IBCIPHERS – СИММЕТРИЧНЫЕ ИТЕРАТИВНЫЕ БЛОЧНЫЕ ШИФРЫ С ФУНКЦИОНАЛЬНЫМИ КЕЙСАМИ

Г. П. Агибалов

Томский государственный университет
Томск, Россия
e-mail: agibalov@isc.tsu.ru

Определяется класс симметричных итеративных блочных шифров, называемых «SIBCiphers». Каждый раунд шифра в этом классе представлен инъективной системой булевых функций, каждая из которых зависит от малого числа аргументов, являющихся некоторыми входами в раунд. Ключ раунда в нем включает в себя некоторые из функций и (или) их фактические аргументы.

Ключевые слова: симметричные итерационные юлочные шифры; дополнительные ключи; функциональные ключим; SIBCiphers; Люцифер-SIBCiphers; Фейстель-SIBCiphers.

SIBCIPHERS – SYMMETRIC ITERATIVE BLOCK CIPHERS WITH FUNCTIONAL KEYS

G. P. Agibalov

Tomsk State University
Tomsk, Russia

A class of symmetric iterative block ciphers called SIBCiphers is defined. Each round of a cipher in this class is represented by an injective system of Boolean functions each depending on a small number of arguments being some inputs to the round. Round key in it includes some of these functions and (or) their actual arguments. The ciphertext bitstring is obtained by permuting the bits on the outputs of the last round. Contemporary symmetric block ciphers with additive round keys belong to this class. Two other subclasses of SIBCiphers are described. They are called by names Lucifer and Feistel and constructed according to the known cryptographic schemes originally suggested by H. Feistel and implemented in ciphers LUCIFER and DES respectively. Some synthesis problems for SIBCiphers are discussed.

Keywords: symmetric iterative block ciphers; additive keys; functional keys; SIBCiphers; Lucifer SIBCiphers; Feistel SIBCiphers.

INTRODUCTION

With the insignificant exception (LUCIFER [1] for example), the most contemporary symmetric iterative block ciphers are characterized by the following properties:

1) round functions of a cipher are some superpositions of elementary logical operations such as negation, conjunction, disjunction, modulo addition, cyclic shift, permutation and so

on as well as substitutions being some little and fixed systems of Boolean functions in a small number of variables;

2) round keys are additive, that is, they are only used as the operands for an addition operation (similar to $key \oplus x$ or $key + x \bmod m$).

Because of these properties, the ciphers are susceptible to algebraic attacks based on solving systems of equations connecting symbols in keys with the symbols in plain and encrypted texts [2, 3], to differential cryptanalysis [4, 5], and to attacks on the basis of statistical analogues [6], particularly to linear cryptanalysis [7, 8].

At the beginning of his scientific career (the first half of 1960s), the author of this article researched symmetric stream ciphers with filter keystream generators, where a filter Boolean function essentially depends on a small number of variables that are components of a generator state and together with these components and, possibly, with the numbers of them form the key of the cipher [9]. The cryptanalysis results for this cipher have been published in [10–13]. The problem that has been solved consists in the following: given a piece of the keystream, determine the essential arguments of filter function and its values for all values of these arguments. The problem is not reduced to solving a system of equations, to differential cryptanalysis, and to attacks on the basis of statistical analogues.

In [14], the watermarking ciphers are defined. They protect both the confidentiality and the usage legality of information. Some examples of stream watermarking ciphers with functions playing the role of a key are given in [14].

The idea to use sets of Boolean functions in a small number of variables and their actual arguments as round keys in symmetric iterative block ciphers has been offered in [15], where such ciphers are called SIBCiphers (from Symmetric Iterative Block Ciphers). Here after correcting detected misprints in [15], an English version of the paper [15] is presented.

Below we define the general scheme of a SIBCipher, classify such ciphers and describe two subclasses of them generalizing the known cryptographic algorithms LUCIFER and DES [1] suggested by H. Feistel, and, at last, formulate some problems concerning the synthesis of SIBCiphers.

GENERAL SCHEME OF SIBCIPHER

Everywhere below, for any string $x = x_1x_2 \ldots x_m$ and $t = 1, \ldots, m$, it is supposed that $x[t] = x_t$.

Generally, in the scheme of a r-round SIBCipher C with the information blocks of length n, the l-th round, $l = 1, 2, \ldots, r$, is described by a system of n Boolean functions $g_1^{(l)}$, $g_2^{(l)}$, …, $g_n^{(l)}$ each depending on a k variables, $k \le n$, and by n mappings $\eta_i^{(l)}: \{1, 2, \ldots, k\} \rightarrow \{1, 2, \ldots, n\}$, $i = 1, 2, \ldots, n$, with the surjectivity property, that is, for any $m \in \{1, 2, \ldots, n\}$, the equality $m = \eta_i^{(l)}(j)$ holds for some $i \in \{1, 2, \ldots, n\}$ and $j \in \{1, 2, \ldots, k\}$, such that the mapping $g^{(l)}: \{0, 1\}^n \rightarrow \{0, 1\}^n$, where $g^{(l)}(u) = g_1^{(l)}(v_1)\, g_2^{(l)}(v_2) \ \ldots\ g_n^{(l)}(v_n)$ for any $u = u_1u_2 \ldots u_n \in \{0, 1\}^n$ and $v_i = u[\eta_i^{(l)}(1)]\, u[\eta_i^{(l)}(2)] \ldots u[\eta_i^{(l)}(k)]$, $i = 1, 2, \ldots, n$, is injective. For the function $g_i^{(l)}$ here, $\eta_i^{(l)}(1), \ldots, \eta_i^{(l)}(k)$ are the numbers of its actual arguments taken from the members $u_1, u_2, \ldots, u_n$ of an information block u given on the inputs of l-th round. So, $g_i^{(l)}$ is a function in variables $u[i_1], u[i_2], \ldots, u[i_k]$ if $\eta_i^{(l)}(j) = i_j$, $j = 1, 2, \ldots, k$. The result of transformation of u by l-th round is the information block $g^{(l)}(u)$ on the outputs of this round. The inverse transformation of $g^{(l)}(u)$ into u is possible because of injectiveness of $g^{(l)}$.

By the definition, the mapping $\mathrm{g}^{(l)}$ is the l-th round function of the SIBCipher C, and Boolean functions $g_i^{(l)}$ are its components also called the l-th round component functions of C.

For every $l = 2, 3, \ldots, r$, an information block on inputs of l-th round coincides with the information block on outputs on $(l - 1)$-th round. It is also supposed that in the general scheme of a SIBCipher there is a permutation h: $\{0, 1\}^n \to \{0, 1\}^n$ defined as $h(u_1u_2 \ldots u_n) = =u[i_1]\, u[i_2] \ldots u[i_n]$ for a substitution η: $\{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$, where $\eta(j) = i_j$, $j = 1, 2, \ldots, n$. The permutation h is applied for permuting symbols of information block on outputs of the last (r-th) round.

Thus, in the SIBCipher C, a plain text $x \in \{0, 1\}^n$ is encrypted into a cipher text $y \in \{0, 1\}^n$ computed as $y = hg^{(r)}g^{(r-1)} \ldots g^{(1)}(x)$, which in turn is decrypted into the plain text x computed as $x = (g^{(1)})^{-1} \ldots (g^{(r-1)})^{-1} (g^{(r)})^{-1} h^{-1}(y)$.

Here and everywhere below, for any mappings $f_1, f_2, \ldots, f_m$, the expression $f_1f_2 \ldots f_m(a)$ means $f_1(f_2(\ldots(f_m(a))\ldots))$.

Evidently, if some mappings $h^{(l)}$: $\{0, 1\}^n \to \{0, 1\}^{kn}$ and $G^{(l)}$: $\{0, 1\}^{kn} \to \{0, 1\}^n$ are defined (in the above notation) as $h^{(l)}(u) = v_1v_2 \ldots v_n$ and $G^{(l)}(v_1v_2 \ldots v_n) = g_1^{(l)}(v_1)\, g_2^{(l)}(v_2) \ldots g_n^{(l)}(v_n)$, then $G^{(l)}(h^{(l)}(u)) = g^{(l)}(u)$ and the encryption in a SIBCipher can be represented as a «flaky pie», where mappings $h^{(l)}$ and $G^{(l)}$ alternate and the plain text x is encrypted into the cipher text $y = hG^{(r)}h^{(r)}G^{(r-1)}h^{(r-1)} \ldots G^{(1)}h^{(1)}(x)$.

According to their destination, the round component functions $g_i^{(l)}$ and the connecting them mappings $\eta_i^{(l)}$, η in the SIBCipher C are called, respectively, *functional* and *connecting components* of the cipher C. It is supposed that the key of the SIBCipher C is defined as a subset of its functional and (or) connecting components. Thus, any specific SIBCipher is uniquely determined by its own parameters n, k, r, components (functional and connecting) and a subset of last ones as a key.

SOME SUBCLASSES OF SIBCIPHERS

Different subclasses of SIBCiphers are defined by setting some limitations on the assortment of components in them and on selection of key components. One such subclass consists of SIBCiphers with fixed connecting components and variable functional components playing all together the key role. The other subclass, on the contrary, contains SIBCiphers with the fixed and, possibly, identical functional components and with the variable (key) connecting components. The third subclass consists of SIBCiphers with each round key including simultaneously some functions used in the round and their actual arguments. This is the case when the cryptanalysis of a SIBCipher with the threat of discovering its key implies the determination of both key functions and their essential variables. We don't know how the methods in [10–13] solving the last problem may be applied in this case.

The set of all symmetric iterative block ciphers with additive round keys is, in fact, a subclass of SIBCiphers. Indeed, adding a key and an argument of a function replaces the latter by another function as follows: $f(\boldsymbol{k} + x) = g_{\boldsymbol{k}}(x)$. Thus, a cipher with the additive round key $\boldsymbol{k}$ is equivalent to a SIBCipher with the functional key $g_{\boldsymbol{k}}$. For instance, DES can be considered as a SIBcipher, where each round key consists of 32 Boolean functions implemented by S-boxes and each depending on 6 variables. As a matter of fact, the use of an additive key is a specific way to select a function from a set, and thus to put a certain functional round key. In particular, this means that the cryptanalysis of SIBCiphers may result in new methods for cryptanalysis of traditional symmetric block ciphers with additive round keys.

FEISTEL SIBCIPHERS

In a Feistel SIBCipher, an information block $u \in \{0, 1\}^n$ has an even length n and is represented by the concatenation of its left and right halves of length $n/2$. For $u = L_0R_0$ and L_0, $R_0 \in \{0, 1\}^{n/2}$, in l-th round of the cipher $g^{(l)}(u) = L_1R_1$, where $L_1 = R_0$ and $R_1[i] = L_0[\eta_i^{(l)}(1)] \oplus f_i^{(l)}(R_0[\eta_{n/2+i}^{(l)}(1)], ..., R_0[\eta_{n/2+i}^{(l)}(k-1)])$ for some Boolean functions $f_i^{(l)}: \{0, 1\}^{k-1} \to \{0, 1\}$ and for some surjective systems of mappings $\eta_i^{(l)}: \{1\} \to \{1, 2, \ldots, n/2\}$ and $\eta_{n/2+i}^{(l)}: \{1, 2, \ldots, k-1\} \to \{1, 2, \ldots, n/2\}$, $i = 1, 2, \ldots, n/2$. The inverse transformation of L_1R_1 into $u = L_0R_0$ is made according to the equalities: $L_0[\eta_i^{(l)}(1)] = R_1[i] \oplus f_i^{(l)}(L_1[\eta_{n/2+i}^{(l)}(1)], ..., L_1[\eta_{n/2+i}^{(l)}(k-1)])$, $i = 1, 2, \ldots, n/2$, and $R_0 = L_1$.

It is immediately verified that $g^{(l)}(u) = g^{(l)}(L_0R_0) = g_1^{(l)}(v_1)\, g_2^{(l)}(v_2) \ldots g_n^{(l)}(v_n)$, where $g_1^{(l)}(v_1) \ldots g_{n/2}^{(l)}(v_{n/2}) = v_1 \ldots v_{n/2} = R_0$, $v_{n/2+i} = L_0[\eta_i^{(l)}(1)]R_0[\eta_{n/2+i}^{(l)}(1)] \ldots R_0[\eta_{n/2+i}^{(l)}(k-1)]$, $g_{n/2+i}^{(l)}(v_{n/2+i}) = L_0[\eta_i^{(l)}(1)] \oplus f_i^{(l)}(R_0[\eta_{n/2+i}^{(l)}(1)], ..., R_0[\eta_{n/2+i}^{(l)}(k-1)]) = R_1[i]$, $i = 1, \ldots, n/2$. Thus, the cipher just described is really a SIBCipher. The round equations in this SIBCipher looks like the round equations in the Feistel's cryptographic scheme. Therefore, we call it Feistel SIBCipher.

LUCIFER SIBCIPHERS

A SIBCipher of the subclass Lucifer is characterized by the following properties: (a) $n = ks$, $s > 1$; (b) for any pair (l, t), $l = 1, 2, \ldots, r$ and $t = 1, 2, \ldots, s$, the mapping $G_t^{(l)}: \{0, 1\}^k \to \{0, 1\}^k$ defined as $G_t^{(l)}(z) = g_{(t-1)k+1}^{(l)}(z)\, g_{(t-1)k+2}^{(l)}(z) \ldots g_{tk}^{(l)}(z)$ for all $z \in \{0, 1\}^k$, is a substitution; (c) $\eta_{(t-1)k+1}^{(l)} = \eta_{(t-1)k+2}^{(l)} = \ldots = \eta_{tk}^{(l)}$, that is, all the functions $g_{(t-1)k+j}^{(l)}$, $j = 1,2, ..., k$, depend on the same set of arguments; and (d) the values $\eta_{tk}^{(l)}(j)$ for all $j = 1, 2, \ldots, k$ and $t = 1, 2, \ldots, s$ are distinct, therefore the mapping $\eta^{(l)}: \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$, where $\eta^{(l)}((t-1)k + j)) = \eta_{tk}^{(l)}(j)$ for all $j = 1, 2, \ldots, k$ and $t = 1, 2, \ldots, s$, is a substitution, and the mapping $h^{(l)}: \{0, 1\}^n \to \{0, 1\}^n$, where $h^{(l)}(u) = h_1^{(l)}(u) h_2^{(l)}(u) \ldots h_s^{(l)}(u)$ and $h_t^{(l)}(u) = u[\eta_{tk}^{(l)}(1)]\, u[\eta_{tk}^{(l)}(2)] \ldots u[\eta_{tk}^{(l)}(k)]$ for $u \in \{0, 1\}^n$ and $t = 1, 2, \ldots, s$, is a permutation.

In other words, all Boolean functions in l-th round and their arguments $u_1, u_2, \ldots, u_n$ in an information block $u = u_1u_2 \ldots u_n$ on the inputs of the round are devided into s subsets $F_t^{(l)} = \{ g_{(t-1)k+j}^{(l)} : j = 1, 2, \ldots, k\}$ and $Z_t^{(l)} = \{u[\eta_{tk}^{(l)}(j)] : j = 1, 2, \ldots, k\}$, respectively, each of cardinality k such that arguments in $Z_t^{(l)}$ and they only are the arguments for any function in $F_t^{(l)}$ and the functions in $F_t^{(l)}$ are the coordinate functions of the substitution $G_t^{(l)}$, $t = 1, 2, \ldots, s$. Thus, $g^{(l)}(u) = G_1^{(l)}(u[\eta_k^{(l)}(1)]\, u[\eta_k^{(l)}(2)] \ldots u[\eta_k^{(l)}(k)])\; G_2^{(l)}(u[\eta_{2k}^{(l)}(1)]\, u[\eta_{2k}^{(l)}(2)] \ldots u[\eta_{2k}^{(l)}(k)]) \ldots G_s^{(l)}(u[\eta_{sk}^{(l)}(1)]\, u[\eta_{sk}^{(l)}(2)] \ldots u[\eta_{sk}^{(l)}(k)])$, the substitutions $G_1^{(l)}, \ldots, G_s^{(l)}$ here play the role of invertible S-boxes, and s is the number of them in each round of the cipher.

If the mapping $E^{(l)}: \{0, 1\}^n \to \{0, 1\}^n$ is defined as $E^{(l)}(u_1u_2 \ldots u_n) = G_1^{(l)}(u_1 \ldots u_k)\, G_2^{(l)}(u_{k+1} \ldots u_{2k}) \ldots G_s^{(l)}(u_{(s-1)k+1} \ldots u_{sk})$, then the encryption and the decryption in this SIBCipher can be made in the following ways: $y = hE^{(r)}h^{(r)}E^{(r-1)}h^{(r-1)} \ldots E^{(1)}h^{(1)}(x)$ and $x = (h^{(1)})^{-1} (E^{(1)})^{-1} \ldots (h^{(r-1)})^{-1} (E^{(r-1)})^{-1} (h^{(r)})^{-1} (E^{(r)})^{-1} h^{-1}(y)$ respectively.

As in the general scheme of SIBCipher, the key in the last SIBCipher may contain any its components $g_i^{(l)}$, $\eta_i^{(l)}$ and η. It can also be put by a subset of mappings $G_t^{(l)}$, $h_t^{(l)}$ and *h*.

In particular, if for all $t = 1, 2, \ldots, s$ and $l = 1, 2, \ldots, r$, the substitutions $G_t^{(l)}$ are taken from two possible ones, say S_0 and S_1, and the SIBCipher key only consists of all of them, then the SIBCipher is the cipher known as LUCIFER [1]. That is why we call the subclass of these SIBCiphers by this name.

SYNTHESIS PROBLEMS FOR SIBCIPHERS

There are at least two problems in the synthesis of SIBCiphers according to the general scheme: 1) generating systems of functional components $g_i^{(l)}$ in a small number of variables such that the round mappings $g^{(l)}$ are injective and 2) selecting a key subset of functional and (or) connecting components having a real key length and providing a needed resistance of the cipher to the possible methods of cryptanalysis. Besides, for preventing attacks exploiting cryptographic weaknesses of Boolean functions, the functional components in SIBCiphers should be balanced and of high correlation immunity, nonlinearity, avalanche criterion, etc. [16–18].

The application of additive round keys is only one of approaches to solving the second problem but it narrows the class of ciphers under consideration. The constructions of Feistel and Lucifer SIBCiphers demonstrate two other approaches to solving this problem.

LITERATURE

1. Hoffman L. J. Modern Methods for Computer Security and Privacy. Prentice Hall Inc., Englewood Cliffs, New Jersey, 1977.

2. Агибалов Г. П. Методы решения систем полиномиальных уравнений над конечным полем // Вестн. Томск. гос. ун-та. Приложение. Август 2006. № 17. С. 4–9.

3. Courtois N., Pieprzyk J. Cryptanalysis of Block Ciphers with Overdefined Systems of Equations // ASIACRYPT 2002, LNCS 2501, 2002, P. 267–287.

4. Biham E., Shamir A. Differential Cryptanalysis of DES-like Cryptosystems / Technical Report. The Weizmann Institute of Science. Department of Applied Mathematics: 1990 // J. Cryptology, 1991. Vol. 4. № 1. P. 3–72.

5. Агибалов Г. П. Элементы теории дифференциального криптоанализа итеративных блочных шифров с аддитивным раундовым ключом // Прикладная дискретная математика. 2008. № 1(1). С. 34–42.

6. Агибалов Г. П., Панкратова И. А. Статистические аналоги дискретных функций и их применение в криптоанализе симметричных шифров // Прикладная дискретная математика. 2010. № 3(9). С. 51–68.

7. Matsui M. Linear Cryptanalysis Method for DES Cipher // LNCS, 1993. Vol. 765. P. 386–397.

8. Matsui M. The First Experimental Cryptanalysis of the Data Encryption Standard // LNCS. 1994. Vol. 839. P. 1–11.

9. Агибалов Г. П. Распознавание операторов, реализуемых в автономных автоматах // Конференция по теории автоматов и искусственному мышлению. Ташкент, 27–31 мая 1968 г. Аннотации докладов и программа. М. : ВЦ АН СССР, 1968. С. 7–8.

10. Агибалов Г. П., Левашников А. А. Статистическое исследование задачи опознания булевых функций одного класса // Всесоюз. коллоквиум по автоматизации синтеза дискретных вычислительных устройств. Тез. докл. 20–25 сентября 1966 г. Новосибирск, 1966. С. 40–45.

11. Агибалов Г. П. Минимизация числа аргументов булевых функций // Проблемы синтеза цифровых автоматов. М. : Наука, 1967. С. 96–100.

12. Агибалов Г. П. О некоторых доопределениях частичной булевой функции // Тр. Сибирского физ.-техн. ин-та. Проблемы кибернетики. 1970. Вып. 49. С. 12–19.

13. Агибалов Г. П., Сунгурова О. Г. Криптоанализ конечно-автоматного генератора ключевого потока с функцией выходов в качестве ключа // Вест. Томск. гос. ун-та. Приложение. Август 2006. № 17. С. 104–108.

14. Agibalov G. P. Watermarking ciphers // Прикладная дискретная математика. 2016. № 1 (31). С. 62–66.

15. Агибалов Г. П. SIBCiphers — симметричные итеративные блочные шифры из булевых функций с ключевыми аргументами // Прикладная дискретная математика. Приложение. 2014. № 7. С. 43–48.

16. Токарева В. Н. Симметричная криптография. Краткий курс : учеб. пособие. Новосибирск : Новосиб. гос. ун-т, 2012.

17. Логачев О. А., Сальников А. А., Смышляев С. В., Ященко В. В. Булевы функции в теории кодирования и криптографии. 2-е изд. М. : МЦНМО, 2012.

18. Панкратова И. А. Булевы функции в криптографии : учеб. пособие. Томск : Том. гос. ун-т, 2014.