УДК 621.391:519.7

А. Н. Алексейчук
Специальный факультет СБ Украины в составе Военного института телекоммуникаций и информатизации НТУУ «КПИ»

Достаточные условия стойкости рандомизированных блочных систем шифрования относительно метода криптоанализа на основе коммутативных диаграмм

Получены достаточные условия отсутствия определенных нетривиальных конгруэнций многоосновных алгебр, описывающих рандомизированные блочные системы шифрования, соответствующие SPN-подобным шифрам или шифрам Фейстеля. Указанные условия исключают возможность применения к таким системам шифрования метода криптоанализа на основе коммутативных диаграмм.

Ключевые слова: *криптографическая защита информации, блочный шифр, рандомизированная система шифрования, конгруэнция, метод коммутативных диаграмм.*

Введение

Одним из перспективных направлений в криптографии является разработка методов построения, анализа и обоснования стойкости рандомизированных криптографических систем [1, 2]. Существенная особенность таких криптосистем состоит в совместном применении криптографических преобразований и случайного кодирования источника открытых сообщений, осуществляемого с целью повышения стойкости криптосистем к различным атакам. Указанное направление включает в себя широкий круг научных задач, имеющих разнообразную прикладную направленность. Отметим среди них задачи исследования теоретической стойкости рандомизированных симметричных систем шифрования [1–4], построения и оценки эффективности протоколов передачи ключей по каналу связи с отводом [3, 5, 6], теоретически стойких схем распределения ключей и схем разделения секрета [5, 7].

В ряду перечисленных задач важное практическое значение имеет разработка новых методов построения рандомизированных блочных систем шифрования, удовлетворяющих современным технологическим требованиям и имеющих обоснованную стойкость к широкому классу криптоаналитических атак. Актуальность данной задачи обусловлена необходимостью повышения стойкости и поддержания

требуемого уровня безопасности используемых в настоящее время блочных шифров.

Одним из стандартных требований к блочным шифрам является их обоснованная стойкость относительно криптоаналитических атак, основанных на группировании открытых, шифрованных сообщений или ключей в классы эквивалентных (или близких, в том или ином смысле) объектов, позволяющем понизить трудоемкость алгоритмов решения (размерность) соответствующих криптоаналитических задач. Единообразный общий подход к построению такого рода атак на блочные шифры получил название метода гомоморфизмов [8–11] или метода коммутативных диаграмм [12]. Сущность метода заключается в построении для данного блочного шифра с множеством открытых (шифрованных) сообщений X, множеством ключей Λ и функцией шифрования $F : X \times \Lambda \to X$ трех отображений $\rho : X \to A$, $\rho' : X \to B$, $g : A \to B$ (где A и B — некоторые конечные множества), удовлетворяющих условию $\rho'(F(x,\lambda)) = g(\rho(x))$ для любых $x \in X$, $\lambda \in \Lambda$. (Указанное условие означает, что соответствующая диаграмма, составленная из четырех множеств и четырех отображений, является коммутативной, откуда и происходит название метода).

В [8–12] показано, что существование нетривиальной коммутативной диаграммы (или, что то же самое, нетривиальной конгруэнции двухосновной универсальной алгебры, описывающей блочный шифр [13]), приводит к уязвимости шифра относительно ряда алгебраических атак. Целью настоящей статьи является обоснование условий, исключающих возможность проведения подобных атак на широкий класс рандомизированных блочных систем шифрования. Полученные условия накладывают ограничения только на конструкцию рандомизатора исходного блочного шифра, допускают простую практическую проверку и позволяют обеспечить обоснованную стойкость соответствующих рандомизированных систем шифрования относительно метода коммутативных диаграмм.

Определения основных понятий

Далее в статье свободно используется ряд алгебраических понятий, определения которых можно найти в [10, 14]. Необходимые сведения об алгебраических моделях шифров изложены в [9, 13].

Пусть G — конечная абелева группа порядка $q \geq 2$, K — непустое конечное множество, $(f_k : k \in K)$ — семейство подстановок на группе G^n. Рассмотрим r-раундовый ($r \geq 2$) блочный шифр $\mathfrak{I} = (G^n, \Lambda, F)$ с множеством открытых (шифрованных) сообщений G^n, множеством ключей $\Lambda = K^r$ и функцией шифрования F: $G^n \times \Lambda \to G^n$. По определению преобразование F_λ открытого сообщения $x \in G^n$ в шифрованный текст $y \in G^n$ на ключе $\lambda = (k(1),\ldots, k(r)) \in \Lambda$ является композицией r-раундовых шифрующих преобразований $f_{k(1)}, \ldots, f_{k(r)}$.

Введем в рассмотрение блочный шифр $\wp = (G^n, K, f)$, функция шифрования f которого задается равенством $f(x, k) = f_k(x)$, $x \in G^n$, $k \in K$. Отметим, что в силу данных определений шифр $\mathfrak{I}$ является r-й степенью шифра $\wp$ [9]. Далее предполагается, что блочный шифр $\mathfrak{I} = \wp^r$ удовлетворяет одному из следующих двух условий:

а) $\wp$ является SPN-подобным шифром, другими словами, существует подстановка $h: G^n \to G^n$ такая, что для любого $k \in K = G^n$ выполняется равенство:

$$f_k(x) = h(x + k),\ x \in G^n; \tag{1}$$

б) $\wp$ является шифром Фейстеля: $n = 2m$ — четное число, $K = G^m$, и существует подстановка φ: $G^m \to G^m$ такая, что для любого $k \in K$:

$$f_k(x) = f_k(x_1, x_2) = (x_2, x_1 + \varphi(x_2 + k)),\ x = (x_1, x_2) \in G^n. \tag{2}$$

Конгруэнцией шифра $\wp$ называется упорядоченная пара $\varepsilon(\wp) = (\varepsilon_1, \varepsilon_2)$ отношений эквивалентности на множестве G^n, удовлетворяющая условию: для любых $x, x' \in G^n$, $k \in K$ соотношение $x \equiv x' (\mathrm{mod}\ \varepsilon_1)$ влечет соотношение $f_k(x) \equiv f_k(x') \mathrm{mod}\ \varepsilon_2$ [9, 13]. Аналогично определяется понятие конгруэнции шифра $\Im$. Конгруэнция $\varepsilon(\wp)$ называется нетривиальной, если $\varepsilon_1 \neq 0_{G^n}$, $\varepsilon_2 \neq 1_{G^n}$, где 0_{G^n} и 1_{G^n} суть наименьшее и наибольшее отношения эквивалентности на группе G^n соответственно. Отношение эквивалентности, задаваемое посредством разложения группы G^n в смежные классы (СК) по ее подгруппе H, называется отношением смежности G^n по H [10].

Пусть π: $G^n \to G^n$ — некоторое отображение. Тогда по определению π имеет тривиальную линейную структуру, если не существует элемента $a \in G^n \backslash 0$ и комплексного характера $\chi \neq 1$ группы G^n таких, что функция $\chi(\pi x + a) + \pi(x))$, $x \in G^n$ является константой. Отметим, что в случае $G = (\mathbf{GF}(2), +)$ сформулированное условие означает, что все нетривиальные линейные комбинации координатных функций отображения π не имеют ненулевых линейных трансляторов [15].

Рандомизированные блочные системы шифрования

Пусть дано разложение группы G^n в прямую сумму собственных подгрупп S и T. Отождествим элементы $x \in G^n$ с упорядоченными парами (s, t) такими, что $s \in S$, $t \in T$. Зафиксируем подстановку π: $G^n \to G^n$ и определим рандомизированную блочную систему шифрования $\mathfrak{R} = \mathfrak{R}_{\Im}(S, T, \pi)$ как шифр с множеством открытых сообщений S, множеством ключей $\Lambda = K^r$, множеством шифрованных сообщений G^n и функцией шифрования ш: $S \times \Lambda \to G^n$ вида

$$\psi(s, \lambda) = F_\lambda(\pi(s, t)),\ s \in S,\ \lambda \in \Lambda, \tag{3}$$

где t — случайный элемент, равномерно распределенный на группе T. Зашифрование открытого сообщения $s \in S$ с помощью шифра $\mathfrak{R}_{\Im}(S, T, \pi)$ осуществляется следующим образом. Вначале случайно с вероятностью $|T|^{-1}$ выбирается сообщение $t \in T$, и упорядоченная пара (s, t) преобразуется под действием подстановки π в сообщение $\pi(s, t)$. Затем полученное сообщение зашифровывается на ключе λ шифра $\Im$. Для восстановления открытого текста s по шифрованному тексту

$y = F_\lambda(\pi(s, t))$ законный получатель находит сообщение $(s, t) = \pi^{-1}(F_\lambda^{-1}(y))$, по которому непосредственно получает s.

Отметим, что рассматриваемый класс рандомизированных блочных систем шифрования включает в себя ряд известных конструкций рандомизированных симметричных криптосистем [1]. В частности, если в приведенном выше определении подстановка π является автоморфизмом группы G^n, и группа S изоморфна группе G^k, где $1 < k < n$, то система шифрования $\mathfrak{R}_\mathfrak{I}(S, T, \pi)$ совпадает с так называемой рандомизацией $\mathfrak{R}_\sigma(\mathfrak{I})$ блочного шифра $\mathfrak{I}$ относительно гомоморфизма $\sigma : G^n \to G^k$, который определяется по формуле $\sigma(\pi(s, t)) = s$, $(s, t) \in G^n$ [16].

Понятие конгруэнции блочного шифра допускает естественное обобщение на случай рандомизированных блочных систем шифрования. А именно, рассмотрим отношения эквивалентности ε_S, ε_T и δ на множествах S, T и G^n соответственно. Назовем упорядоченный набор $\varepsilon(\mathfrak{R}) = (\varepsilon_S, \varepsilon_T, \delta)$ конгруэнцией системы шифрования $\mathfrak{R}$, если для любых s, $s' \in S$, t, $t' \in T$, $\lambda \in \Lambda$ выполняется условие:

$$(s \equiv s' \pmod{\varepsilon_S},\ t \equiv t' \pmod{\varepsilon_T}) \Rightarrow F_\lambda(\pi(s, t)) \equiv F_\lambda(\pi(s', t')) \pmod{\delta}.$$

Конгруэнция $\varepsilon(\mathfrak{R})$ называется нетривиальной, если $\delta \neq 1_{G^n}$, и выполняется хотя бы одно из неравенств $\varepsilon_S \neq 0_S$, $\varepsilon_T \neq 0_T$.

Нетрудно видеть, что существование для рандомизированной системы шифрования $\mathfrak{R}$ нетривиальной коммутативной диаграммы (то есть сюръективных отображений $\rho : S \to A$, $\rho' : X \to B$, $g : A \to B$ таких, что $1 < |A| < |S|$, $1 < |B| < |X|$ и $\rho'(F_\lambda(\pi(s,t))) = g(\rho(s))$ для любых $s \in S$, $t \in T$, $\lambda \in \Lambda$) равносильно существованию ее нетривиальной конгруэнции вида $\varepsilon(\mathfrak{R}) = (\varepsilon_S, 1_T, \delta)$. При наличии такой конгруэнции применение метода коммутативных диаграмм позволяет уменьшить трудоемкость ряда алгоритмов криптоанализа системы шифрования $\mathfrak{R}$ путем сведения исходной криптоаналитической задачи, сформулированной для этой системы, к аналогичной задаче меньшей размерности для ее гомоморфного образа по конгруэнции $\varepsilon(\mathfrak{R})$. Таким образом, обоснование стойкости рассматриваемых рандомизированных систем шифрования относительно метода коммутативных диаграмм равносильно доказательству отсутствия указанных выше нетривиальных конгруэнций этих систем.

Достаточные условия отсутствия нетривиальных конгруэнций рандомизированных блочных систем шифрования

Прежде всего, убедимся в справедливости следующего утверждения.

Утверждение 1. Если блочный шифр $\mathfrak{I}$ не имеет нетривиальных конгруэнций, то для любого разложения группы G^n в прямую сумму собственных подгрупп S, T и произвольной подстановки π: $G^n \to G^n$ рандомизированная система шифрования $\mathfrak{R} = \mathfrak{R}_\mathfrak{I}(S, T, \pi)$ не имеет нетривиальных конгруэнций.

Доказательство. Допустим, что $\varepsilon(\mathfrak{R}) = (\varepsilon_S, \varepsilon_T, \delta)$ есть нетривиальная конгруэнция системы шифрования $\mathfrak{R}$. Определим на группе G^n бинарное отношение $\varepsilon(\pi)$, полагая для любых $s, s' \in S$, $t, t' \in T$

$$((\pi(s, t), \pi(s', t')) \in \varepsilon(\pi)) \Leftrightarrow (s \equiv s' \,(\mathrm{mod}\ \varepsilon_S),\ t \equiv t' \,(\mathrm{mod}\ \varepsilon_T)). \qquad (4)$$

Непосредственная проверка показывает, что $\varepsilon(\pi)$ является отношением эквивалентности на группе G^n, и классы эквивалентности по модулю $\varepsilon(\pi)$ имеют вид:

$$X_{ij} = \pi(S_i \times T_j),\ i \in \overline{1, a},\ i \in \overline{1, b}, \qquad (5)$$

где $S_1, \ldots, S_a$ и $T_1, \ldots, T_b$ — классы эквивалентности по модулям ε_S и ε_T соответственно. Из равенства (5) вытекает, что $\varepsilon(\pi) \neq 0_{G^n}$, если $\varepsilon_S \neq 0_S$ или $\varepsilon_T \neq 0_T$. Следовательно, на основании соотношения (4) система $(\varepsilon(\pi), \delta)$ является нетривиальной конгруэнцией шифра $\Im$, что противоречит условию утверждения. Итак, система шифрования $\Re$ не имеет нетривиальных конгруэнций, что и требовалось доказать.

Следующее утверждение устанавливает необходимые условия, при которых данная пара отношений эквивалентности на группе G^n является нетривиальной конгруэнцией блочного шифра $\Im$, раундовые шифрующие преобразования которого имеют вид (1) или (2).

Утверждение 2. Пусть (ε, δ) — нетривиальная конгруэнция шифра $\Im = \wp^r$, где шифр $\wp$ удовлетворяет любому из сформулированных выше условий (а), (б). Тогда отношение ε содержится в отношении смежности группы G^n по некоторой ее собственной подгруппе.

Доказательство. Пусть шифр $\Im$ удовлетворяет условию (а), то есть является SPN-подобным шифром. Зафиксируем элементы $k(2), \ldots, k(r) \in K$ и определим отношение δ' на группе G^n, полагая для любых $y', y'' \in G^n$

$$y' \,\delta'\, y'' \Leftrightarrow (f_{k(2)} \ldots f_{k(r)}\, h(y'))\ \delta\, (f_{k(2)} \ldots f_{k(r)}\, h(y'')),$$

где h: $G^n \to G^n$ — подстановка, определяемая равенством (1). Заметим, что δ' является отношением эквивалентности на группе G^n, причем $\delta' \neq 1_{G^n}$, так как $\delta \neq 1_{G^n}$. Далее, на основании условия утверждения и формулы (1) для любых x', $x'' \in G^n$, $k \in K$ справедливы соотношения

$$x' \,\varepsilon\, x'' \Rightarrow (f_{k(2)} \ldots f_{k(r)}\, h(x' + k))\ \delta\, (f_{k(2)} \ldots f_{k(r)}\, h(x'' + k)) \Leftrightarrow (x' + k)\ \delta'\, (x'' + k),$$

из которых вытекает, что тройка отношений эквивалентности $(\varepsilon,\ 0_{G^n},\ \delta')$ является конгруэнцией абелевой группы G^n (см. определение, приведенное в статье [10]). Согласно теореме 1, доказанной в [10], существует подгруппа H группы G^n такая, что отношение ε содержится в отношении смежности G^n по H, а отношение δ' содержит указанное отношение смежности. При этом, поскольку $\delta' \neq 1_{G^n}$, то $H \neq G^n$. Таким образом, ε содержится в отношении смежности группы G^n по ее собственной подгруппе H, что и требовалось доказать.

Предположим теперь, что блочный шифр $\Im$ удовлетворяет условию (б), то есть является шифром Фейстеля. По условию утверждения выполняются равенст-

ва $\mathfrak{I} = \wp^r = \wp^2 \wp^{r-2}$ ($r \geq 2$), и аналогично рассмотренному выше случаю, в котором шифр $\mathfrak{I}$ удовлетворяет условию (а), существует отношение эквивалентности δ' на группе G^n такое, что пара (ε, δ') является нетривиальной конгруэнцией шифра $\wp^2$. Отсюда на основании теоремы 2 из [10] заключаем, что существует подгруппа H группы G^n такая, что ε содержится в отношении смежности G^n по H, а δ' содержит это отношение. Наконец, в силу условия $\delta' \neq 1_{G^n}$ имеем $H \neq G^n$, что и требовалось доказать.

Итак, утверждение 2 полностью доказано.

Докажем теперь теорему, содержащую основной результат настоящей статьи.

Теорема. Пусть $\mathfrak{R} = \mathfrak{R}_{\mathfrak{I}}(S, T, \pi)$ — рандомизированная блочная система шифрования, соответствующая шифру $\mathfrak{I} = \wp^r$, где шифр $\wp$ удовлетворяет любому из условий (а), (б). Предположим, что подстановка π имеет тривиальную линейную структуру. Тогда система шифрования $\mathfrak{R}$ не имеет нетривиальных конгруэнций (ε_S, ε_T, δ) таких, что хотя бы одно из отношений ε_S, ε_T содержит отношение смежности группы S, T соответственно по некоторой ненулевой подгруппе этой группы.

Доказательство. Пусть (ε_S, ε_T, δ) — нетривиальная конгруэнция системы шифрования $\mathfrak{R}$, и отношение эквивалентности ε_S содержит отношение смежности группы S по ее подгруппе $L \neq 0$. Тогда для любого $a \in L \backslash 0$ выполняется условие

$$(s \in S) \Rightarrow (s + a \equiv s \pmod{\varepsilon_S}),$$

из которого на основании соотношения (4) вытекает, что

$$\pi(s + a, t) \equiv \pi(s, t) \pmod{\varepsilon(\pi)},\ s \in S,\ t \in T,\ a \in L \backslash 0. \tag{6}$$

Далее, поскольку ($\varepsilon(\pi)$, δ) является нетривиальной конгруэнцией шифра $\mathfrak{I}$ (см. доказательство утверждения 1), то, согласно утверждению 2, отношение $\varepsilon(\pi)$ содержится в отношении смежности группы G^n по некоторой ее собственной подгруппе H. Отсюда, в силу соотношения (6) получаем:

$$\pi(s + a, t) \equiv \pi(s, t) \pmod{H},\ s \in S,\ t \in T,\ a \in L \backslash 0. \tag{7}$$

Если теперь χ — нетривиальный характер группы G^n, аннулирующий подгруппу H, то на основании соотношения (7) для любых $s \in S$, $t \in T$ имеет место равенство

$$\chi(\pi((s, t) + (a, 0)) - \pi(s, t)) = 0,$$

причем $(a, 0) \in G^n \backslash 0$. Однако полученное равенство противоречит условию тривиальности линейной структуры подстановки π.

Итак, отношение эквивалентности ε_S не содержит отношений смежности группы S по ненулевым подгруппам этой группы. Аналогично показывается, что ε_T не содержит отношений смежности по ненулевым подгруппам группы T. Теорема доказана.

Следствие. При выполнении условий теоремы для любого отношения эквивалентности $\delta \neq 1_{G^n}$ на группе G^n упорядоченные наборы $(1_S, 0_T, \delta)$ и $(0_S, 1_T, \delta)$ не являются конгруэнциями рандомизированной блочной системы шифрования $\mathfrak{R}$. В частности, эта система шифрования имеет обоснованную стойкость относительно метода коммутативных диаграмм.

Выводы

Полученные результаты свидетельствуют о том, что стойкость рандомизированных блочных систем шифрования относительно метода коммутативных диаграмм может быть обеспечена при достаточно слабых ограничениях на множество раундовых шифрующих преобразований исходного блочного шифра $\mathfrak{I}$. В частности, условие тривиальности линейной структуры подстановки π в выражении (3) гарантирует отсутствие широкого класса конгруэнций рандомизированной системы шифрования $\mathfrak{R}$ независимо от конкретного вида отображений f_k, $k \in K$, определенных по формулам (1) или (2). (Отметим, что проверка этого условия сводится к вычислению таблицы линейных аппроксимаций подстановки π и в практически важном случае G = (**GF**(2), +) может быть проведена с использованием результатов, изложенных в [15], стр. 106). Таким образом, практическое построение рандомизированных блочных систем шифрования, имеющих обоснованную стойкость относительно метода коммутативных диаграмм, возможно, в том числе, при условии отсутствия полной информации о криптографической схеме исходного блочного шифра $\mathfrak{I}$.

1. *Rivest R.L., Sherman A.T.* Randomization Encryption Techniques // Advances in Cryptology — CRYPTO'82, Proceedings. – Springer Verlag, 1982. — P. 145–167.

2. *Massey J.L.* An Introdution to Contemporary Cryptology // Proc. IEEE. — 1988. — Vol. 76, N 5. — P. 533–549.

3. *Maurer U.M.* Provable Security in Cryptography: Diss. ETH N 9260. — 1990. — 120 p.

4. *Штарьков Ю.М., Юхансон Т., Смитс Б.Дж.М.* О совместной стойкости защиты информации и ключа в секретных системах // Проблемы передачи информации. — 1998. — Т. 34. — Вып. 2. — С. 117–127.

5. *Ahlswede R., Csiszar I.* Common Randomness in Information Theory and Cryptography. — Part 1: Secret sharing // IEEE Trans. Inform. Theory. — 1993. — Vol. 39, N 4. — P. 1121–1132.

6. *Чисар И.* Почти независимость случайных величин и пропускная способность криптостойкого канала // Проблемы передачи информации. — 1996. — Т. 32. — Вып. 1. — С. 48-57.

7. *Stinson D.R.* On Some Methods for Unconditionally Secure Key Distribution and Broadcast Encryption // Designs, Codes and Cryptography. — 1997. — Vol. 12. — P. 215–243.

8. *Горчинский Ю.Н.* О гомоморфизмах многоосновных универсальных алгебр в связи с криптографическими применениями // Труды по дискретной математике.— М.: ТВП, 1997. — Т. 1. — С. 67–84.

9. *Бабаш А.В., Шанкин Г.П.* Криптография. — М.: Солон-Р, 2002. — 511с.

10. *Шапошников И.Г.* О конгруэнциях конечных многоосновных универсальных алгебр // Дискретная математика. — 1999. — Т. 11. — Вып. 3. — С. 48–62.

11. *Paterson K.G.* Imprimitive Permutation Groups and Trapdoors in Iterated block Ciphers // Fast Software Encryption. — FSE'99, Proceedings. — Springer Verlag, 1999. — P. 201–214.

12. *Wagner D.* Towards a Unifying View of Block Cipher Cryptanalysis // Fast Software Encryption. — FSE'04, Proceedings. — Springer Verlag, 2004. — P. 116–135.

13. *Алексейчук А.Н., Романов А.И.* Регулярные конгруэнции и строение алгебраических моделей симметричных криптосистем // Радиотехника. — 2002. — Вып. 126. — С. 42–58.

14. *Глухов М.М., Елизаров В.П., Нечаев А.А.* Алгебра: Учебник. В 2-х т., Т. I. — М.: Гелиос АРВ, 2003. — 336 с.

15. *Логачев О.А., Сальников А.А., Ященко В.В.* Булевы функции в теории кодирования и криптологии. — М.: МЦНМО, 2004. — 470 с.

16. *Алексейчук А.Н., Васюков И.В., Корнейко А.В.* Обоснование стойкости вероятностных моделей рандомизированных блочных шифров к методу разностного криптоанализа // Электронное моделирование. — 2004. — Т. 26, № 4. — С. 23–35.

Поступила в редакцию 08.12.2006