| 報告番号 | 甲　第　14032　号 |
| --- | --- |

# 主　論　文　の　要　旨

論文題目　Design and Analysis of Diffusion in Feistel-Type Symmetric-Key Cryptosystems
(Feistel 型共通鍵暗号システムの拡散層の設計と解析)

氏　　名　渋谷　香士

## 論　文　内　容　の　要　旨

Information security is a crucial technology for people all over the world to live safely and securely. It consists of several technologies including network security and application security to mainly ensure confidentiality, integrity and availability. Among them, cryptography is a fundamental technology to design information security applications. Cryptography provides several important functionalities including authenticity, confidentiality, integrity and randomness. It also has several categories and two fundamental technologies are known as public-key and symmetric-key cryptography. We focus on the latter one including block ciphers, cryptographic hash functions and stream ciphers. The main advantage of symmetric-key cryptography compared to public-key cryptography is its high computational performance. Thus, symmetric-key cryptography is necessary for most information security applications even when public-key cryptography is used in the applications.

A block cipher, one of symmetric-key primitives, is a keyed permutation used for encrypting and decrypting digital data by a given secret key. It has much wider applications than just data encryption. In fact, it has been well known as modes of operation that it provides several functionalities including authenticity and data integrity by using a block cipher as a component. Namely, if we have a good block cipher, we can easily derive several cryptographic applications such as a cryptographic hash

function, a stream cipher and a message authentication code by using the block cipher as a component. Therefore, a block cipher is considered to play a central role in symmetric-key primitives.

A modern block cipher typically has iterative structure which iteratively utilizes a round function consisting of non-linear functions and linear functions. The confusion and diffusion, which are known as two important properties for designing a secure block cipher, are considered to be provided by non-linear functions and linear functions, respectively. The research related to the confusion including a method to design a good small nonlinear permutation called S-box has been well studied. On the other hand, there still exist some rooms to improve the diffusion. In general, a cipher with slow diffusion requires a lot of iterations to be secure, and then takes a long encryption / decryption time. Therefore, improving the diffusion is crucial for designing an efficient and secure block cipher.

While various structures have been proposed to design a block cipher, Substitution Permutation Networks (SPNs) and Feistel-type structures have been known as two main structures among them. SPNs consist of a substitution layer (several small non-linear maps referred to as S-boxes applied in parallel) and a permutation layer (also known as a linear diffusion layer) in a round. One of the advantages of SPNs compared to Feistel-type structures is its fast diffusion, since all input data are converted by a substitution layer and a permutation layer in a round. On the other hand, SPNs require an inverse function for a decryption. This implies that an encryption function and a decryption function are required to be separately implemented for SPNs. Feistel-type structures divide input data into more than two sub-blocks, then almost half of them are converted by non-linear functions called F-functions in a round. In other words, almost half of the input data are unchanged in a round. In contrast to SPNs, the main advantage of Feistel-type structures is the involution property which does not require an inverse function for a decryption. That is, for Feistel-type structures, only an encryption function is required to be implemented for both encryption and decryption. Moreover, the size of F-functions, non-linear functions used in Feistel-type structures, in a round is almost half compared to that of SPNs. These properties lead to a compact implementation. On the other hand, its main drawback is slow diffusion compared to SPNs, since almost half of the input data are unchanged in a round.

This thesis is dedicated to design and analysis of diffusion in Feistel-type symmetric-key cryptosystems including balanced Feistel networks (BFNs) and generalized Feistel networks (GFNs). BFNs and d-line GFNs divide input data into two and d sub-blocks, respectively, where $d > 2$ is a positive integer. Thanks to the involution

property which does not require an inverse function for a decryption, Feistel-type constructions are known to be implemented more compact than SPNs. However, it has been well known that the diffusion of Feistel-type constructions is slower than that of SPN-type constructions. Despite the wide use and long research history of Feistel-type structures, its diffusion properties have not been thoroughly analyzed. We tackle this problem in this thesis to unveil the theoretical limitation of the diffusion layers for Feistel-type structures. More specifically, we address mainly three topics in this thesis to improve the diffusion of Feistel-type structures: accurate evaluations for the security of Feistel-type structures regarding the diffusion, efficient design strategies for F-functions of Feistel-type structures, and efficient design strategies for round permutations which are linear permutations between each round.

First, we study the way to precisely evaluate the security of wide variety of BFNs and GFNs against differential and linear cryptanalysis. We propose a new approach to efficiently and accurately evaluate the security of BFNs and GFNs regarding the diffusion with large parameters. Second, we focus on 3-line GFNs. Then, it is proven that 3-line GFNs with double substitution permutation (SP)-functions as F-functions are superior to 4-line GFNs with respect to an efficiency metric for the diffusion. Third, we classify all possible connections of 4-line GFNs, then show that there are only 2 non-contracting constructions in the class of 4-line GFNs up to equivalence, namely, the type-I and type-II GFNs, where 4-line type-I and type-II GFNs have one and two F-functions in a round, respectively. Moreover, we propose to instantiate the GFNs with SPS-functions (two substitution layers separated by a permutation layer) or double SP-functions instead of single SP-functions (one substitution-permutation layer) as F-functions, and show that those constructions are more efficient regarding the diffusion than single SP-functions. Forth, we explore the optimality of BFNs with the wide class of $(SP)^u$ and $(SP)^uS$ F-functions, where u is an arbitrary positive integer. We provide the tight lower bounds on the minimum number of active S-boxes, which is an important metric for the diffusion, for those constructions, then show that SPS and SPSP F-functions are optimal among $(SP)^u$ and $(SP)^uS$ constructions in terms of the efficiency metric for the diffusion. Finally, we present how to further improve the diffusion of type-II GFNs by modifying their round permutations (linear permutation between each round). We propose to alternately use two different round permutations instead of a single round permutation, then show the first optimal constructions for 12-line GFNs which achieve the theoretical lower bound on the maximum diffusion round, another metric for the diffusion.

Our results are useful for a deeper understanding the security and theoretical

limitations of Feistel-type symmetric-key cryptosystems. One of the direct applications of our results is designing more efficient and secure symmetric-key primitives.