Preface

Feistel ciphers take an important part in secret key cryptography from both theoretical and practical point of view. After DES, Feistel ciphers used in the Industry had a dynamic revival. First of all, new schemes have been published, like GOST in Russia, RC-6 and SIMON in the United States. On the other hand, new needs appeared, beyond resistance against classical cryptography attacks, like resistance to physical attacks, or obfuscation. With Feistel ciphers, it is very easy to generate permutations from various round functions. This allowed to construct many proprietary algorithms (hence secret algorihtms) for specific needs and used by the Industry. This is why we considerd that is was needed to have an up to date comprehensive survey on different kinds of Feistel ciphers, including attacks and security results. From a theoretical point of view, it is from these ciphers that Luby and Rackoff proved in 1989 their famous theorem. This subsequently leads to a very large number of research papers in cryptography. This theorem gave a very innovative and powerful method to obtain security proof for "generic" ciphers. It was then possible to prove that one can obtain pseudorandom permutations (i.e., permutations easily generated by computers that are indistinguishable from truly random permutations) using pseudorandom functions. More recently (2008–2011), again from Feistel ciphers, it was possible to prove the equivalence between the random oracle model and the ideal cipher model, a famous problem that was left open for many years.

From a practical point of view, Feistel ciphers had their days of glory with the DES algorithm and its variants (3DES with two or three keys, XDES, etc.) that were the most widely used secret key algorithms around the world between 1977 and 2000. Since then, the AES algorithm, which is not a Feistel cipher, became the standard for secret key encryption. However, 3DES is still used in many applications, like in banking applications. Notice that the replacement of DES by AES is due to the fact that the parameters used in DES (in particular the size of the key) or in 3DES (in particular the size of the inputs and the outputs) have become too small for many modern applications, whereas the principle of Feistel ciphers stays very strong.

Versailles, Yvelines, France — Jacques Patarin
January 2017

http://www.springer.com/978-3-319-49528-6

Feistel Ciphers
Security Proofs and Cryptanalysis
Nachef, V.; Patarin, J.; Volte, E.
2017, XV, 309 p. 39 illus., 6 illus. in color., Hardcover
ISBN: 978-3-319-49528-6