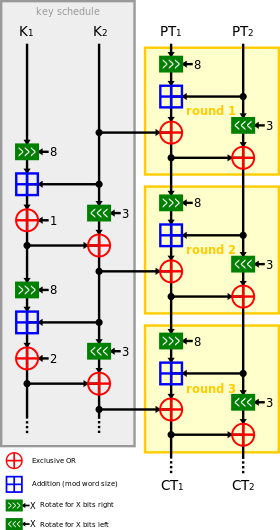
1. speck

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

|  |  |
| --- | --- |
| **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) |



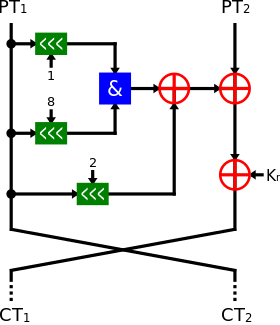
1. Simon

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

|  |  |
| --- | --- |
| [**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) |



1. Lucifer

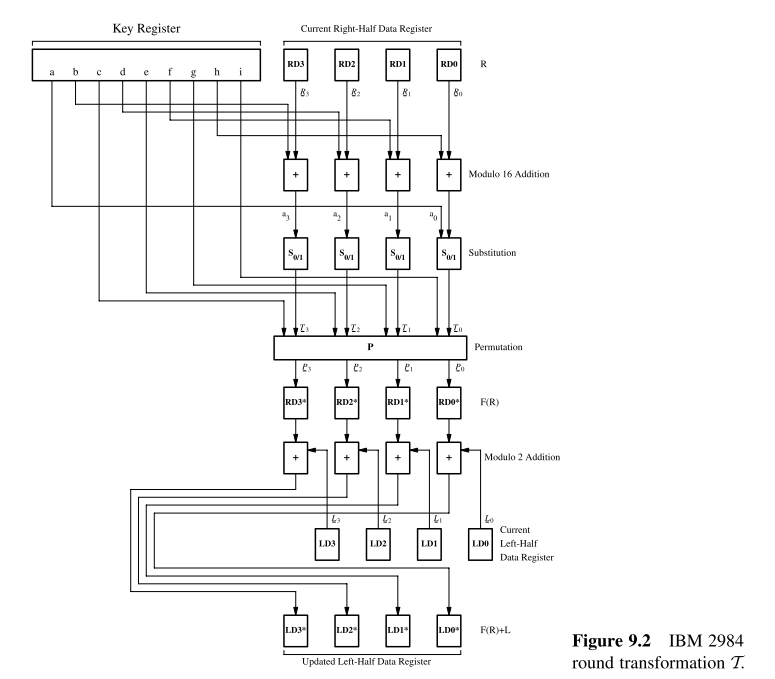
Sorkin, Arthur. "Lucifer, a cryptographic algorithm." Cryptologia 8.1 (1984): 22-42.

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

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

|  |  |
| --- | --- |
| [**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 |





1. CLEFIA

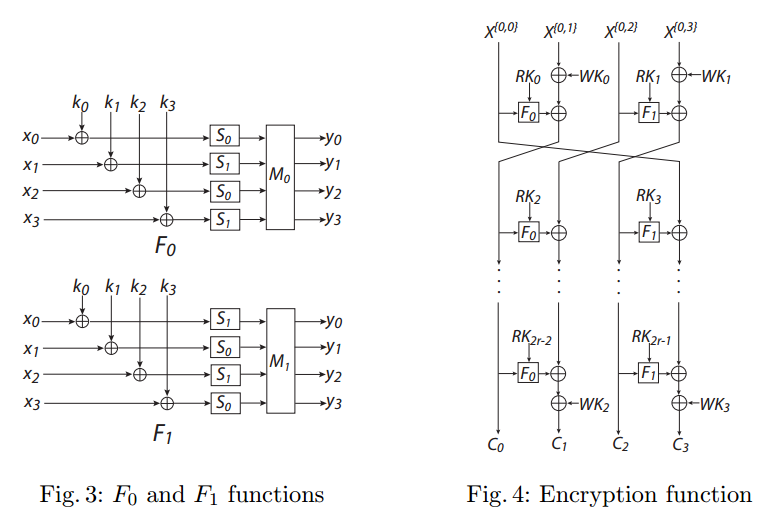
Tezcan, Cihangir. "The improbable differential attack: Cryptanalysis of reduced round CLEFIA." *Progress in Cryptology-INDOCRYPT 2010*. Springer Berlin Heidelberg, 2010. 197-209.

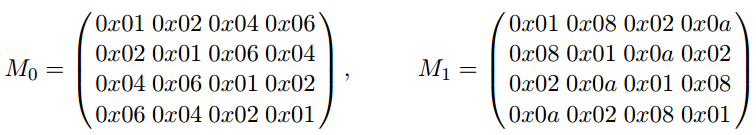
Shirai, Taizo, et al. "The 128-bit blockcipher CLEFIA." *Fast software encryption*. Springer Berlin Heidelberg, 2007.

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

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

|  |  |
| --- | --- |
| [**Key sizes**](https://en.wikipedia.org/wiki/Key_size) | 128, 192, or 256 bits |
| **，[Block sizes](https://en.wikipedia.org/wiki/Block_size_(cryptography)" \o "Block size (cryptography))** | 128 bits |
| **Structure** | [Feistel network](https://en.wikipedia.org/wiki/Feistel_network) |
| **Rounds** | 18, 22, or 26 |





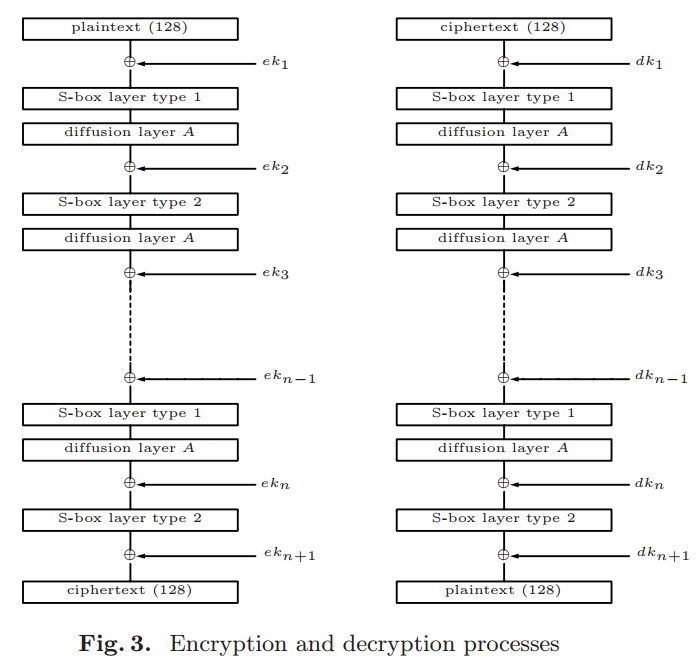
1. ARIA

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)

|  |  |
| --- | --- |
| [**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 |



6. 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

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

