Информационные процессы, Том 9, № 3, 2009, стр. 138–146

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Криптографические возможности упорядоченной системы образующих симметрической группы

Калинчук С.А.*, Сагалович Ю.Л.**

**NetCracker Technology, Москва, Россия*

***Институт проблем передачи информации, Российская академия наук, Москва, Россия*

Поступила в редколлегию 7.09.2009

Аннотация—Предложена криптографическая система, построенная на основе упорядоченной системы образующих симметрической группы S_n. В роли секретного ключа выступает система образующих, а криптоаналитику вместе с наблюдаемым зашифрованным сообщением известна только степень симметрической группы.

1. ВВЕДЕНИЕ

Пусть система транспозиций

$$\Psi = \mathcal{T}_1\ \mathcal{T}_2\ \ldots\ \mathcal{T}_r$$

есть упорядоченная система образующих [1–3] симметрической группы S_n. (Напомним, что требование упорядоченности существенно из-за некоммутативности операции в симметрической группе.)

Тогда каждая подстановка изображается произведением

$$\mathcal{P} = \mathcal{T}_1^{\gamma_1} \cdot \mathcal{T}_2^{\gamma_2} \cdot \ldots \cdot \mathcal{T}_r^{\gamma_r}\,, \tag{1}$$

где $\gamma_j = 0, 1, j = \overline{1, r}$.

Иначе говоря, каждому двоичному вектору $\Gamma = (\gamma_1, \gamma_2, \ldots, \gamma_r)$ отвечает подстановка $\mathcal{P} \in S_n$, как произведение тех транспозиций, для которых $\gamma_j = 1$. Однако это соответствие отнюдь не взаимно однозначное. Необходимое условие

$$2^r > n!$$

означает, что одна и та же подстановка $\mathcal{P} \in S_n$ может быть представлена несколькими векторами Γ.

Обозначим множество этих векторов символом $\mathcal{M}_\mathcal{P}$, а мощность самого множества символом $M_\mathcal{P}$. Величиной $M_\mathcal{P}$ частично определяются некоторые криптографические свойства упорядоченной системы образующих (УСО) симметрической группы.[1]

Данная статья построена следующим образом. В разделе 2 описана криптографическая система на основе УСО. Далее в разделе 3 выводится асимптотическая нижняя граница числа упорядоченных систем образующих и их орбит как классов эквивалентности, на которые распадается множество УСО под действием преобразования из группы S_n. В разделе 4 дается оценка стойкости предложенной криптосистемы.

[1] Именно этот факт, как основной, рекомендовал изучить А.А.Нечаев, впервые в 2006 г. заметивший и подсказавший авторам использовать возможности УСО в качестве криптографической системы. Ведь если для некоторой подстановки $\mathcal{P} \in S_n$ окажется, что $M_\mathcal{P} = 1$, то криптографическая стойкость исчезает! К счастью, отнюдь не величина $M_\mathcal{P}$ определяет криптостойкость УСО, тем более, что случай $M_\mathcal{P} = 1$ действительно встретился. Обнаружилась другая, более надежная защита вектора Γ от атаки криптоаналитика. Она подробно рассмотрена в следующем параграфе.

2. КРИПТОГРАФИЧЕСКАЯ СИСТЕМА НА ОСНОВЕ УСО

Прежде чем приступать к описанию криптографической системы на основе упорядоченной системы образующих, рассмотрим ряд свойств УСО. Эти свойства будут использованы для оценки криптостойкости.

Лемма 1. *В УСО не существует независимых транспозиций.*

Доказательство. Предположим противное, и пусть (a, b) – такая транспозиция. Тогда она коммутирует со всеми транспозициями УСО, и потому, УСО $\Psi = \Psi'(a, b)$, где $(a, b) \notin \Psi'$. Это означает одно из двух:

1. Ψ' есть УСО симметрической группы S_{n-2}. Тогда индекс группы S_{n-2} в группе S_n равен $n!/(n-2)! = n(n-1)$, в то время как УСО $\Psi = \Psi'(a, b)$, порождает только два смежных класса, т.е. саму группу S_{n-2} и смежный класс $S_{n-2}(a, b)$.

2. Ψ' вообще не является УСО. Но тогда и Ψ не является УСО.

Замечание. Легко видеть, что данное доказательство годится на случай любого числа независимых транспозиций, в том числе когда независимая транспозиция (a, b) повторяется не единожды. Действительно, если каждая из независимых транспозиций встречается только один раз, то к ней доказательство леммы применяется непосредственно. Если же независимая транспозиция повторяется несколько раз, то так как она коммутирует со всеми остальными транспозициями УСО, то все её экземпляры можно собрать в одном месте УСО. В случае их четного количества, их произведение равно тождественной подстановке. В случае нечетного – это произведение превращается в одну единственную транспозицию, а этот случай рассмотрен в основном доказательстве леммы.

Элементы, перемещаемые транспозициями $\mathcal{T}_1, \mathcal{T}_2, \ldots, \mathcal{T}_r$, входящими в УСО Ψ, можно подвергнуть произвольной подстановке $s \in S_n$. Обозначим данное преобразование символом θ_s. Очевидно, что новая система $\Psi' = \theta_s(\Psi)$, полученная таким образом, также будет являться УСО.

Пример 1. Система $\Psi = (1, 2)(1, 3)(2, 4)(1, 4)(2, 3)$ является УСО симметрической группы S_4. Пусть $s = (3, 1, 4, 2)$. Тогда система

$$\Psi' = \theta_s(\Psi) = (1, 3)(3, 4)(1, 2)(2, 3)(1, 4)$$

тоже является УСО группы S_4.

Можно заметить, что

$$\Psi' = \theta_s(\Psi) = \theta_s(\mathcal{T}_1)\ \theta_s(\mathcal{T}_2)\ \ldots\ \theta_s(\mathcal{T}_r)\,,$$

где $\theta_s(\mathcal{T}_i) = s^{-1}\mathcal{T}_i s\,,\ 1 \leqslant i \leqslant r$.

Также $\theta_s^{-1} = \theta_{s^{-1}}$, $\theta_{s_2}\theta_{s_1} = \theta_{s_1 s_2}$.

Лемма 2. *Произвольная нетождественная подстановка $s \in S_n$, примененная к УСО (преобразование θ_s), сохраняет ее свойства как УСО, но всегда найдется по крайней мере одна такая транспозиция $\mathcal{T}_i$, что $\theta_s(\mathcal{T}_i) \neq \mathcal{T}_i$.*

Доказательство. Поскольку подстановка s не тождественна, что существует такое a, что $s(a) = b \neq a$. Возможны два случая, когда УСО либо содержит транспозицию (a, b), либо

нет. В первом случае, поскольку по лемме 1 транспозиция (a,b) не является независимой, то УСО содержит транспозицию (a,x) или также (b,y), где $x \neq a,b$, $y \neq a,b$. Во втором случае, когда УСО не содержит (a,b), то она обязательно содержит транспозиции и (a,x), и (b,y), где $x \neq a,b$, $y \neq a,b$. Получается, что в обоих случаях УСО содержит транспозицию (a,x) или также (b,y).

После действия преобразования θ_s транспозиция (a,x) превратится в транспозицию $\theta_s((a,x)) = (b,s(x))$, а (b,y) – в $\theta_s((b,y)) = (s(b),s(y))$. Поскольку $b \neq a,x$ и $b = s(a) \neq s(b),s(y)$ $(b \neq a,\ y \neq a)$, то $(a,x) \neq (b,s(x))$ и $(b,y) \neq (s(b),s(y))$.

Отсюда следует, что всегда найдется по крайней мере одна такая транспозиция, которая после не тождественного преобразования θ_s, заведомо изменится. Что и требовалось доказать.

Замечание. Для каждой транспозиции $\mathcal{T}_i$ найдется сохраняющее ее преобразование θ_s.

Следствие 1. *Различные подстановки, примененные к одной и той же УСО, дают и различные УСО.*

Доказательство. Предположим противное. Пусть при $s_1 \neq s_2$ имеет место $\theta_{s_1}(\Psi) = \theta_{s_2}(\Psi)$. Применив к обеим частям равенства преобразование $\theta_{s_2}^{-1}$ (или $\theta_{s_1}^{-1}$), получим $\theta_{s_1 s_2^{-1}}(\Psi) = \Psi$ (или $\Psi = \theta_{s_2 s_1^{-1}}(\Psi)$) вопреки лемме 2.

Назовем *орбитой*, или *классом эквивалентности*, множество УСО, получаемых друг из друга всеми подстановками $s \in S_n$. Очевидно, что две орбиты либо не пересекаются, либо совпадают.

Из следствия 1 немедленно получается

Утверждение 1. *Мощность орбиты (класса эквивалентности) УСО равна* $n!$.

Теперь, перейдем с рассмотрению криптографической системы на основе УСО. Пусть сообщения передаются последовательностями Г. Криптоаналитик наблюдает подстановку $\mathcal{P} \in S_n$, отвечающую вектору Г (см.(1)). Ему надо решить, какой именно вектор Г передан из множества $\mathcal{M}_{\mathcal{P}}$.

Ясно, что атака на передаваемую подстановку $\mathcal{P} \in S_n$ будет тем менее эффективной, чем большее число векторов Г ей отвечает, т.е. чем больше число $M_{\mathcal{P}}$. С другой стороны для криптографа эта задача должна быть максимально облегчена

Отсюда следует, что секретный ключ должен содержать прямое указание криптографам, как найти истинный вектор Г. Этим указанием может быть, старший или младший вектор в лексикографическом порядке векторов $\Gamma \in \mathcal{M}_{\mathcal{P}}$.

Что касается числа $M_{\mathcal{P}}$, то пока нельзя пойти дальше тривиального предположения: при достаточно больших n среднее значение для $M_{\mathcal{P}}$ равно $M_{\mathcal{P}}^{\text{средн}} = 2^r/n!$, и что $1 \leqslant M_{\mathcal{P}}^{\text{мин}} \leqslant M_{\mathcal{P}}^{\text{средн}} \leqslant M_{\mathcal{P}}^{\text{макс}} \leqslant 2^r - (n!-1)$. Обозначим символом $C(M_{\mathcal{P}})$ число подстановок $\mathcal{P}$ с одним им тем же размером $M_{\mathcal{P}}$. Для обозримых значений n на ЭВМ получены таблицы:

Пример 2. При $n = 8$ и $r = 22$ для УСО:

$$(1,5)(1,7)(3,5)(1,3)(5,7)(2,6)(2,8)(4,6)(2,4)(6,8)$$
$$(1,2)(3,4)(1,4)(3,2)(5,6)(7,8)(5,8)(7,6)(1,8)(2,7)(3,6)(4,5)\,.$$

$M_{\mathcal{P}}$	32	48	64	72	88	96	144	256	384	576
$C(M_{\mathcal{P}})$	1024	4096	4352	6144	4096	9216	10240	128	512	512

Пример 3. При $n = 8$ и $r = 18$ для УСО:

$$(1,3)(5,7)(1,7)(3,5)(2,4)(2,8)(4,6)$$
$$(1,2)(3,4)(1,4)(3,2)(5,6)(7,8)(5,8)(7,6)(1,8)(3,6)(4,5)\,.$$

$M_{\mathcal{P}}$	2	4	5	6	8	9	10	16	24	36
$C(M_{\mathcal{P}})$	4096	6144	10240	8192	256	8192	2048	128	512	512

Пример 4. При $n = 6$ и $r = 12$ для УСО:

$$(1,3)(1,4)(1,5)(1,6)(2,3)(2,5)(1,2)(4,6)(4,5)(3,6)(3,4)(5,6)$$

$M_{\mathcal{P}}$	1	2	3	4	5	6	7	8	9	10	11	12
$C(M_{\mathcal{P}})$	128	112	32	32	32	80	64	64	32	16	64	64

Значительный разброс величины $M_{\mathcal{P}}$ (да к тому же появление пресловутой единицы в последнем примере) делает ее ненадежным показателем криптостойкости УСО. Однако благодаря утверждению 1, центр тяжести криптостойкости системы можно перенести на другое свойство УСО, именно, на мощность $n!$ орбиты и на число орбит. Даже если бы для каждой УСО существовала всего одна орбита, и секретный ключ содержал бы указание именно на одну УСО из всех $n!$ УСО орбиты, то это создало для криптоаналитика факториальную сложность атаки. Но и орбита может оказаться не единственной. Например, с помощью ЭВМ было получено, что при $n = 4$, $r = 5$ существует как минимум 4 УСО, являющихся представителями своих непересекающихся орбит:

$$\begin{array}{ll}(1,2)(1,3)(2,4)(1,4)(2,3); & (1,2)(3,4)(1,3)(2,4)(1,4);\\ (1,2)(1,3)(2,4)(2,3)(1,4); & (1,2)(3,4)(1,3)(2,4)(2,3).\end{array} \qquad (2)$$

Легко проверить, что эти УСО не могут быть получены друг из друга никакими подстановками группы S_4. Различными ухищрениями можно увеличить число орбит для заданного n. Было показано, например, что при $n = 5$ и $r = 8$ существует по меньшей мере 296 орбит УСО.

Оценке числа орбит посвящен следующий параграф.

Криптоаналитику известен единственный параметр. Это степень n группы S_n.

Из сказанного следует, что криптографическую систему на основе УСО можно построить следующим образом.

Секретный ключ

1. Номер орбиты, если она не единственная, и номер в ней упорядоченной системы образующих Ψ симметрической группы S_n

2. Указание, как специальным образом выбирать один двоичный вектор Γ (например, старший или младший вектор в лексикографическом порядке) из множества $\mathcal{M}_{\mathcal{P}}$, где $\mathcal{P} = \mathcal{T}_1^{\gamma_1} \cdot \mathcal{T}_2^{\gamma_2} \cdot \ldots \cdot \mathcal{T}_r^{\gamma_r}$.

По сути такое указание определяется взаимно однозначным соответствием F_Ψ между $n!$ подстановками группы S_n и передаваемыми $n!$ двоичными векторами Γ размера r.

Параметр, известный криптоаналитику

Степень n симметрической группы S_n.

Множество допустимых сообщений

Множество двоичных векторов Γ размера r.

Подчеркнём, что из всех 2^r векторов криптограф будет использовать не более $n!$ векторов.

Шифрование

Вычисляется сообщение, а именно, подстановка $\mathcal{P} = \Psi(\Gamma)$.

Расшифрование

Вычисляется двоичный вектор $\Gamma = F_\Psi(\mathcal{P})$.

Замечание. Подчеркнём, что и при шифровании, и при расшифровании необходима операция построения множества $\mathcal{M}_\mathcal{P}$ для заданной подстановки $\mathcal{P} \in S_n$. Поскольку для реализации этой операции на данный момент не существует другого алгоритма, отличного от полного перебора всех 2^r двоичных векторов, то сложность и шифрования, и расшифрования равна по порядку 2^r. При $r \sim n \log_2^2 n$ объем перебора будет равен $n^{n \log_2 n}$.

Стойкость этой системы основана на том, что для её взлома необходимо решить задачу поиска орбиты (класса эквивалентности) упорядоченных систем образующих размера r, задачу выбора нужной УСО из этого класса и задачу выбора подходящего вектора Γ из множества $\mathcal{M}_\mathcal{P}$.

Несмотря на то, что выше доминирующая роль в криптостойкости предлагаемой системы отведена строению УСО и их орбит, значение множества $\mathcal{M}_\mathcal{P}$ также достаточно велико, так как ничто не мешает запретить при передаче шифрованных текстов использовать те из них, которым отвечают $\mathcal{M}_\mathcal{P}$ с малыми значениями $M_\mathcal{P}$.

Таким образом, дешифрование криптоаналитиком зашифрованного сообщения проходит в два этапа: 1. Определение УСО. 2. Определение множества $\mathcal{M}_\mathcal{P}$ и вектора Γ в нём.

Завершим описание криптографических свойств УСО следующей леммой

Лемма 3. *Если система* $\Psi = \mathcal{T}_1\ \mathcal{T}_2\ \ldots\ \mathcal{T}_r$ *является УСО, то и система*

$$\widehat{\Psi} = \mathcal{T}_r\ \ldots\ \mathcal{T}_2\ \mathcal{T}_1$$

является упорядоченной системой образующих.

Доказательство. Так как УСО Ψ порождает всю группу S_n, то вместе с произвольной подстановкой $\mathcal{P} = \mathcal{T}_1^{\gamma_1}\mathcal{T}_2^{\gamma_2} \cdot \ldots \cdot \mathcal{T}_r^{\gamma_r}$, она порождает и подстановку

$$\mathcal{P}^{-1} = (\mathcal{T}_1^{\gamma_1}\mathcal{T}_2^{\gamma_2} \cdots \mathcal{T}_r^{\gamma_r})^{-1} = \mathcal{T}_r^{-1\gamma_r}\mathcal{T}_{r-1}^{-1\gamma_{(r-1)}} \cdots \mathcal{T}_1^{-1\gamma_1} = \mathcal{T}_r^{\gamma_r}\mathcal{T}_{r-1}^{\gamma_{(r-1)}} \cdots \mathcal{T}_1^{\gamma_1}, \tag{3}$$

ввиду $\mathcal{T}_i^{-1} = \mathcal{T}_i$.

Это означает, что любая подстановка группы S_n может быть представлена в виде (3), что и требовалось.

Очевидно, отношение $(\widehat{\ })$ рефлексивно.

Пусть имеется комплект уже построенных l непересекающихся орбит, и пусть Ψ есть представитель одной из них. Спрашивается является ли новой орбита, которой принадлежит УСО $\widehat{\Psi}$, или она содержится среди уже построенных. Ответ даёт очевидная

Лемма 4. *Пусть*

$$\Omega_1, \Omega_2, \ldots, \Omega_l \tag{4}$$

уже построенные орбиты, и пусть УСО $\Psi_{\Omega_i} \in \Omega_i, i = 1, 2, \ldots l$.

УСО $\widehat{\Psi}_{\Omega_i}$ не принадлежит никакой из орбит (4) *тогда и только тогда, когда не найдётся такой подстановки $s \in S_n$, что каково бы ни было $j = 1, \ldots, l$,*

$$\Psi_{\Omega_j} = \theta_s(\widehat{\Psi}_{\Omega_i}) \, . \tag{5}$$

Пример 5. В (2) были приведены четыре УСО, которые являются представителями разных орбит. Рассмотрим следующую таблицу

Орбита Ω_i	Её представитель Ψ_{Ω_i}	$\widehat{\Psi}_{\Omega_i}$	s
Ω_1	$(1,2)(1,3)(2,4)(1,4)(2,3)$	$(2,3)(1,4)(2,4)(1,3)(1,2)$	$s_1 = (1432)$
Ω_2	$(1,2)(1,3)(2,4)(2,3)(1,4)$	$(1,4)(2,3)(2,4)(1,3)(1,2)$	$s_2 = (1234)$
Ω_3	$(1,2)(3,4)(1,3)(2,4)(1,4)$	$(1,4)(2,4)(1,3)(3,4)(1,2)$	$s_3 = (1234)$
Ω_4	$(1,2)(3,4)(1,3)(2,4)(2,3)$	$(2,3)(2,4)(1,3)(3,4)(1,2)$	$s_4 = (1432)$

Непосредственной проверкой убеждаемся, что $\theta_{s_1}(\widehat{\Psi}_{\Omega_1}) = \Psi_{\Omega_3}$, и $\theta_{s_2}(\widehat{\Psi}_{\Omega_2}) = \Psi_{\Omega_4}$.

Иными словами, система $(1,2)(1,3)(2,4)(1,4)(2,3)$, которая является представителем орбиты Ω_1, после применения к ней преобразования леммы 3, переходит в систему $(2,3)(1,4)(2,4)$ $(1,3)(1,2)$. Эта система принадлежит орбите Ω_3, поскольку существует подстановка $s_1 = (4,1,2,3)$, которая переводит полученную систему в представителя орбиты Ω_3, т.е в систему $(1,2)(3,4)(1,3)(2,4)(1,4)$.

Аналогичная фраза формулируется относительно систем орбит 2 и 4.

Таким образом, операция $(\widehat{\ })$ новых орбит не прибавила.

На случай $i = j$ имеет место

Утверждение 2. *Две УСО Ψ и $\widehat{\Psi}$ принадлежат одной орбите тогда и только тогда, когда существует такая подстановка s, что для любой транспозиции $\mathcal{T}_i \in \Psi$ выполняется равенство $\mathcal{T}_i = \theta_s(\mathcal{T}_{r-i+1})$, т.е. $\Psi = \theta_s(\widehat{\Psi})$.*

3. ОЦЕНКА ЧИСЛА ОРБИТ УСО

Дальнейшее усложнение взлома основано на добавлении к УСО фиктивных транспозиций. От этой операции УСО не перестанет быть таковой. Но число орбит возрастёт, что и усложнит взлом.

Обозначим символом L максимальное число $\frac{n(n-1)}{2}$ различных транспозиций группы S_n.

Здесь и далее в этом разделе будем рассматривать только такие системы, которые содержат различные транспозиции. Такое ограничение вводится только для простоты счёта и будет подробнее прокомментировано ниже.

Пусть $\mathcal{Y}_L^k$ множество упорядоченных систем транспозиций, которые состоят из k различных транспозиций группы S_n. Количество таких систем обозначим $Y_L^k \triangleq |\mathcal{Y}_L^k|$.

Очевидно, что $Y_L^k = \frac{L!}{(L-k)!}$, числу размещений (без повторений) L транспозиций по k местам. Причем, $(L-k)^k < Y_L^k < L^k$. Заметим, что количество всех таких упорядоченных систем транспозиций равно $\sum\limits_{k=1}^{L} Y_L^k = L! \cdot (\sum\limits_{k=1}^{L} \frac{1}{(N-k)!}) < L! \cdot e$.

Лемма 5. *Пусть известна некоторая УСО размера m. Добавив в эту систему $(k-m)$ транспозиций из оставшихся $(L-m)$, получим УСО размера k. Тогда количество различных УСО, построенных таким образом, равно*

$$a_m^k = \frac{k!}{m!(k-m)!} \cdot \frac{(L-m)!}{(L-k)!} \, , \tag{6}$$

где $m \leqslant k \leqslant L$.

Доказательство. Из $(L-m)$ транспозиций $(k-m)$ упорядоченных неповторяющихся транспозиций можно выбрать $\frac{(L-m)!}{((L-m)-(k-m))!} = \frac{(L-m)!}{(L-k)!}$ способами.

Далее будем размещать $(k-m)$ добавленных транспозиций среди m транспозиций исходной УСО так, чтобы порядки следования транспозиций в каждом из двух множеств не менялись. Это можно сделать $C^m_{m+(k-m)} = \frac{k!}{m!(k-m)!}$ способами.

Число a^k_m равно произведению количества способов выбора $(k-m)$ транспозиций и числа их размещений среди m транспозиций. Что и требовалось доказать.

Следствие 2.

$$a^m_m = 1,\ a^{m+1}_m = (m+1)(L-m),\ a^L_m = \frac{L!}{m!}\,.$$

Следствие 3.

$$a^k_m \geqslant \frac{(k-m+1)^m}{m^m} \cdot (L-k+1)^{k-m}\,.$$

Причем, если выбрать числа $m = m(n)$, $k = k(n)$ *в зависимости от числа* n *такие, что* $1 = o(m(n))$, $m(n) = o(k(n))$, $k(n) = o(L(n))$ *при* $n \to \infty$ [2], *то*

$$a^k_m \gtrsim (k/m)^m\, e^{-m^2/k} \cdot L^{k-m} e^{-k^2/L}\,.\ [3] \tag{7}$$

Обозначим символом $\mathcal{H}^m_m$ множество таких упорядоченных систем образующих размера m, что удаление любой транспозиции из каждой такой УСО лишает ее этого свойства.

Обозначим символом $\mathcal{H}^k_m$, $k > m$, множество упорядоченных систем образующих размера k, полученных добавлением $(k-m)$ транспозиций в каждую из УСО множества $\mathcal{H}^m_m$. Таким образом, все УСО множества $\mathcal{H}^k_m$ построены на основе УСО множества $\mathcal{H}^m_m$ способом, описанным в лемме 5.

Из определения множества $\mathcal{H}^m_m$ следует, что

$$\mathcal{H}^k_k \ \cap\ \mathcal{H}^k_m = \varnothing,\ m < k\,.$$

Количество УСО множеств $\mathcal{H}^m_m$, $\mathcal{H}^k_m$ соответственно обозначим H^m_m, H^k_m.

Утверждение 3. $a^k_m \leqslant H^k_m \leqslant a^k_m \cdot H^m_m$.

Замечание. Знак неравенства возникает из того, что из разных УСО размера m можно получить одну и ту же УСО размера k.

Обозначим символом l_0 такой размер УСО, что $H^{l_0}_{l_0} > 0$ и $H^k_k = 0$ при $k < l_0$.

Пусть $\mathcal{Z}^k_L$ множество упорядоченных систем образующих, которые состоят из k различных транспозиций группы S_n. Количество таких систем обозначим $Z^k_L \triangleq |\mathcal{Z}^k_L|$.

Очевидно, что

$$\mathcal{Z}^k_L = \bigcup_{m=l_0}^{k} \mathcal{H}^k_m\,.$$

[2] $g(n) = o(f(n))$ при $n \to \infty$ обозначает, что $\lim\limits_{n\to\infty} g(n)/f(n) = 0$.

[3] $g(n) \sim o(f(n))$ при $n \to \infty$ обозначает, что $\lim\limits_{n\to\infty} g(n)/f(n) = 1$.

Тогда

$$Z_L^k \geqslant max(H_{l_0}^k, H_{l_0+1}^k, \ldots, H_k^k)\,.$$

Из утверждения 3 и предыдущего неравенства следует, что

$$Z_L^k \geqslant a_m^k, \text{ где } l_0 \leqslant m \leqslant k\,.$$

Это неравенство означает, что если мы умеем строить хотя бы одну УСО размера m, то существует по крайней мере a_m^k УСО размера k, которые можно построить способом, описанным в лемме 5.

Найдём нижнюю границу числа орбит УСО размера k.

В [3] показано, что существуют УСО размера m, где $m(n) \sim n \log_2^2 n$ при $n \to \infty$. Отметим, что $L(n) \sim n^2/2$ при $n \to \infty$. Выберем

$$k(n) \sim n^\alpha \log_2^\beta n \text{ при } n \to \infty, \text{ где } 1 < \alpha < 2, 2 < \beta\,. \tag{8}$$

Легко видеть, что

$$1 = o(m(n)),\ m(n) = o(k(n)),\ k(n) = o(L(n)) \text{ при } n \to \infty. \tag{9}$$

Преобразуем соотношение (7) к виду

$$a_m^k \gtrsim e^{m\left(\ln\left(\frac{k}{m}\right) - \frac{m}{k}\right)} \cdot e^{k\left(\ln L - \frac{m}{k}\ln L - \frac{k}{L}\right)} > e^{1/2\, k \ln L} = L^{k/2}\,, \tag{10}$$

где $\ln\left(\frac{k}{m}\right) > \frac{m}{k}$, $\frac{1}{2}\ln L > \frac{m}{k}\ln L + \frac{k}{L}$ в силу условий (9).

Подставив $L(n)$ и $k(n)$ в неравенство (10), найдём

$$a_m^k \gtrsim (n^2/2)^{1/2\, n^\alpha \log_2^\beta n} > (n/e)^{n \log_2^2 n}\,.$$

Отсюда легко получить нижнюю границу числа орбит УСО размера k, удовлетворяющего соотношению (8). Для этого воспользуемся тем, что орбиты не пересекаются, и согласно утверждению 1 мощность каждой орбиты равна $n!$. Получим, что искомая граница равна по порядку величине $(n/e)^{n \log_2^2 n}/n!$.

Теперь ясно, что сняв ограничение, которое было введено в начале этого параграфа, и допустив возможность повторяемости транспозиций в УСО, мы только бы усилили полученную нижнюю границу.

4. ОЦЕНКА СТОЙКОСТИ КРИПТОСИСТЕМЫ

Перейдем к оценке стойкости криптосистемы, построенной на основе упорядоченной системы образующих. Для этого приведем типы атак, которым теоретически может быть подвергнута такая криптосистема.

Атака *1*. Предположим, что криптоаналитик обладает несколькими, или даже пусть всеми $n!$ шифрованными сообщениями, то есть, ему известно число n. Ничего более о криптосистеме сказать он не сможет. Ведь криптограф может выбрать УСО любого размера r. И криптоаналитику остается только гадать над значением числа r, начиная процесс поиска с нижнего предела $\log_2 n!$ и делая его сколь угодно большим.

Атака *2*. Пусть криптоаналитику повезло, и он перехватил хотя бы одно открытое сообщение. Таким образом, ему стало известно число r. Но тогда согласно оценке (6) криптоаналитику

все равно придется построить как минимум $a^r_{n\log_2^2 n}$ УСО. Что в случае условий (8) является величиной не меньшей, чем $(n/e)^{n\log_2^2 n}$.

Атака *3*. Считаем, что криптоаналитику каким-то образом стала известна УСО Ψ, что возможно, например, после успешной *атаки 2*. Знание УСО по сути эквивалентно знанию множества $\mathcal{M}_\mathcal{P}$ для каждой подстановки $\mathcal{P}$ симметрической группы S_n. Но это все равно не позволяет сказать, какой именно двоичный вектор Γ длины r из множества $\mathcal{M}_\mathcal{P}$ соответствует каждой подстановки $\mathcal{P}$. Воспользуемся тем, что средняя мощностью множества $\mathcal{M}_\mathcal{P}$ равна $2^r/n!$. Тогда число вариантов, которыми можно выбрать $n!$ векторов Γ, составляет $(2^r/n!)^{n!}$. При $r \sim n\log_2^2 n$ объем перебора будет равен

$$\left(n^{n\log_2 n}/n!\right)^{n!} \tag{11}$$

Отсюда следует, что процесс взлома предложенной криптосистемы требует такого объёма вычислений, который экспоненциально зависит от порядка симметрической группы степени n, т.е. от $n!$ Много это или мало?! Авторам неизвестны криптосистемы с такой сложностью взлома. Так или иначе, окончательный ответ может дать только практика, которая издавна считается критерием истины.

Отметим также, что в то время, когда процесс дешифрования требует от криптоаналитика усилий, экспоненциально сложных по $n!$ (11), криптограф и при шифровании, и при расшифровании тратит усилий, величина которых от того же параметра зависит линейно.

5. ЗАКЛЮЧЕНИЕ

В данной статье предложена криптографическая система на основе упорядоченной системы образующих. Её стойкость определяется сложностью решения задач, связанных с УСО. Это задачи поиска орбиты УСО, выбора нужной УСО из неё и выбора подходящего вектора Γ из множества $\mathcal{M}_\mathcal{P}$. Показано, что процесс взлома предложенной криптосистемы требует от криптоаналитика усилий, сложность которых *экспоненциально* зависит от порядка симметрической группы степени n, т.е. от $n!$.

Предложенная тематика может быть источником дальнейших плодотворных постановок задач, связанных с построением новых криптографических систем.

СПИСОК ЛИТЕРАТУРЫ

1. *Калинчук С.А., Сагалович Ю.Л.* Упорядоченная система образующих симметрической группы для решения задач коммутации // Автоматика и телемеханика. 2009. Вып. 2. С. 142–152.

2. *Kalinchuk S.A., Sagalovich Yu.L.* The problem of minimal ordered basis of symmetric group // Proceedings of the Tenth International Workshop “Algebraic and combinatorial coding theory” (ACCT-10), pp. 139-142, September 3-9, 2006, Zvenigorod, Russia.

3. *Kalinchuk S.A., Sagalovich Yu.L.* The least known length of ordered basis of symmetric group // Proceedings of the Eleventh International Workshop “Algebraic and combinatorial coding theory” (ACCT-11), pp. 134-139, June 16-22, 2008, Pamporovo, Bulgaria.