б) если $\lambda_1 > 1$ и $r = 2$, то

$$\exp(H^\delta + H^\tau) \leqslant \lambda_1\lambda_2 - 2\lambda_1 - \lambda_2 + 2n;$$

в) если $\lambda_1 = 1$ и μ — наибольшее число, делящее τ, среди чисел $l_1, \ldots, l_m$, то

$$\exp(H^\delta + H^\tau) \leqslant 2n - 1 - \mu.$$

Оценки пп. 3*б* и 3*в* получены с использованием оценок соответственно [3, с. 104] и [4, с. 408].

Следствие 1. Если выполнены условия п. 3*а* теоремы, то

$$\exp(H^\delta + H^\tau) \leqslant \lambda_1\lambda_r - \lambda_1 - \lambda_r + n(r+1) - \sum_{i=1}^{r} \lambda_i.$$

Следствие вытекает из оценки числа Фробениуса [5, теорема 3.1.1] $g(\lambda_1, \ldots, \lambda_r) \leqslant$ $\leqslant \lambda_1\lambda_r - \lambda_1 - \lambda_r$, $r > 1$.

Данные оценки могут быть уточнены для частных классов перемешивающих матриц H базового преобразования генератора (δ, τ)-самоусечения.

ЛИТЕРАТУРА

1. *Rueppel R. A.* When shift registers clock themselves // Advances in Cryptology — Eurocrypt'87. LNCS. 1988. V. 304. P. 53–64.
2. *Фомичев В. М.* Методы дискретной математики в криптологии. М.: Диалог-МИФИ, 2010. 424 с.
3. *Фомичев В. М.* Оценки экспонентов примитивных графов // Прикладная дискретная математика. 2011. № 2(12). С. 101–112.
4. *Сачков В. Н., Тараканов В. Е.* Комбинаторика неотрицательных матриц. М.: ТВП, 2000. 448 с.
5. *Alfonsin J. R.* The Diophantine Frobenius Problem. Oxford University Press, 2005.

УДК 519.113.6

SIBCiphers — СИММЕТРИЧНЫЕ ИТЕРАТИВНЫЕ БЛОЧНЫЕ ШИФРЫ ИЗ БУЛЕВЫХ ФУНКЦИЙ С КЛЮЧЕВЫМИ АРГУМЕНТАМИ

Г. П. Агибалов

Вводится в рассмотрение класс SIBCipher многораундовых симметричных блочных шифров, в которых каждый раунд представлен инъективной системой булевых функций, зависящих существенно от ограниченного числа аргументов из информационного блока на входе раунда, и в которых раундовый ключ является подмножеством этих функций и (или) наборов их существенных аргументов. Современные симметричные блочные шифры с аддитивным раундовым ключом принадлежат этому классу. Описываются два других семейства шифров в классе SIBCipher — Фейстеля и Люцифер, построенных по известным одноимённым криптографическим схемам.

Ключевые слова: *криптография, булевы функции, симметричные итеративные блочные шифры, сеть Фейстеля, шифр Люцифер.*

Введение

За малым исключением (Люцифер [1] и т. п.), большинство современных симметричных итеративных блочных шифров характеризуются следующими свойствами:

1) функция каждого раунда шифра является суперпозицией элементарных логических операций, таких, как отрицание, конъюнкция, дизъюнкция, сложение по модулю (2 или более), циклические сдвиги, перестановки и т. п., а также блоков замен — небольших фиксированных систем булевых функций от малого числа переменных;
2) ключ каждого раунда шифра аддитивный — входит в суперпозицию с другими операндами, в том числе и с аргументами булевых функций, посредством операции сложения (например, как $k \oplus x$ или $(k + x) \bmod m$).

Благодаря этим свойствам, такие шифры поддаются (хотя и не всегда просто) алгебраическим атакам (на основе решения систем уравнений, связывающих символы ключа с символами открытых и шифрованных текстов) [2, 3], дифференциальному криптоанализу [4, 5] и атакам на основе статистических аналогов [6], в частности линейному криптоанализу [7, 8].

Когда-то, на заре своей научной карьеры (первая половина 60-х годов XX века), автор настоящей работы предложил, говоря современным языком, симметричный поточный шифр с фильтрующим генератором ключевого потока, в котором булева фильтрующая функция существенно зависит от ограниченного числа аргументов — компонент состояния генератора — и вместе с номерами этих аргументов образует ключ шифра [9]. Криптоанализ этого шифра породил ряд публикаций [10 – 13]. Он заключается в определении по отрезку ключевого потока существенных аргументов фильтрующей функции и её значений на наборах значений этих аргументов и, похоже, не сводится к решению системы уравнений, дифференциальному криптоанализу и атаке на основе статистических аналогов.

В данной работе эта идея использования в качестве ключа шифра не набора символов с аддитивным вхождением в алгоритм шифрования, а набора его функциональных компонент — булевых функций вместе с ограниченным числом их существенных аргументов — реализуется в симметричных итеративных блочных шифрах. Для краткости предлагаемые шифры называются SIBCiphers — от Symmetric Iterative Block Ciphers. Ниже даётся их общая схема построения, указывается их некоторая классификация по семействам и описываются два их семейства: SIBCiphers, построенные по схеме Фейстеля, и SIBCiphers, построенные по схеме шифра Люцифер.

1. Общая схема шифра SIBCipher

В общей схеме r-раундового шифра SIBCipher с длиной информационного блока n раунд с номером $l = 1, 2, \ldots, r$ представляет собой систему из n булевых функций $g_1^{(l)}$, $g_2^{(l)}$, $\ldots$, $g_n^{(l)}$ от $k \leqslant n$ переменных каждая и систему из n отображений $\eta_i^{(l)} : \{1, 2, \ldots, k\} \to \{1, 2, \ldots, n\}$, $i = 1, 2, \ldots, n$, обладающую свойством сюръективности: для любого $m \in \{1, 2, \ldots, n\}$ имеет место $m = \eta_i^{(l)}(j)$ для некоторых $i \in \{1, 2, \ldots, n\}$ и $j \in \{1, 2, \ldots, k\}$, и такую, что инъективно отображение $g^{(l)} : \{0, 1\}^n \to \to \{0, 1\}^n$, где $g^{(l)}(u) = g_1^{(l)}(v_1) g_2^{(l)}(v_2) \ldots g_n^{(l)}(v_n)$ для любого $u = u_1 u_2 \ldots u_n \in \{0, 1\}^n$ и $v_i = u_{\eta_i^{(l)}(1)} u_{\eta_i^{(l)}(2)} \ldots u_{\eta_i^{(l)}(k)}$ для $i = 1, 2, \ldots, n$. Для функции $g_i^{(l)}$ здесь $\eta_i^{(l)}(1)$, $\ldots$, $\eta_i^{(l)}(k)$ суть номера её существенных аргументов из ряда членов $u_1, u_2, \ldots, u_n$ информационного блока u, заданного на входах l-го раунда. Результатом преобразования l-м раундом

блока u является информационный блок $g^{(l)}(u)$ на выходах этого раунда. Его обратное преобразование в u возможно ввиду инъективности $g^{(l)}$.

Для каждого $l = 2, 3, \ldots, r$ информационный блок на входе l-го раунда шифра совпадает с информационным блоком на выходе его $(l-1)$-го раунда.

Общая схема шифра SIBCipher предполагает также наличие перестановки $h : \{0,1\}^n \to \{0,1\}^n$, определяемой как $h(u_1 u_2 \ldots u_n) = u_{i_1} u_{i_2} \ldots u_{i_n}$ для некоторой подстановки $\eta : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$, где $\eta(j) = i_j$, $j = 1, 2, \ldots, n$. В шифровании она применяется для перестановки символов информационного блока на выходе r-го раунда.

Если определить отображение $h^{(l)} : \{0,1\}^n \to \{0,1\}^{kn}$ как $h^{(l)}(u) = v_1 v_2 \ldots v_n$ и отображение $G^{(l)} : \{0,1\}^{kn} \to \{0,1\}^n$ как $G^{(l)}(v_1 v_2 \ldots v_n) = g_1^{(l)}(v_1) g_2^{(l)}(v_2) \ldots g_n^{(l)}(v_n)$, то шифрование в SIBCipher можно представить как «слоёный пирог», в котором отображения $h^{(l)}$ чередуются с отображениями $G^{(l)}$, преобразуя блок открытого текста x в блок шифртекста y по правилу $y = hG^{(r)}h^{(r)}G^{(r-1)}h^{(r-1)} \ldots G^{(1)}h^{(1)}(x)$, а расшифрование y в x — по правилу $x = {g^{(1)}}^{-1} \ldots {g^{(r-1)}}^{-1} {g^{(r)}}^{-1} h^{-1}(y)$. Здесь и далее в подобных выражениях для любых отображений f_1, f_2, …, f_m под $f_1 f_2 \ldots f_m(a)$ подразумевается $f_1(f_2(\ldots(f_m(a))\ldots))$.

В соответствии с предназначением, булевы функции $g_i^{(l)}$ называются далее функциональными компонентами, а связывающие их отображения $\eta_i^{(l)}$ и η — соединительными компонентами шифра SIBCipher. Предполагается, что ключ шифра задаётся как подмножество из некоторых его соединительных и (или) функциональных компонент. Таким образом, любой конкретный SIBCipher однозначно определяется своими числовыми параметрами — n, r, k, своими компонентами (соединительными и функциональными) и своим ключом — подмножеством последних.

2. Возможные семейства шифров SIBCipher

Разные семейства шифров SIBCipher получаются путём наложения ограничений на определение входящих в них компонент и на выбор тех из них, которые образуют ключ шифра. Одно такое семейство состоит из шифров с фиксированными соединительными компонентами и с ключевыми функциональными компонентами. Другое, наоборот, содержит шифры с фиксированными (и, возможно, одинаковыми) функциональными компонентами, но с изменяемыми соединительными компонентами, совокупно выбираемыми в качестве ключа. Самое широкое семейство рассматриваемых шифров достигается, когда одновременно соединительные и функциональные компоненты (все или некоторые) образуют ключ шифра. Это именно тот случай, когда криптоанализ шифра с угрозой полного его раскрытия сводится к нахождению существенных аргументов функциональных компонент и значений последних на наборах значений этих аргументов. Насколько применимы для решения этой задачи алгоритмы из [10 – 13], вопрос открытый, даже при малом количестве раундов шифра.

Для предотвращения других атак, эксплуатирующих криптографические слабости булевых функций, для построения функциональных компонент в шифрах класса SIBCipher естественно рекомендовать булевы функции с высокими корреляционной и алгебраической иммунностью, нелинейностью, степенью критерия распространения и т. п. [14, 15].

Что касается симметричных итеративных блочных шифров с аддитивным раундовым ключом, то они ведь тоже образуют семейство в классе шифров SIBCipher, поскольку прибавление к аргументам булевой функции (из блока замены) символов

закрытого ключа изменяет её на неизвестную функцию и таким образом придаёт ей свойство ключа. По существу, такое применение аддитивного ключа — это такой способ выбора конкретной функции из множества возможных. Сие означает, в частности, что криптоанализ шифров из класса SIBCipher может привести к созданию новых методов криптоанализа традиционных симметричных блочных шифров с аддитивным раундовым ключом.

Есть, по крайней мере, две проблемы в построении конкретного SIBCipher: выбор компонент, гарантирующих инъективность раундовых отображений $g^{(l)}$, и выбор ключевого подмножества компонент с реальной длиной ключа — разумеется, с обеспечением требуемой стойкости шифра к криптоанализу. Собственно, применение аддитивного ключа — это только один из подходов к решению второй проблемы, но он значительно сужает класс рассматриваемых шифров. Ниже показывается, как первая проблема решается в SIBCiphers из семейств Фейстеля и Люцифер.

3. SIBCiphers семейства Фейстеля

Так мы называем шифры класса SIBCipher, в которых n чётное и информационные блоки на входе и выходе l-го раунда шифра представляются конкатенациями своих левой и правой половинок длиной $n/2$ — L_0R_0 и L_1R_1 соответственно и связаны между собой соотношениями $L_1 = R_0$ и $R_1 = p^{(l)}(L_0) \oplus g^{(l)}(R_0)$, где $p : \{0,1\}^{n/2} \to \{0,1\}^{n/2}$ — перестановка и, аналогично общей схеме (но без требования инъективности), $g^{(l)} : \{0,1\}^{n/2} \to \{0,1\}^{n/2}$, $g^{(l)}(u) = g_1^{(l)}(v_1)g_2^{(l)}(v_2)\dots g_{n/2}^{(l)}(v_{n/2})$ для любого $u = u_1u_2\dots u_{n/2} \in \{0,1\}^{n/2}$ и $v_i = u_{\eta_i^{(l)}(1)}u_{\eta_i^{(l)}(2)}\dots u_{\eta_i^{(l)}(k)}$ для сюръективной системы отображений $\eta_i^{(l)} : \{1,2,\dots,k\} \to \{1,2,\dots,n/2\}$, $i = 1,2,\dots,n/2$. Обратное преобразование L_1R_1 в L_0R_0 выполняется по правилу $L_0 = p^{(l)-1}(R_1 \oplus g^{(l)}(L_1))$, $R_0 = L_1$.

Осведомлённый читатель сразу же заметит, что уравнения раунда здесь по форме близки к уравнениям Фейстеля в раунде DES, поэтому можно говорить, что сами шифры здесь построены действительно по схеме Фейстеля. Кроме того, внимательный читатель сможет без труда формально доказать, что эти шифры действительно образуют семейство шифров класса SIBCipher.

4. SIBCiphers семейства Люцифер

В шифре этого семейства предполагается: 1) $n = ks$ для некоторого $s > 1$; 2) для каждой пары (l,i), где $l = 1,2,\dots,r$ и $i = 1,2,\dots,s$, отображение $G_i^{(l)} : \{0,1\}^k \to \{0,1\}^k$, где $G_i^{(l)}(z) = g_{(i-1)k+1}^{(l)}(z)g_{(i-1)k+2}^{(l)}(z)\dots g_{ik}^{(l)}(z)$ для всех $z \in \{0,1\}^k$, есть подстановка на $\{0,1\}^k$; 3) все функции $g_{(i-1)k+j}^{(l)}$, $j = 1,2,\dots,k$, зависят от одного и того же набора аргументов в информационном блоке на входе l-го раунда, т. е. $\eta_{(i-1)k+1}^{(l)} = \eta_{(i-1)k+2}^{(l)} = \dots = \eta_{ik}^{(l)}$; 4) отображение $p^{(l)} : \{0,1\}^n \to \{0,1\}^n$, где $p^{(l)}(u) = p_1^{(l)}(u)p_2^{(l)}(u)\dots p_s^{(l)}(u)$ и $p_i^{(l)}(u) = u_{\eta_{ik}^{(l)}(1)}u_{\eta_{ik}^{(l)}(2)}\dots u_{\eta_{ik}^{(l)}(k)}$ для $p_i^{(l)} : \{0,1\}^n \to \{0,1\}^k$ и $i = 1,2,\dots,s$, есть перестановка.

Иначе говоря, все булевы функции раунда шифра разбиты на s подсистем $F_i^{(l)}$ по k функций в каждой, а их аргументы в информационном блоке — на s наборов $z_i^{(l)}$ по k аргументов в каждом так, что аргументы в наборе $z_i^{(l)}$ служат аргументами всех функций в подсистеме $F_i^{(l)}$, и функции в последней являются координатными функциями подстановки $G_i^{(l)}$, $i = 1,2,\dots,s$. Таким образом, подстановки $G_1^{(l)}, \dots, G_s^{(l)}$ здесь выступают в роли обратимых блоков замены и s — их количество в одном раунде шифра.

Если определить отображение $E^{(l)} : \{0,1\}^n \to \{0,1\}^n$ как

$$E^{(l)}(u_1u_2\dots u_n) = G_1^{(l)}(u_1\dots u_k)G_2^{(l)}(u_{k+1}\dots u_{2k})\dots G_s^{(l)}(u_{(s-1)k+1}\dots u_{sk}),$$

то шифрование и расшифрование в таком SIBCipher можно выполнить по правилам $y = hE^{(r)}p^{(r)}E^{(r-1)}p^{(r-1)}\dots E^{(1)}p^{(1)}(x)$ и $x = {p^{(1)}}^{-1}{E^{(1)}}^{-1}\dots {E^{(r-1)}}^{-1}{p^{(r)}}^{-1}{E^{(r)}}^{-1}h^{-1}(y)$ соответственно.

В состав ключа этого шифра, как и шифра по общей схеме, могут входить любые его компоненты $g_i^{(l)}$, $\eta_i^{(l)}$ и η. Его можно задать и подмножеством отображений $G_i^{(l)}$, $f_i^{(l)}$ и h. В частности, если в данном шифре перестановка f_1 тождественная, перестановки f_2, …, f_r, h фиксированные, а ключ образуется только из подстановок $G_i^{(l)}$, то получается шифр, известный по имени Люцифер [1]. Именно поэтому описанные в этом разделе шифры SIBCiphers и отнесены к семейству под этим именем.

ЛИТЕРАТУРА

1. *Хоффман Л. Дж.* Современные методы защиты информации. М.: Сов. радио, 1980. 264 с.
2. *Агибалов Г. П.* Методы решения систем полиномиальных уравнений над конечным полем // Вестник Томского государственного университета. Приложение. Август 2006. № 17. С. 4–9.
3. *Courtois N. and Pieprzyk J.* Cryptanalysis of block ciphers with overdefined systems of equations // ASIACRYPT 2002. LNCS. 2002. V. 2501. P. 267–287.
4. *Biham E. and Shamir A.* Differential cryptanalysis of DES-like cryptosystems // J. Cryptology. 1991. No. 4. P. 3–72.
5. *Агибалов Г. П.* Элементы теории дифференциального криптоанализа итеративных блочных шифров с аддитивным раундовым ключом // Прикладная дискретная математика. 2008. № 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. V. 765. P. 386–397.
8. *Matsui M.* The first experimental cryptanalysis of the Data Encryption Standard // LNCS. 1994. V. 839. P. 1–11.
9. *Агибалов Г. П.* Распознавание операторов, реализуемых в автономных автоматах // Конф. по теории автоматов и искусственному мышлению. Ташкент, 27–31 мая 1968. 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 // Тез. докл. к Всесоюзному коллоквиуму по автоматизации синтеза дискретных вычислительных устройств, 20–25 сентября 1966. 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 // Труды Сибирского физико-технического института. 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 // Вестник Томского государственного университета. Приложение. Август 2006. № 17. С. 104–108.
14. Введение в криптографию / под ред. В. В. Ященко. М.: МЦНМО, «ЧеРо», 1998. 272 с.

15. *Панкратова И. А.* Булевы функции в криптографии: учеб. пособие. Томск: Издательский Дом Томского государственного университета, 2014. 88 с.

УДК 519.24

АСИМПТОТИЧЕСКИЕ СВОЙСТВА МНОЖЕСТВА РЕШЕНИЙ ИСКАЖЁННЫХ СИСТЕМ УРАВНЕНИЙ

А. В. Волгин

Рассматриваются две однородные системы уравнений: система уравнений, в левой части которых стоят функции k-значной логики, и система уравнений, в левой части которых стоят функции, полученные из функций первой системы путём их независимого случайного искажения. Выведены условия на вероятностные законы искажений функций, обеспечивающие три варианта взаимного поведения множеств решений этих систем при согласованном увеличении числа уравнений и числа неизвестных.

Ключевые слова: *системы уравнений, функции k-значной логики, искажённые функции.*

Пусть $\Omega_k = \{0, 1, \ldots, k-1\}$, $F_k(n) = \{f : \Omega_k^n \to \Omega_k\}$ — множество всех n-местных функций k-значной логики от переменных $x_1, \ldots, x_n$, $n, k \in \mathbb{N}$. Рассмотрим систему из $T \in \mathbb{N}$ уравнений

$$f_t(x) = 0, \quad f_t \in F_k(n), \quad t = 1, \ldots, T. \tag{1}$$

Через S обозначим множество решений системы (1).

Каждой функции $f \in F_k(n)$ сопоставим множества $A_0(f)$ и $A_1(f)$ тех значений аргумента, на которых она принимает значение нуль и отлична от нуля соответственно. Обозначим $a_0(f) = |A_0(f)|$, $a_1(f) = |A_1(f)|$. Для каждой функции $f \in F_k(n)$ и целого числа $0 \leqslant d \leqslant a_0(f)$ рассмотрим множество функций

$$B(f, d) = \{g \in F_k(n) : |A_0(f) \cup A_1(g)| + |A_1(f) \cup A_0(g)| = d\},$$

таких, что при $g \in B(f, d)$ число значений аргументов, в которых одна из функций f и g принимает значение нуль, а другая отлична от нуля, равно d.

На множествах $B(f_1, d), \ldots, B(f_T, d)$ зададим равномерные вероятностные распределения, в соответствии с которыми выберем случайно и независимо функции $\tilde{f}_1, \ldots, \tilde{f}_T$. Рассмотрим систему случайных уравнений

$$\tilde{f}_t(x_1, \ldots, x_n) = 0, \quad \tilde{f}_t \in B(f_t, d), \quad t = 1, \ldots, T. \tag{2}$$

Множество её решений обозначим через $\tilde{S}$.

Рассматривается задача нахождения связи между множествами S и $\tilde{S}$ решений систем уравнений (1) и (2) при выполнении следующих асимптотических условий: при $T, n \to \infty$ сами функции $f_1, \ldots, f_T$ меняются так, что

1) число решений системы (1) имеет конечный предел, т. е. $|S| \to \Sigma \in \mathbb{N}$;

2) число значений аргументов, на которых функции f_t, $t = 1, \ldots, T$, принимают значение нуль, неограниченно возрастает, т. е. $a_0(f_t) \to \infty$, $t = 1, \ldots, T$.

В [1] данная задача рассматривается для случая булевых уравнений, при этом предполагается, что каждая функция системы (1) является уравновешенной, т. е. принимает каждое из значений нуль и единица ровно на 2^{n-1} значениях аргумента. В данной