.org/wiki/Orange_Labs), [Ruhr University Bochum](https://en.wikipedia.org/wiki/Ruhr_University_Bochum) and the [Technical University of Denmark](https://en.wikipedia.org/wiki/Technical_University_of_Denmark) |
| First published | 2007-08-23 |
| Cipher detail | |
| [Key sizes](https://en.wikipedia.org/wiki/Key_size) | 80 or 128 bits |
| [Block sizes](https://en.wikipedia.org/wiki/Block_size_(cryptography)) | 64 bits |
| Structure | [SPN](https://en.wikipedia.org/wiki/Substitution-permutation_network) |
| Rounds | 31 |



其中sbox是4-4的



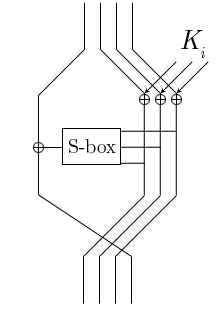
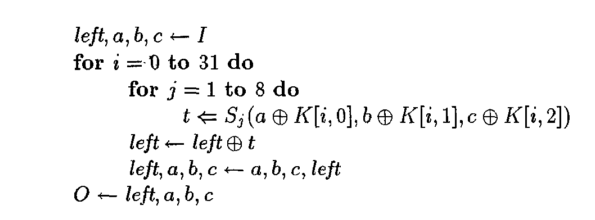
pLayer是64bit置换：



# MacGuffin

Blaze, Matt, and Bruce Schneier. "The MacGuffin block cipher algorithm." *Fast Software Encryption*. Springer Berlin Heidelberg, 1995.

|  |  |
| --- | --- |
| Designers | [Bruce Schneier](https://en.wikipedia.org/wiki/Bruce_Schneier), [Matt Blaze](https://en.wikipedia.org/wiki/Matt_Blaze) |
| First published | 1994-12-14 |
| Derived from | [DES](https://en.wikipedia.org/wiki/Data_Encryption_Standard) |
| Cipher detail | |
| [Key sizes](https://en.wikipedia.org/wiki/Key_size) | 128 bits |
| [Block sizes](https://en.wikipedia.org/wiki/Block_size_(cryptography)) | 64 bits |
| Structure | Unbalanced [Feistel network](https://en.wikipedia.org/wiki/Feistel_network" \o "Feistel network) |
| Rounds | 32 |



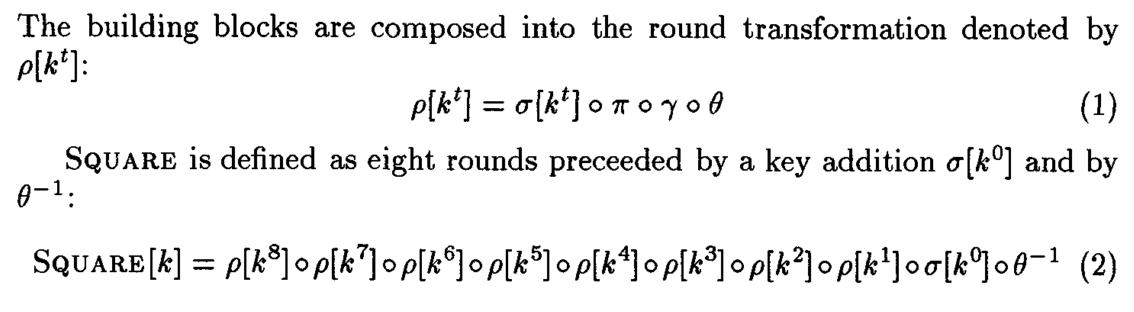
# Square

Daemen, Joan, Lars Knudsen, and Vincent Rijmen. "The block cipher Square."*Fast Software Encryption*. Springer Berlin Heidelberg, 1997.

Knudsen, Joan Daemen, Lars, and Vincent Rijmen. "The block cipher SQUARE." *Fast Software Encryption: 4th International Workshop, FSE'97, Haifa, Israel, January 1997. Proceedings*. Springer Berlin/Heidelberg, 1997.

维基：<https://en.wikipedia.org/wiki/Square_(cipher)>

|  |  |
| --- | --- |
| Designers | [Joan Daemen](https://en.wikipedia.org/wiki/Joan_Daemen), [Vincent Rijmen](https://en.wikipedia.org/wiki/Vincent_Rijmen) |
| First published | 1997 |
| Successors | [AES](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard), [CRYPTON](https://en.wikipedia.org/wiki/CRYPTON), [Twofish](https://en.wikipedia.org/wiki/Twofish" \o "Twofish),[Serpent](https://en.wikipedia.org/wiki/Serpent_(cipher)) |
| Cipher detail | |
| [Key sizes](https://en.wikipedia.org/wiki/Key_size) | 128 bits |
| [Block sizes](https://en.wikipedia.org/wiki/Block_size_(cryptography)) | 128 bits |
| Structure | [substitution-permutation network](https://en.wikipedia.org/wiki/Substitution-permutation_network) |
| Rounds | 8 |



其中：

 秘钥加

字节置换

sbox

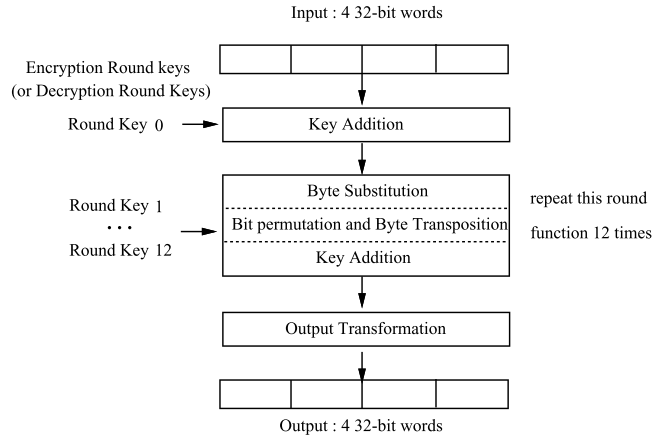
有限域乘法

# CRYPTON

Lim, Chae Hoon. "CRYPTON: A new 128-bit block cipher." *NIsT AEs Proposal*(1998).

维基：https://en.wikipedia.org/wiki/CRYPTON

|  |  |
| --- | --- |
| Designers | [Chae Hoon Lim](https://en.wikipedia.org/w/index.php?title=Chae_Hoon_Lim&action=edit&redlink=1) |
| First published | 1998 |
| Derived from | [Square](https://en.wikipedia.org/wiki/Square_(cipher)) |
| Cipher detail | |
| [Key sizes](https://en.wikipedia.org/wiki/Key_size) | 128, 192, or 256 bits |
| [Block sizes](https://en.wikipedia.org/wiki/Block_size_(cryptography)) | 128 bits |
| Structure | [Substitution-permutation network](https://en.wikipedia.org/wiki/Substitution-permutation_network) |
| Rounds | 12 |

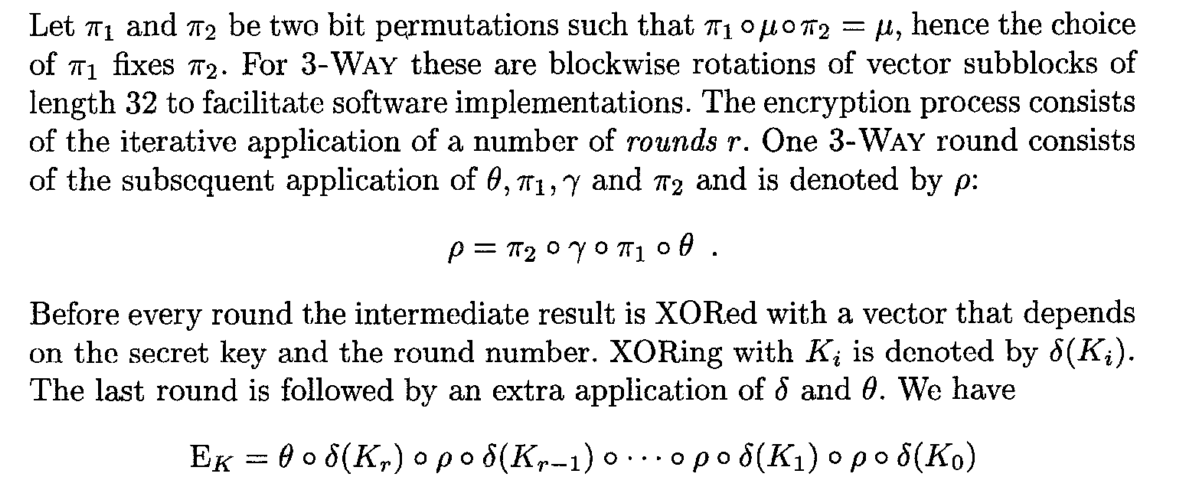


# 3-Way

Daemen, Joan, René Govaerts, and Joos Vandewalle. "A new approach to block cipher design." *Fast Software Encryption*. Springer Berlin Heidelberg, 1994.

维基：https://en.wikipedia.org/wiki/3-Way

|  |  |
| --- | --- |
| Designers | [Joan Daemen](https://en.wikipedia.org/wiki/Joan_Daemen) |
| First published | 1994 |
| Successors | [NOEKEON](https://en.wikipedia.org/wiki/NOEKEON) |
| Related to | [BaseKing](https://en.wikipedia.org/wiki/BaseKing) |
| Cipher detail | |
| [Key sizes](https://en.wikipedia.org/wiki/Key_size) | 96 bits |
| [Block sizes](https://en.wikipedia.org/wiki/Block_size_(cryptography)) | 96 bits |
| Structure | [Substitution-permutation network](https://en.wikipedia.org/wiki/Substitution-permutation_network) |
| Rounds | 11 |



其中：

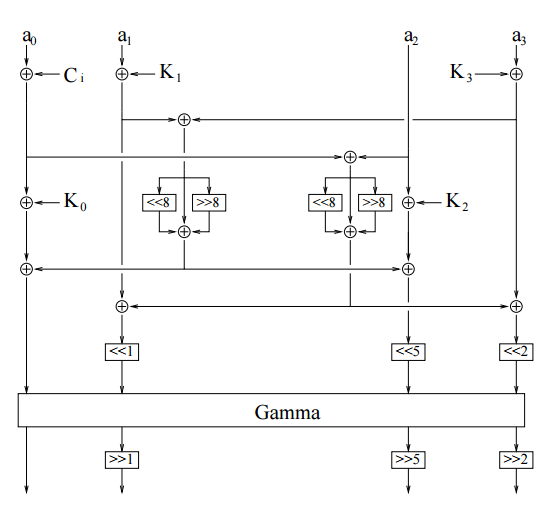
# NOEKEON

Daemen, Joan, et al. "Nessie proposal: NOEKEON." *First Open NESSIE Workshop*. 2000.

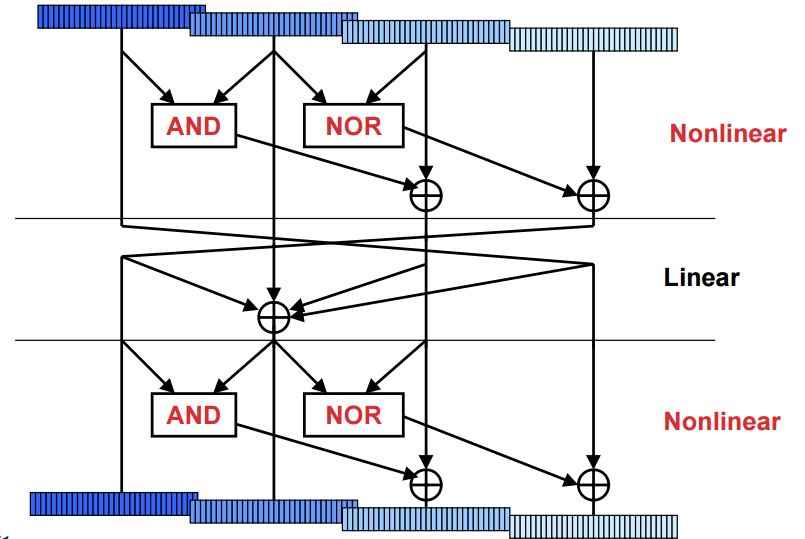
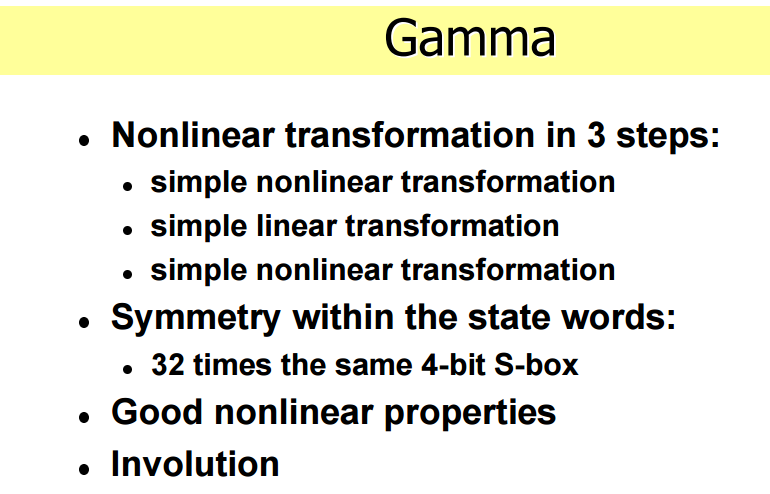
Knudsen, Lars R., and Håvard Raddum. "On noekeon." (2001).

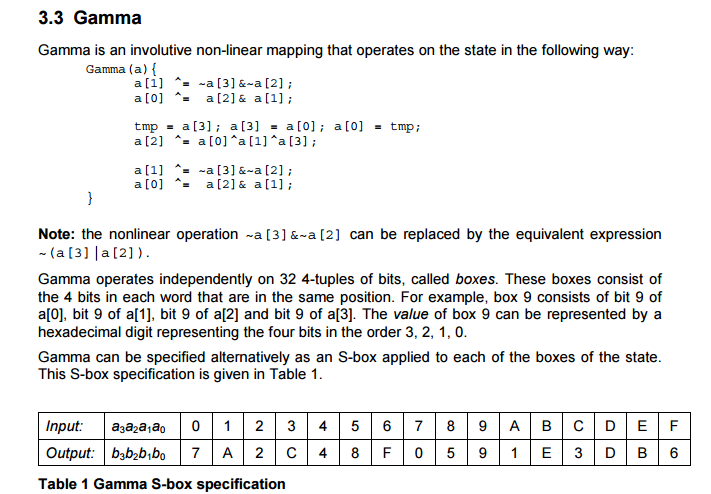
维基：https://en.wikipedia.org/wiki/NOEKEON

|  |  |
| --- | --- |
| Designers | [Joan Daemen](https://en.wikipedia.org/wiki/Joan_Daemen), [Michaël Peeters](https://en.wikipedia.org/w/index.php?title=Micha%C3%ABl_Peeters&action=edit&redlink=1), [Gilles Van Assche](https://en.wikipedia.org/wiki/Gilles_Van_Assche), [Vincent Rijmen](https://en.wikipedia.org/wiki/Vincent_Rijmen) |
| First published | 2000-09 |
| Derived from | [3-Way](https://en.wikipedia.org/wiki/3-Way), [BaseKing](https://en.wikipedia.org/wiki/BaseKing" \o "BaseKing) |
| Cipher detail | |
| [Key sizes](https://en.wikipedia.org/wiki/Key_size) | 128 bits |
| [Block sizes](https://en.wikipedia.org/wiki/Block_size_(cryptography)) | 128 bits |
| Rounds | 16 |



其中：



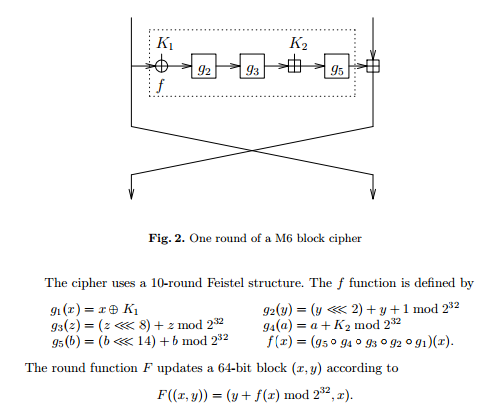


# M6

Kelsey, John, Bruce Schneier, and David Wagner. "Mod n cryptanalysis, with applications against RC5P and M6." *Fast Software Encryption*. Springer Berlin Heidelberg, 1999.

维基：<https://en.wikipedia.org/wiki/M6_(cipher)>

|  |  |
| --- | --- |
| Designers | [Hitachi](https://en.wikipedia.org/wiki/Hitachi,_Ltd.) |
| First published | 1997 |
| Successors | [M8](https://en.wikipedia.org/wiki/M8_(cipher)) |
| Cipher detail | |
| [Key sizes](https://en.wikipedia.org/wiki/Key_size) | 40-64 bits |
| [Block sizes](https://en.wikipedia.org/wiki/Block_size_(cryptography)) | 64 bits |
| Structure | [Feistel network](https://en.wikipedia.org/wiki/Feistel_cipher) |
| Rounds | 10 |

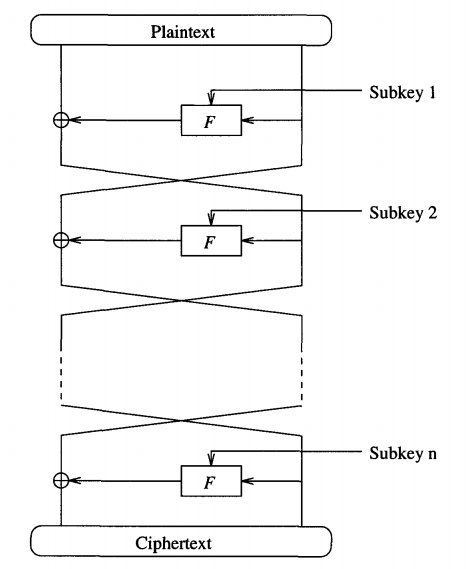


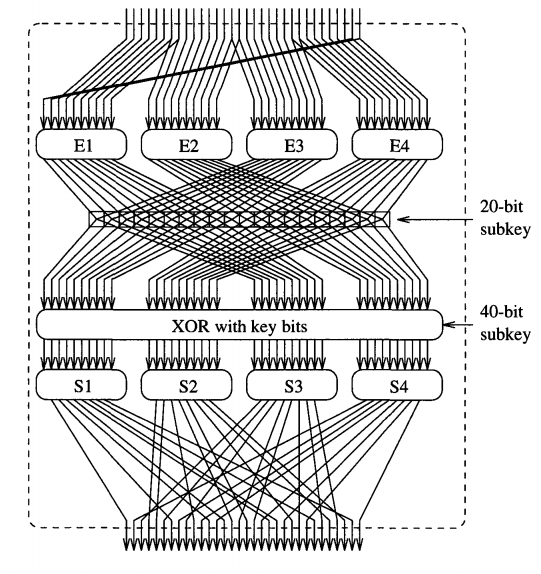
# ICE

Kwan, Matthew. "The design of the ICE encryption algorithm." *Fast Software Encryption*. Springer Berlin Heidelberg, 1997.

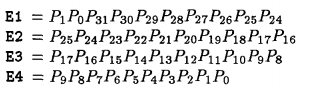
维基：<https://en.wikipedia.org/wiki/ICE_(cipher)>

|  |  |
| --- | --- |
| Designers | Matthew Kwan |
| First published | 1997 |
| Derived from | [DES](https://en.wikipedia.org/wiki/Data_Encryption_Standard) |
| Cipher detail | |
| [Key sizes](https://en.wikipedia.org/wiki/Key_size) | 64 bits (ICE), 64×n bits (ICE-n) |
| [Block sizes](https://en.wikipedia.org/wiki/Block_size_(cryptography)) | 64 bits |
| Structure | [Feistel network](https://en.wikipedia.org/wiki/Feistel_network) |
| Rounds | 16 (ICE), 8 (Thin-ICE), 16×n(ICE-n) |

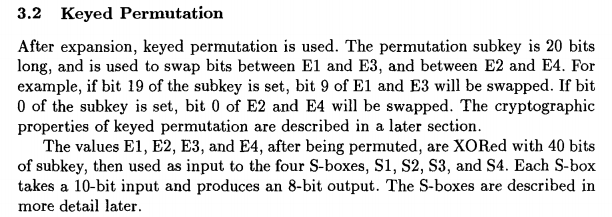




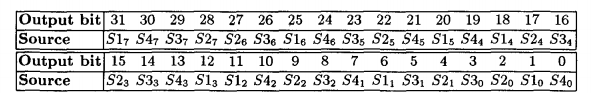
其中E是扩展，和DES的一样



交换（秘钥）



最后的置换

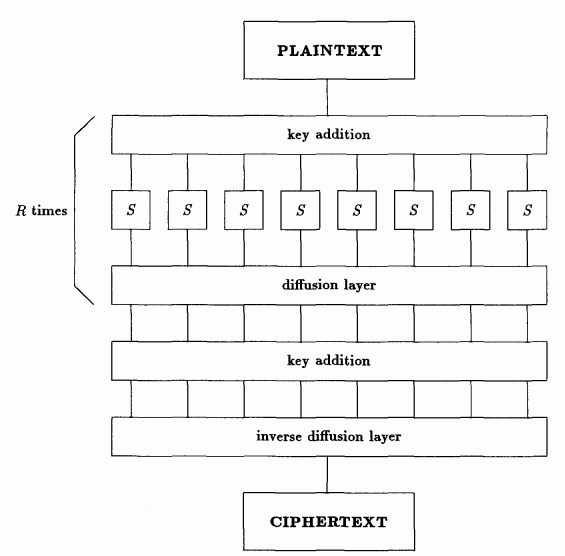


# SHARK

Rijmen, Vincent, et al. "The cipher SHARK." *Fast Software Encryption*. Springer Berlin Heidelberg, 1996.

维基：<https://en.wikipedia.org/wiki/SHARK>

|  |  |
| --- | --- |
| Designers | [Vincent Rijmen](https://en.wikipedia.org/wiki/Vincent_Rijmen), [Joan Daemen](https://en.wikipedia.org/wiki/Joan_Daemen),[Bart Preneel](https://en.wikipedia.org/wiki/Bart_Preneel), [Antoon Bosselaers](https://en.wikipedia.org/w/index.php?title=Antoon_Bosselaers&action=edit&redlink=1), [Erik De Win](https://en.wikipedia.org/w/index.php?title=Erik_De_Win&action=edit&redlink=1) |
| First published | 1996 |
| Successors | [KHAZAD](https://en.wikipedia.org/wiki/KHAZAD), [Rijndael](https://en.wikipedia.org/wiki/Rijndael) |
| Cipher detail | |
| [Key sizes](https://en.wikipedia.org/wiki/Key_size) | 128 bits |
| [Block sizes](https://en.wikipedia.org/wiki/Block_size_(cryptography)) | 64 bits |
| Structure | [Substitution-permutation network](https://en.wikipedia.org/wiki/Substitution-permutation_network) |
| Rounds | 6 |



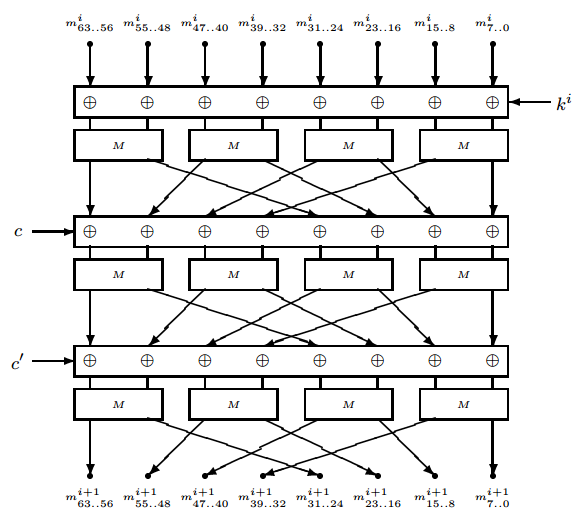
其中diffusion layer是有限域乘2^m(m为sbox的输出)

# CS-Cipher

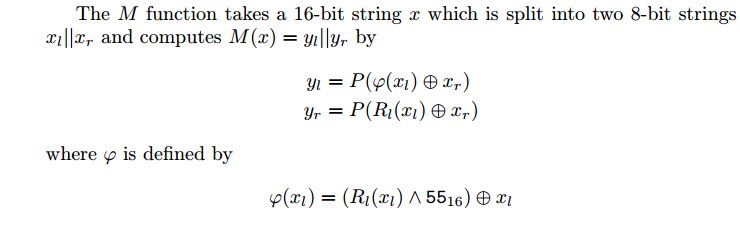
Stern, Jacques, and Serge Vaudenay. "Cs-cipher." *Fast Software Encryption*. Springer Berlin Heidelberg, 1998.

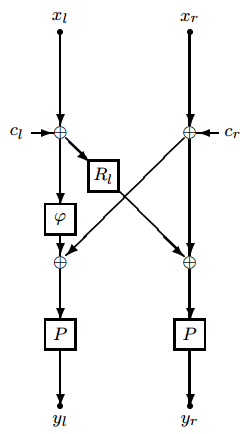
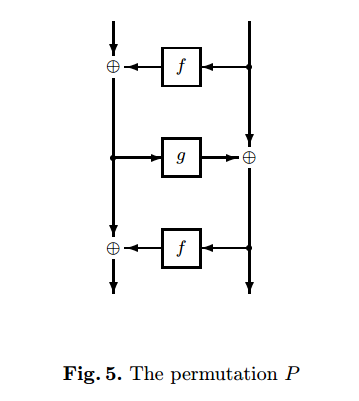
维基：<https://en.wikipedia.org/wiki/CS-Cipher>

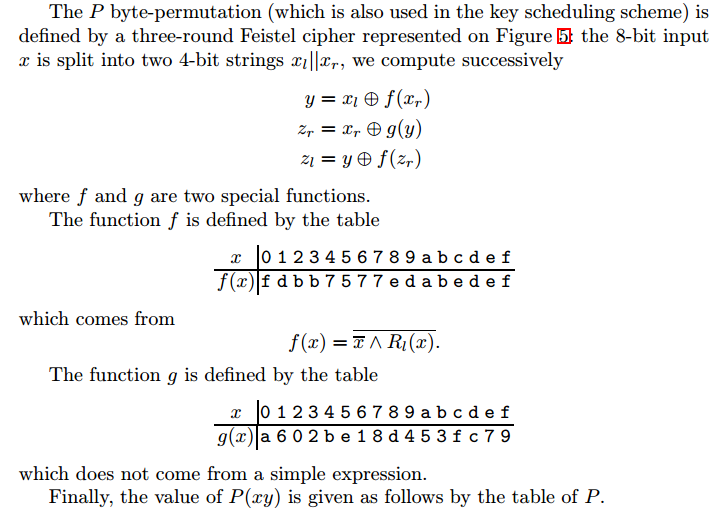
|  |  |
| --- | --- |
| Designers | [Jacques Stern](https://en.wikipedia.org/wiki/Jacques_Stern) and [Serge Vaudenay](https://en.wikipedia.org/wiki/Serge_Vaudenay) |
| First published | 1998 |
| Cipher detail | |
| [Key sizes](https://en.wikipedia.org/wiki/Key_size) | 128 bits |
| [Block sizes](https://en.wikipedia.org/wiki/Block_size_(cryptography)) | 64 bits |
| Structure | [Feistel network](https://en.wikipedia.org/wiki/Feistel_cipher) |
| Rounds | 8 |

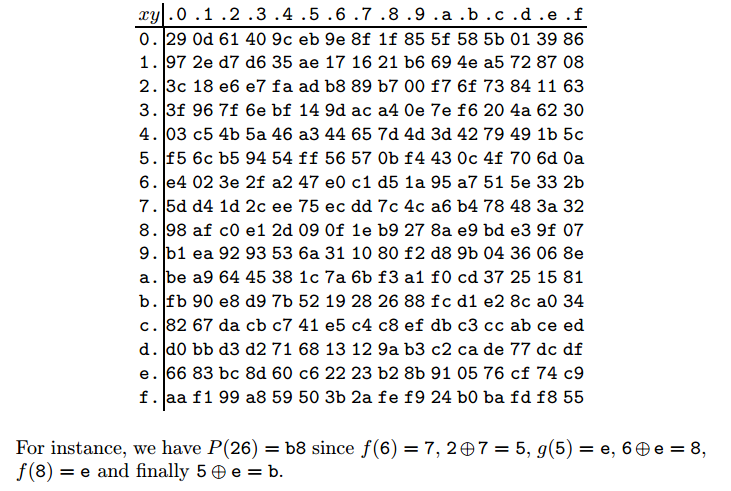


其中：M





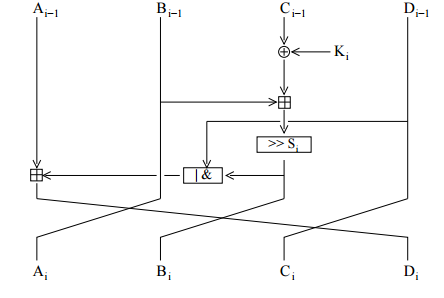


# NUSH

Knudsen L R, Raddum H. A first report on Whirlpool, NUSH, SC2000, Noekeon, Two-Track-Mac and RC6, 2001[J].

维基：<https://en.wikipedia.org/wiki/NUSH>

|  |  |
| --- | --- |
| Designers | [Anatoly Lebedev](https://en.wikipedia.org/w/index.php?title=Anatoly_Lebedev&action=edit&redlink=1), [Alexey Volchkov](https://en.wikipedia.org/w/index.php?title=Alexey_Volchkov&action=edit&redlink=1) |
| First published | 2000 |
| Cipher detail | |
| [Key sizes](https://en.wikipedia.org/wiki/Key_size) | 128, 192, or 256 bits |
| [Block sizes](https://en.wikipedia.org/wiki/Block_size_(cryptography)) | 64, 128, or 256 bits |
| Rounds | 9, 17, or 33 |
| Best public [cryptanalysis](https://en.wikipedia.org/wiki/Cryptanalysis) | |
| A [linear attack](https://en.wikipedia.org/wiki/Linear_cryptanalysis) faster than exhaustive search has been found. | |



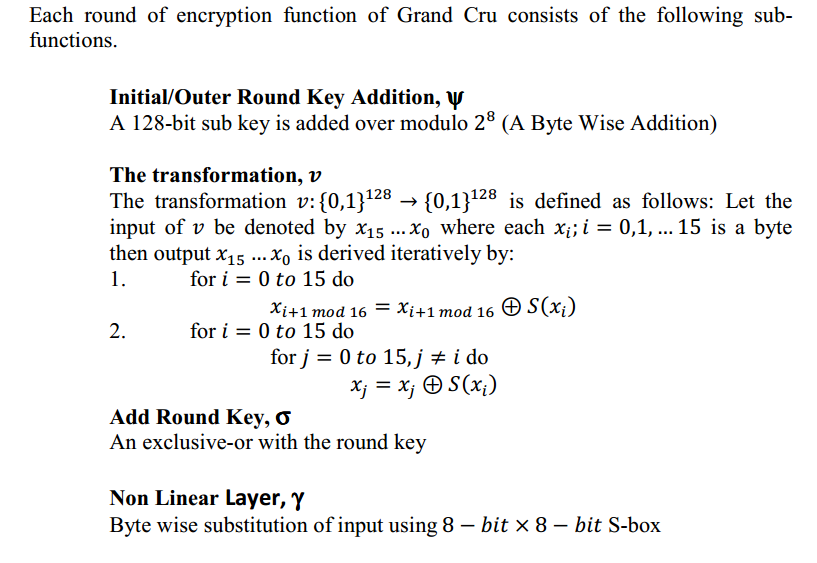
NUSH is a block cipher that accepts 128-, 192- or 256-bit keys, and with block lengths that can be 64, 128 or 256 bits. Each block consists of four registers, which are mixed with key material and transformed through a number of rounds. For the 64-, 128- and 256-bit block versions, the number of rounds are 9, 17 and 33 respectively. Whitening keys are added to the block before the first round, and after the last round. Each round consists of four iterations where the registers are mixed with each other and with key material. In each iteration two of the registers are changed in a non-linear way, and the registers are rotated as in a type-3 Feistel network. The details of one round are given in the following figure.The number of bit rotations, Si , follows a schedule, and is different in each round. The box with ’—&’ in it denotes the logical OR or AND operations, a schedule defines which one is used in the different rounds.

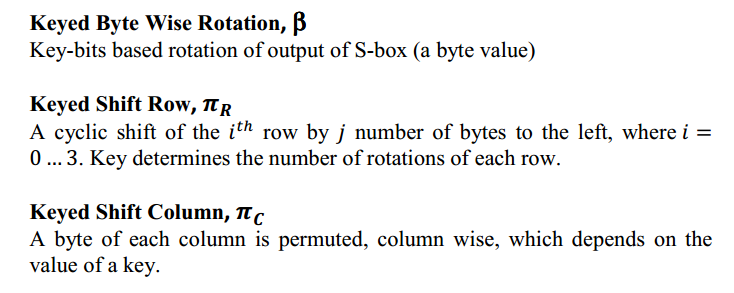
# Grand Cru

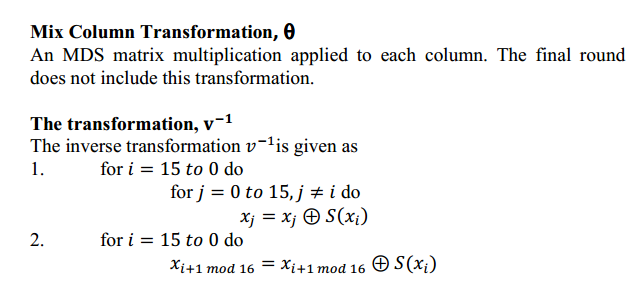
Khan A A, Murtaza G. Efficient Implementation of Grand Cru with TI C6x+ Processor[J]. IACR Cryptology ePrint Archive, 2011, 2011: 385.

维基：https://en.wikipedia.org/wiki/Grand\_Cru\_(cipher)

|  |  |
| --- | --- |
| Designers | [Johan Borst](https://en.wikipedia.org/w/index.php?title=Johan_Borst&action=edit&redlink=1) |
| First published | 2000 |
| Derived from | [Rijndael](https://en.wikipedia.org/wiki/Rijndael) |
| Cipher detail | |
| [Key sizes](https://en.wikipedia.org/wiki/Key_size) | 128 bits |
| [Block sizes](https://en.wikipedia.org/wiki/Block_size_(cryptography)) | 128 bits |
| Structure | [Substitution-permutation network](https://en.wikipedia.org/wiki/Substitution-permutation_network) |
| Rounds | 10 |





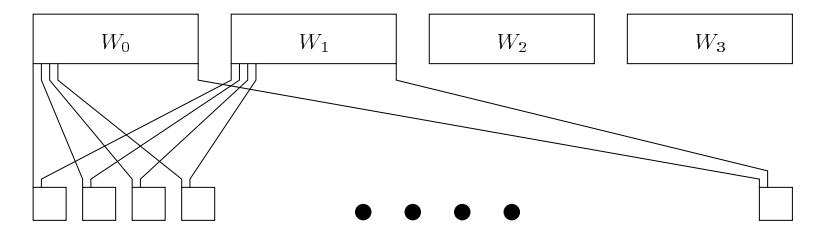


# Q

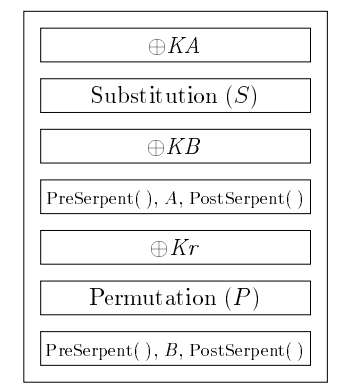
Keliher L, Meijer H, Tavares S. High probability linear hulls in Q[C]//Proceedings of Second Open NESSIE Workshop, Royal Holloway College, University of London, Egham, UK. 2001.

维基：<https://en.wikipedia.org/wiki/Q_(cipher)>

|  |  |
| --- | --- |
| Designers | [Leslie McBride](https://en.wikipedia.org/w/index.php?title=Leslie_McBride&action=edit&redlink=1) |
| First published | November 2000 |
| Derived from | [AES](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard), [Serpent](https://en.wikipedia.org/wiki/Serpent_(cipher)) |
| Cipher detail | |
| [Key sizes](https://en.wikipedia.org/wiki/Key_size) | 128, 192, or 256 bits |
| [Block sizes](https://en.wikipedia.org/wiki/Block_size_(cryptography)) | 128 bits |
| Structure | [Substitution-permutation network](https://en.wikipedia.org/wiki/Substitution-permutation_network) |
| Rounds | 8 or 9 |



PreSerpent( ) bit wise permutation PostSerpent( )则相反



# E2

Matsui M, Tokita T. Cryptanalysis of a reduced version of the block cipher E2[C]//Fast Software Encryption. Springer Berlin Heidelberg, 1999: 71-80.

维基：<https://en.wikipedia.org/wiki/E2_(cipher)>

|  |  |
| --- | --- |
| Designers | [NTT](https://en.wikipedia.org/wiki/Nippon_Telegraph_and_Telephone) |
| First published | 1998 |
| Successors | [Camellia](https://en.wikipedia.org/wiki/Camellia_(cipher)) |
| Cipher detail | |
| [Key sizes](https://en.wikipedia.org/wiki/Key_size) | 128, 192, or 256 bits |
| [Block sizes](https://en.wikipedia.org/wiki/Block_size_(cryptography)) | 128 bits |
| Structure | [Feistel network](https://en.wikipedia.org/wiki/Feistel_cipher) |
| Rounds | 12 |

