Feistel cipher

From Wikipedia, the free encyclopedia

In cryptography, a **Feistel cipher** is a symmetric structure used in the construction of block ciphers, named after the German-born physicist and cryptographer Horst Feistel who did pioneering research while working for IBM (USA); it is also commonly known as a **Feistel network**. A large proportion of block ciphers use the scheme, including the Data Encryption Standard (DES). The Feistel structure has the advantage that encryption and decryption operations are very similar, even identical in some cases, requiring only a reversal of the key schedule. Therefore, the size of the code or circuitry required to implement such a cipher is nearly halved.

A Feistel network is an iterated cipher with an internal function called a round function.[1]

Contents

Historical

Feistel networks were first seen commercially in IBM's Lucifer cipher, designed by Horst Feistel and Don Coppersmith in 1973. Feistel networks gained respectability when the U.S. Federal Government adopted the DES (a cipher based on Lucifer, with changes made by the NSA). Like other components of the DES, the iterative nature of the Feistel construction makes implementing the cryptosystem in hardware easier (particularly on the hardware available at the time of DES's design).

Theoretical work

Many modern and also some old symmetric block ciphers are based on Feistel networks (e.g. GOST 28147-89 block cipher), and the structure and properties of Feistel ciphers have been extensively explored by cryptographers. Specifically, Michael Luby and Charles Rackoff analyzed the Feistel cipher construction, and proved that if the round function is a cryptographically secure pseudorandom function, with K_i used as the seed, then 3 rounds are sufficient to make the block cipher a pseudorandom permutation, while 4 rounds are sufficient to make it a "strong" pseudorandom permutation (which means that it remains pseudorandom even to an adversary who gets oracle access to its inverse permutation).[2]

Because of this very important result of Luby and Rackoff, Feistel ciphers are sometimes called Luby–Rackoff block ciphers. Further theoretical work has generalized the construction somewhat, and given more precise bounds for security.[3][4]

Construction details

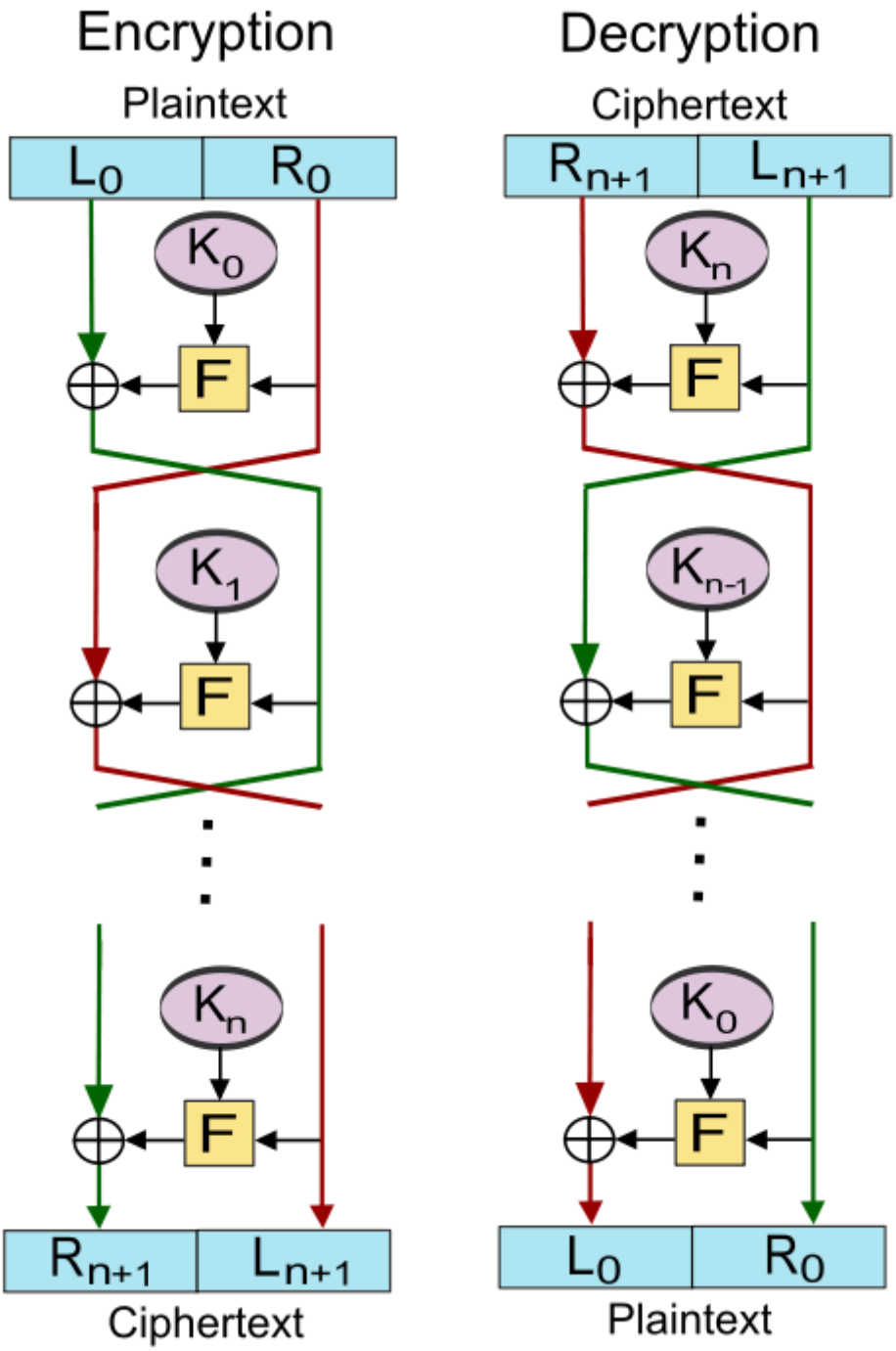
Let $\mathbf{F}$ be the round function and let $K_0, K_1, \ldots, K_n$ be the sub-keys for the rounds $0, 1, \ldots, n$ respectively.

Then the basic operation is as follows:

Split the plaintext block into two equal pieces, (L_0, R_0)

For each round $i = 0, 1, \ldots, n$, compute

$$L_{i+1} = R_i$$



$$R_{i+1} = L_i \oplus \mathbf{F}(R_i, K_i).$$

Then the ciphertext is (R_{n+1}, L_{n+1}).

Decryption of a ciphertext (R_{n+1}, L_{n+1}) is accomplished by computing for $i = n, n-1, \ldots, 0$

$$R_i = L_{i+1}$$
$$L_i = R_{i+1} \oplus \mathbf{F}(L_{i+1}, K_i).$$

Then (L_0, R_0) is the plaintext again.

One advantage of the Feistel model compared to a substitution-permutation network is that the round function $\mathbf{F}$ does not have to be invertible.

The diagram illustrates both encryption and decryption. Note the reversal of the subkey order for decryption; this is the only difference between encryption and decryption.

Unbalanced Feistel cipher

Unbalanced Feistel ciphers use a modified structure where L_0 and R_0 are not of equal lengths.[5] The Skipjack cipher is an example of such a cipher. The Texas Instruments Digital Signature Transponder uses a proprietary unbalanced Feistel cipher to perform challenge-response authentication.[6]

The Thorp shuffle is an extreme case of an unbalanced Feistel cipher in which one side is a single bit. This has better provable security than a balanced Feistel cipher but requires more rounds.[7]

Other uses

The Feistel construction is also used in cryptographic algorithms other than block ciphers. For example, the optimal asymmetric encryption padding (OAEP) scheme uses a simple Feistel network to randomize ciphertexts in certain asymmetric key encryption schemes.

A generalized Feistel algorithm can be used to create strong permutations on small domains of size not a power of two (see format-preserving encryption).[7]

Feistel networks as a design component

Whether the entire cipher is a Feistel cipher or not, Feistel-like networks can be used as a component of a cipher's design. For example, MISTY1 is a Feistel cipher using a three-round Feistel network in its round function, Skipjack is a modified Feistel cipher using a Feistel network in its G permutation, and Threefish (part of Skein) is a non-Feistel block cipher that uses a Feistel-like MIX function.

List of Feistel ciphers

Feistel or modified Feistel:

- Blowfish
- Camellia
- CAST-128
- DES
- FEAL
- GOST 28147-89
- ICE
- KASUMI
- LOKI97
- Lucifer
- MARS
- MAGENTA
- MISTY1
- RC5
- Simon
- TEA
- Triple DES
- Twofish
- XTEA

Generalised Feistel:

- CAST-256
- CLEFIA
- MacGuffin
- RC2
- RC6
- Skipjack
- SMS4

See also

- Cryptography

- Stream cipher
- Substitution-permutation network
- Lifting scheme for discrete wavelet transform has pretty much the same structure
- Format-preserving encryption
- Lai-Massey scheme

References

1. Menezes, Alfred J.; Oorschot, Paul C. van; Vanstone, Scott A. (2001). *Handbook of Applied Cryptography* (Fifth ed.). p. 251. ISBN 0849385237.
2. Luby, Michael; Rackoff, Charles (April 1988), "How to Construct Pseudorandom Permutations from Pseudorandom Functions", *SIAM Journal on Computing*, **17** (2): 373–386, ISSN 0097-5397 (https://www.worldcat.org/issn/0097-5397), doi:10.1137/0217022 (https://doi.org/10.1137%2F0217022)
3. Patarin, Jacques (October 2003), Boneh, Dan, ed., "Luby-Rackoff: 7 Rounds Are Enough for $2^{n(1-\varepsilon)}$ Security" (https://www.iacr.org/archive/crypto2003/27290510/27290510.pdf) (PDF), *Advances in Cryptology—CRYPTO 2003*, Lecture Notes in Computer Science, **2729**: 513–529, doi:10.1007/b11817 (https://doi.org/10.1007%2Fb11817), retrieved 2009-07-27
4. Yuliang Zheng; Tsutomu Matsumoto; Hideki Imai. "On the Construction of Block Ciphers Provably Secure and Not Relying on Any Unproved Hypotheses". 2001. doi: 10.1007/0-387-34805-0_42 (https://dx.doi.org/10.1007%2F0-387-34805-0_42)
5. http://www.schneier.com/paper-unbalanced-feistel.html
6. S. Bono, M. Green, A. Stubblefield, A. Rubin, A. Juels, M. Szydlo. "Security Analysis of a Cryptographically-Enabled RFID Device". In *Proceedings of the USENIX Security Symposium*, August 2005. (pdf) (http://www.usenix.org/events/sec05/tech/bono/bono.pdf)
7. Ben Morris, Phillip Rogaway, Till Stegers. "How to Encipher Messages on a Small Domain". CRYPTO 2009. (pdf) (http://www.cs.ucdavis.edu/~rogaway/papers/thorp.pdf)

Categories: Cryptography | Feistel ciphers
