Из графиков видно, что процесс просеивания распараллеливается практически идеально, процесс Гауссова исключения распараллеливается заметно хуже. Это объясняется тем, что при просеивании межпроцессное взаимодействие практически отсутствует (только лишь учёт количества найденных векторов показателей), а при исключении приходится пересылать достаточно много информации (опорная строка).

При нахождении дискретного логарифма важную роль в оптимизации времени вычислений играет такой параметр, как размер базиса. Если размер базиса будет слишком велик, то можно будет легко найти гладкие числа, но достаточно тяжело будет осуществлять проверки на гладкость. Также сильно возрастёт размер матрицы и соответственно время выполнения исключения. Если размер базиса будет слишком мал, то проверка на гладкость и Гауссово исключение будут легко осуществляться, но сложно будет найти достаточное количество гладких чисел.

Также на скорость выполнения вычислений влияют параметры вычислительной системы – количество и производительность процессоров, а главное – передающая среда.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Ростовцев А.Г., Маховенко Е.Б.* Теоретическая криптография. – СПб.: АНО НПО «Профессионал», 2005. – 480 с.

2. *Gordon D.* Discrete Logarithms in GF(p) using the Number Field Sieve //SIAM Journal on Discrete Mathematics. 1993, Vol. 6 p. 124-138.

3. *Weber D.* Computing discrete logarithms with the number field sieve. //Algorithmic Number Theory: Second international Symposium, ANTS-II. Talence, France, May 1996. Processing, Lecture notes in Computer Science. Springer-Verlag, 1996. Vol 1122, p. 391-403.

4. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Изд-во ТРИУМФ, 2003. – 816 с.

УДК 004.056

**Мкртичян В.В.**

## ОБ ЭКСПЕРИМЕНТАЛЬНОМ ИССЛЕДОВАНИИ НАДЕЖНОСТИ И ПРИМЕНЕНИИ СХЕМЫ СПЕЦИАЛЬНОГО ШИРОКОВЕЩАТЕЛЬНОГО ШИФРОВАНИЯ

### 1. Введение и постановка задачи

На практике хорошо известны и широко применяются различные схемы защиты распространяемых данных, использующие криптографическое сокрытие информации и секретное распределение уникальных ключей пользователей [1]. К таким схемам относятся как системы, имеющие аппаратную основу, так и системы, реализованные программно. Отметим, что разработкой этих систем занимаются группы компаний, включающие такие известные фирмы, как IBM, Hitachi, Intel, Matsushita, Sony и Toshiba [2]. К системам первого типа относятся: система защиты телевидения HDTV высокой четкости HDCP, системы защиты CD, DVD-дисков и сменных носителей CPPM и CPRM, система AACS защиты лазерных дисков нового поколения Blu-ray (например, [2]). Примерами систем второго типа являются: система Verimatrix VCAS защиты цифрового интерактивного телевидения IPTV, система DTCP защиты мультимедиа файлов, распространяемых в цифровых сетях, а также программные реализации некоторых из указанных выше аппаратных систем. Отметим, что особенностью систем Verimatrix VCAS и DTCP является тот

факт, что она специализируется не на физических носителях информации, а на цифровых файлах.

В работе [3] представлен перспективный способ защиты легально тиражируемой цифровой продукции от несанкционированного распространения, идея которого получила развитие в работе [4]. В соответствии с [3] будем называть этот способ схемой специального широковещательного шифрования (ССШШ). Эти схемы защиты могут иметь как аппаратную, так и программную реализацию. В [4] замечено, что на ССШШ возможны атаки коалициями легальных пользователей, для борьбы с которыми предлагается основанный на хешировании метод обнаружения членов коалиций. Этот метод является весьма затратным по времени, и в [5] он был улучшен путем применения так называемых следящих кодов с полупереборными декодерами. В [6] доказано, что в качестве следящего кода можно использовать помехоустойчивый обобщенный код Рида-Соломона (ОРС-код), а в качестве декодера – эффективный списочный декодер Гурусвами-Судана [7].

Работы [8] – [12] посвящены различным аспектам разработки компьютерной модели эффективной ССШШ на основе ОРС-кодов и списочного декодера Гурусвами-Судана. Именно в [8] построена математическая модель ССШШ; компьютерная модель списочного декодера Гурусвами-Судана для ОРС-кодов, выступающая наиболее сложным элементом ССШШ, построена в [9], [10]; в [11] представлены программные реализации модели защиты от коалиционных атак и модели самой коалиционной атаки, а в [12] – программная реализация модели распространения данных в ССШШ. Построенная компьютерная модель эффективной ССШШ позволяет гарантированно находить как минимум одного, а иногда и всех членов коалиции злоумышленников, атакующих систему защиты в случае, когда мощность коалиции не превышает некоторого заранее предусмотренного в системе порога. Настоящая статья посвящена экспериментальному исследованию надежности функционирования разработанной компьютерной модели в случае, когда число злоумышленников в коалиции превышает предусмотренный порог, а также некоторым аспектам ее практического применения.

**2. Математическая модель ССШШ**

*Распространение данных в ССШШ.* Рассмотрим ситуацию, когда распространитель предоставляет цифровые данные, доступ к которым должны получать только легальные пользователи. Распространитель разбивает данные на блоки и выбирает шифры $(X',K',Y',E',D')$ и $(X,K,Y,E,D)$ для защиты блоков и блоковых ключей соответственно. Очередной блок $M\in X'$ зашифровывается на ключе $s\in K'$: $e'=E'_s(M)$. Ключу $s$ по специальному правилу разделения секрета $\sigma$ сопоставляется вектор $\sigma(s)=(s_1,\ldots,s_r)\in X'^r$. Далее $\sigma^{(-1)}$ – правило восстановления секрета: $s=\sigma^{(-1)}(s_1,\ldots,s_r)$. Каждая координата $s_i$ зашифровывается на $q$ частичных ключах $\{k_{i,1},\ldots,k_{i,q}\}\subseteq K$: $e_{i,1}=E_{k_{i,1}}(s_i),\ldots,e_{i,q}=E_{k_{i,q}}(s_i)$, составляющих вектор разрешенных ключей $\Lambda_i=(k_{i,1},\ldots,k_{i,q})$ для $s_i$. Шифрограммы $e'$ и $Y_0=(e_{i,j})_{i\in\{1;\ldots;r\},j\in\{1;\ldots;q\}}$ распространитель передает по открытому каналу, а ключи $\{k_{i,j}\}$ хранит в секрете. Каждому легальному пользователю $u$ распространитель выдает уникальный вектор-номер $J_u=(j_1,\ldots,j_r)$, где $j_1,\ldots,j_r\in\{1;\ldots;q\}$ и вектор-ключ $K_u=(\kappa_1,\ldots,\kappa_r)=(k_{1,j_1},\ldots,k_{r,j_r})$. Будем полагать, что множество $S$ всевозможных вектор-номеров пользователей ССШШ совпадает с образом некоторого кода $C$ при отображении $\lambda$: $C\to S$. Далее для простоты вектор-номера и их кодовые представления мы различать не будем. Пользователь $u$, получив шифрограммы $e'$, $Y_0$ и имея в вектор-ключе $K_u$ ключ $\kappa_i$ из каждого $\Lambda_i$, может расшифровать каждую часть блокового ключа:

$$D_{\kappa_i}(e_{i,j_i}) = D_{k_{i,j_i}}(E_{k_{i,j_i}}(s_i)) = s_i,\ i=\{1;...;r\},$$

восстановить $s = \sigma^{(-1)}(s_1,\ldots,s_r)$ и расшифровать блок данных $D'_s(e')=D'_s(E'_s(M)) = M$.

*Коалиционные атаки на ССШШ.* Пусть $\mathbf{N}$ – множество натуральных чисел, $\mathbf{N}_1=\mathbf{N}\backslash\{1\}$, $F_q^r$ – линейное $r$-мерное пространство Хемминга над полем Галуа $F_q$, $S\subseteq F_q^r$ – линейный код. Множеством $c$-коалиций $\mathrm{coal}_c(S)$ кода $S$, где $c\in\mathbf{N}$, назовем множество его непустых подмножеств мощности не более $c$. Множеством вектор-ключей коалиции $C_0\in\mathrm{coal}_c(S)$ назовем $K(C_0)=\{(k_{1,j_1},\ldots,k_{r,j_r})\in K^r:(j_1,\ldots,j_r)\in C_0\}$. Множество $i$-х координат вектор-номеров коалиции $C_0$ обозначим $C_{0,i}$. Множеством потомков коалиции $C_0$ и множеством $c$-потомков кода $S$ назовем

$$\mathrm{desc}(C_0)=\{w\in F_q^r:\ \forall i\in\{1;\ldots;r\}\ w_i\in C_{0,i}\},\ \mathrm{desc}_c(S) = \bigcup_{C_i\in coal_c(S)}\mathrm{desc}(C_i)$$

соответственно. Пиратским вектор-номером коалиции $C_0\in\mathrm{coal}_c(S)$ назовем элемент $\mathrm{desc}(C_0)\backslash C_0$. По коалиции $C_0$ и множеству $K(C_0)$ можно строить пары пиратских вектор-номеров и вектор-ключей, подходящие к расшифрованию.

*Защита от коалиционных атак на ССШШ.* Пусть $d(x,y)=r-|I(x,y)|$ – метрика Хемминга в $F_q^r$; $B(x,\rho)=\{z\in F_q^r|\ d(x,z)\le\rho\}$ – замкнутый шар с центром в точке $x$ радиуса $\rho$; $d(x,Y)$ – расстояние от $x\in F_q^r$ до множества $Y\subseteq F_q^r$. Для защиты от атак коалиций мощности не более $c(\in\mathbf{N}_1)$ в схеме распространения данных в качестве кода $C$ можно использовать произвольный линейный код с таким минимальным расстоянием $d$ и длиной $r$, что выполняется условие

$$d > r - r/c^2 \qquad (1)$$

([5], теорема 4.4). Пусть $r_0 := r - r/c$, $w\in\mathrm{desc}_c(C)$. Из раздела 2 работы [6] следует, что $\varnothing \ne B(w,r_0)\cap C \subseteq C_0$.

Напомним, что линейный код длины $r$, размерности $k$ с минимальным расстоянием $d$ называется МДР $(r,k)$-кодом, если в неравенстве Синглтона $d \le r - k + 1$ достигается равенство $d = r - k + 1$ ([13], С. 60). Учитывая последнее равенство и целочисленность величины $c$, для МДР $(r,k)$-кода неравенство (1) можно преобразовать к виду

$$c \le B_0(C) := \lceil (r/(k\text{-}1))^{1/2} \rceil - 1. \qquad (2)$$

Таким образом, для защиты от коалиционных атак контролеру достаточно применять следующий порядок действий при обнаружении пиратского вектор-номера $w$: найти все кодовые слова шара с центром в $w$ радиуса $r_0$ и использовать полученный список как список легальных вектор-номеров из коалиции. Для решения этой задачи используют переборные декодеры, так как в общем случае эффективных алгоритмов поиска элементов множества $B(w,r_0)\cap C$ не существует [13].

Защиту от коалиционных атак на ССШШ можно сделать эффективной, применив в схеме распространения данных ОРС-коды и методы списочного декодирования. Входными параметрами имеющего полиномиальную сложность алгоритма списочного декодирования Гурусвами-Судана (АСДГС) являются длина $r$ и размерность $k$ обобщенного кода Рида-Соломона ($(r,k)$-ОРС-кода) и параметр

$t(\in\{\lfloor(r(k\text{-}1))^{1/2}+1\rfloor;\ldots;r\})$ [5]. При декодировании на вход подается вектор $x\in F_q^r$, и АСДГС находит все $v\in C$ в шаре $B(x, r–t)$. Пусть $C$ – $(r,k)$-ОРС-код над полем $F_q$; $c(\in\mathbf{N}_1)$ – величина, не превышающая порога $B_0(C)$, $r_{00}=\lfloor r\text{-}(r(k\text{-}1))^{1/2}\rfloor$. Из раздела 3 работы [6] следует, что, во-первых:

$$\forall C_0\in\mathrm{coal}_c(C)\ \forall w\in\mathrm{desc}(C_0)\colon \varnothing\neq B(w,r_{00})\cap C\subseteq C_0,$$

во-вторых, если $r>\log_2 q$, и в качестве значения параметра $t$ АСДГС выбрать $\lceil r/c\rceil$, то радиус работы АСДГС достигнет $r_{00}$. Для эффективной защиты от коалиционных атак определим следующий порядок действий контролера при обнаружении пиратского вектор-номера $w$: подать $w$ на вход АСДГС с управляющим параметром $t=\lceil r/c\rceil$ и получить на выходе список легальных вектор-номеров из коалиции.

*Теоретические границы применимости ССШШ в случае превышения допустимого числа злоумышленников.* Выше отмечено, что условие (2) является необходимым для корректной работы эффективной ССШШ. Приведем классификацию различных случаев его нарушения. Пусть $C$ – $(r,k)$-ОРС-код, $r_{00}=\lfloor r–(r(k\text{-}1))^{1/2}\rfloor$. Рассмотрим множества $\Omega_i$, называемые областями компрометации кода $C$. Пусть

$$\Omega_1(C)=\{c\in\mathbf{N}_1\colon \exists v\in C\ \exists C_0\in\mathrm{coal}_c(C\backslash\{v\})\ \exists w\in\mathrm{desc}(C_0)\backslash C_0\colon d(v,w)\le r_{00}\}.$$

Область $\Omega_1(C)$ кода $C$ это множество мощностей таких коалиций, у которых имеется возможность компрометации невиновного пользователя в результате применения списочного декодера Гурусвами-Судана к потомку коалиции. Теперь рассмотрим произвольный линейный код $C$. Пусть

$$\Omega_2(C)=\{c\in\mathbf{N}_1\colon \exists v\in C\ \exists C_0\in\mathrm{coal}_c(C\backslash\{v\})\ \exists w\in\mathrm{desc}(C_0)\backslash C_0\ \forall u\in C_0\colon d(v,w)\le d(w,u)\}\ .$$

Область $\Omega_2(C)$ кода $C$ есть множество мощностей таких коалиций, при которых для некоторого кодового слова $v$ существует коалиция $C_0$, у которой хотя бы один из потомков расположен не далее от $v$, чем от любого элемента $C_0$. Пусть

$$\Omega_3(C)=\{c\in\mathbf{N}_1\colon \exists v\in C\ \exists C_0\in\mathrm{coal}_c(C\backslash\{v\})\colon v\in\mathrm{desc}(C_0)\backslash C_0\}.$$

Область $\Omega_3(C)$ кода $C$ это множество мощностей таких коалиций, при которых для некоторого кодового слова $v$ существует коалиция, у которой $v$ является потомком.

Очевидно, $\Omega_i(C)$ – целочисленный отрезок вида $\Omega_i(C)=\{R_i(C);\ldots;|C|\}$, где $R_i(C)$ – величина, называемая рубежом областей компрометации $\Omega_i(C)$. Непосредственно из определений вытекает справедливость вложения $\Omega_3(C)\subseteq\Omega_2(C)$, а вложение $\Omega_2(C)\subseteq\Omega_1(C)$ является следствием сформулированной ниже теоремы 2.

Пусть $C$ – произвольный код длины $r$, размерности $k$, $B_1(C) = B_0(C) + 1 = \lceil(r/(k\text{-}1))^{1/2}\rceil$, $B_2(C)=\lceil(r+k\text{-}1)/(2(k\text{-}1))\rceil$, $B_3(C)=\lceil r/(k\text{-}1)\rceil$. Нетрудно показать, что $2\le B_1(C)\le B_2(C)\le B_3(C)$. При этом равенство $B_1(C)=B_2(C)$ выполняется тогда и только тогда, когда $r\le 3(k\text{-}1)$, а равенство $B_2(C)=B_3(C)$ выполняется тогда и только тогда, когда $r\le 2(k\text{-}1)$. В работе [14] анонсированы следующие теоремы:

**Теорема 1.** Пусть $C$ – МДР-код длины $r$ и размерности $k$. Тогда $B_1(C)\le R_2(C)$, $B_3(C)\le R_3(C)$.

**Теорема 2.** Пусть $C$ – $(r,k)$ – ОРС-код. Тогда $R_1(C) = B_1(C)\le R_2(C)\le B_2(C)\le R_3(C) = B_3(C)$.

**3. Эксперименты по исследованию надежности ССШШ**

Пусть $c \geq 2$ – натуральное число, $C$ – $(r,k)$ – ОРС-код, $C_0$ – случайно выбранная из кода $C$ коалиция мощности не более $c$, $w$ – случайно выбранный потомок $C_0$. Рассмотрим следующие события: 1) $A_1$: в результате применения списочного декодера Гурусвами-Судана к потомку $w$ произошла компрометация некоторого невиновного пользователя с вектор-номером $v \in C \setminus C_0$; 2) $A_2$: ближайшим к потомку $w$ является вектор-номер $v \in C \setminus C_0$ некоторого невиновного пользователя; 3) $A_3$: самим потомком $w$ является вектор-номер $v \in C \setminus C_0$ некоторого невиновного пользователя. Нетрудно видеть, что: $A_3 \supseteq A_2 \supseteq A_1$. Отметим, что если произошло событие $A_i$, то $c \in \Omega_i(C)$.

На основе применения программных реализаций моделей коалиционной атаки и защиты от коалиционных атак, полученных в [11], и компьютерной модели списочного декодера Гурусвами-Судана для ОРС-кодов, полученной в [9], [10], построена информационная система (ИС) исследования надежности функционирования ССШШ в случае, когда число злоумышленников в коалиции превышает порог, предусмотренный системой защиты.

Рассмотрим кратко схему проведения экспериментов:

– выбрать $(r,k)$ – ОРС-код $C$ и вычислить для него $B_1(C)$ и $B_3(C)$;

– положить $c$ равным $B_1(C)$, выбрать случайным образом $c$ элементов $F_q^r$, закодировать их и получить случайную коалицию $C_0$; выбрать случайным образом потомка $w$ коалиции $C_0$;

– если $c \geq B_3(C)$, то проверить условие $w \in C \setminus C_0$ вычислением синдрома для $w$; если $w \in C \setminus C_0$, то зафиксировать событие $A_3$, в противном случае продолжить;

– подать $w$ на вход АСДГС с управляющим параметром $t = \lceil r/(B_1(C)-1) \rceil$, получить на выходе список $L \subseteq C$;

– если $L \subseteq C_0$, то зафиксировать, что события $A_1$, $A_2$, $A_3$ не произошли; в противном случае продолжить;

– если $d(w, L \setminus C_0) \leq d(w, C_0)$, то зафиксировать событие $A_2$; в противном случае зафиксировать событие $A_1$.

Эти эксперименты для величины $c$ повторяются заданное количество раз. Затем в цикле значение $c$ увеличивается на единицу, и эксперименты повторяются до тех пор, пока не выполнится условие: $c > r$.

Приведем экспериментальные результаты для (19,3) – ОРС-кода $C^1$ и (101,2) – ОРС-кода $C^2$. Для каждого кода при каждом фиксированном целом $c (\in [B_1(C^i), r])$ проведено 40 000 экспериментов и зафиксированы частоты появлений событий $A_1$, $A_2$, $A_3$. Отметим, что согласно [15] можно вычислить количество экспериментов, необходимое для того, чтобы по частоте оценить вероятность появления событий $A_i$ с заданной точностью оценки $\delta$ и доверительной вероятностью $p_\alpha$: $n$=38 416 для $\delta$=0,005, $p_\alpha$=0,95. Таким образом, проведенного количества экспериментов достаточно, чтобы для кодов $C^1$ и $C^2$ дать оценки $p(A_i,c)$ вероятностей появления событий $A_1$, $A_2$, $A_3$ для каждого значения величины $c \geq B_1(C^i)$.

В табл. 1 содержатся полученные оценки $p(A_1,c)$ и $p(A_2,c)$ для кода $C^1$ с указанием приведенных в теореме 1 границ областей компрометации.

Для кода $C^2$ получены результаты для всех значений величины $c \geq B_1(C^2)=11$. Оценки $p(A_1,c)$ равны нулю для всех значений $c \in \{11;\ldots;101\}$. Оценки $p(A_2,c)$ для $c \in \{11; 51; 61; 69; 75; 78; 83; 85; 89; 94; 95; 98; 101\}$ равны $2{,}5 \cdot 10^{-5}$, для $c$=99 составляет $5 \cdot 10^{-4}$, а для других значений $c \in \{11;\ldots;101\}$ оценки $p(A_2,c)$ равны нулю.

Оценки $p(A_3,c)$ для кода $C^1$ при $c \in \{10;\ldots;19\}$ и для кода $C^2$ при $c = B_3(C^2)=101$ равны нулю по результатам экспериментов. Вероятности появления события $A_3$

для кода $C^1$ при $c \in \{4;\ldots;9\}$ и для кода $C^2$ при $c \in \{11;\ldots;100\}$ равны нулю в силу того, что по теореме 1 граница $B_3(C)$ является рубежом $\Omega_3(C)$. Из наличия ненулевых оценок $p(A_2,c)$ для $C^1$ при $c<6$ следует, что $B_2(C)$ не является рубежом $\Omega_2(C)$.

Таблица 1

Оценки вероятностей событий $A_1$, $A_2$ для кода $C^1$ при нарушении необходимого условия корректной работы ССШШ

| *Код* $C^1$, $c$ | $4 = B_1(C^1)$ | 5 | $6 = B_2(C^1)$ | 7 | 8 | 9 | $10=B_3(C^1)$ | 11 |
|---|---|---|---|---|---|---|---|---|
| $p(A_1,c)$ | 0,015 | 0,014 | 0,01 | 0,008 | 0,007 | 0,004 | 0,002 | 0,002 |
| $p(A_2,c)$ | 0,027 | 0,063 | 0,095 | 0,118 | 0,137 | 0,144 | 0,16 | 0,165 |
| *Код* $C^1$, $c$ | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 |
| $p(A_1,c)$ | 0,002 | 0,002 | 0,001 | 0,001 | 0,001 | 0 | 0 | 0,001 |
| $p(A_2,c)$ | 0,168 | 0,172 | 0,173 | 0,174 | 0,176 | 0,176 | 0,178 | 0,184 |

Рассмотрим график зависимости оценок вероятности $p$ событий $A_1$, $A_2$ от величины $c$ при нарушении необходимого условия (2) корректной работы ССШШ.

Напомним, что событие $A_2$ отличается от $A_1$ тем, что в случае его возникновения потомок коалиции не просто попадает в шар радиуса $r_{00}=\lfloor r-(r(k-1))^{1/2} \rfloor$ с центром в кодовом слове, не принадлежащем коалиции, а оказывается ближе к кодовому слову не из коалиции. Отметим, что возможной причиной сокращения оценки $p(A_1,c)$ и роста $p(A_1,c)$ с увеличением $c$ является рост доли таких удаленных от коалиции потомков в общем числе потомков.

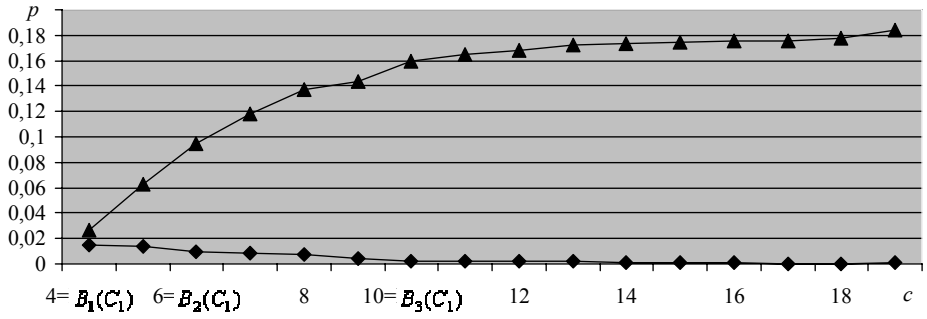


*Рис. 1. Зависимость оценок вероятности событий $A_1$, $A_2$ от мощности коалиции для (19,3)-ОРС-кода: —◆— - $p(A_3,c)$, —▲— - $p(A_3,c)$*

Эксперименты проведены на сорока компьютерах, с процессорами мощностью 2,5 ГГц и ОЗУ объемом 512 Мб в течение 10 часов. В силу того, что рассмотренные события $A_1$, $A_2$, $A_3$ соответствуют трем различным случаям компрометации коалициями невиновного пользователя, полученные результаты позволяют оценить вероятность каждого такого случая для (19,3)-ОРС-кода и (101,2)-ОРС-кода при каждом значении мощности коалиции, превышающем допустимое число злоумышленников.

**4. Применение ССШШ**

Перспективным применением ССШШ представляется защита программного обеспечения, предполагающего наличие обновляемых баз данных (ПООБД). Примерами ПООБД являются программы, предоставляющие базы правовой информации, и антивирусные программы. Договор, заключаемый между распространителем и пользователем ПООБД, может предполагать не периодическую оплату за его использование, а разовую оплату ПООБД, накопившейся у распространителя

на момент заключения договора базы, и дальнейшую периодическую оплату выходящих обновлений. Защита периодических обновлений может быть организована с помощью ССШШ.

Рассмотрим схему защиты периодических обновлений ПООБД на базе программной реализации ССШШ. Эта реализация, основанная на описанной выше математической модели, построена под операционные системы Windows 95/98/NT/2000/XP/Vista и представлена в работах [10]–[12]. Она состоит из следующих основных элементов: программное обеспечение распространителя данных ССШШ [12], программное обеспечение пользователя ССШШ [12], программное обеспечение контролера [10], [11]. Поставщику ССШШ необходимо передать по открытому каналу распространителю данных ПО распространителя данных ССШШ, а контролеру – ПО контролера. В тот момент, когда новый подписчик приобретает ПООБД, накопившуюся базу данных и доступ к обновлениям базы, распространитель должен сделать следующее: передать подписчику ПООБД и ПО пользователя ССШШ по открытому каналу; сгенерировать при помощи ПО распространителя вектор-номер и вектор-ключ пользователя; передать подписчику эту пару векторов и накопившуюся базу данных по гарантированно защищенному каналу. При выходе очередных обновлений баз распространитель должен защитить их при помощи ПО распространителя, и передать соответствующие шифрограммы по открытому каналу подписчикам. При получении шифрограмм обновлений баз подписчик должен расшифровать обновления, применив ПО пользователя с вектор-ключем и вектор-номером пользователя, а затем активировать обновления в ПООБД. Теперь рассмотрим действия контролера в случае коалиционных атак на схему защиты периодических обновлений ПООБД. При обнаружении нелегального распространения пиратского вектор-номера и соответствующего ему вектор-ключа, контролеру необходимо подать пиратский вектор-номер на вход ПО контролера и на выходе получить список вектор-номеров злоумышленников, построивших эту пару.

Другим областью применения ССШШ могут выступать новостные сайты с платным доступом. С помощью ССШШ на таких сайтах может быть организована защита файлов любого типа, содержащих новости. Для реализации защиты можно использовать разработанное в [10] – [12] ПО, при этом необходимо выполнить действия, аналогичные описанным выше действиям по защите систем, предполагающих наличие обновляемых баз данных.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Rosenblatt W.*, *Mooney S.*, *Trippe W.* Digital Rights Management: Business and Technology. New York: Hungry Minds/John Wiley&Sons. 2002. 312 p.

2. Официальный сайт группы компаний 4centity: http://www.4centity.com.

3. *Berkovits S.* How to Broadcast a Secret. In Advances in Cryptology - EUROCRYPT ’91 (LNCS 547). 1991. P. 535-541.

4. *Chor B.*, *Fiat A.*, *Naor M.* Tracing Traitors. In Advances in Cryptology - Crypto ’94 (LNCS 839). 1999. P. 257-270.

5. *Staddon J.N.*, *Stinson D.R.*, *Wei R.* Combinatorial properties of frameproof and traceability codes. // IEEE Trans. Inf. Theory. 2001. V. 47. P. 1042-1049.

6. *Silverberg A.*, *Staddon J.*, *Walker J.* Application of list decoding to tracing traitors. //IEEE Trans. Inf. Theory, 2003. V. 4. P. 1312-1318.

7. *Guruswami V.*, *Sudan M.* Improved decoding of Reed-Solomon and algebraic-geometric codes. // IEEE Trans. Inf. Theory, 1999. V. 45. P. 755-764.

8. *Деундяк В.М.*, *Мкртичян В.В.* Математическая модель эффективной схемы специального широковещательного шифрования. В сб. “Труды VI школы-семинара “Математическое моделирование, вычислительная механика и геофизика. Ростов-на-Дону. 2007”. – Ростов-на-Дону: ЦВВР, 2008. С. 87-89.

9. *Мкртичян В.В.* Компьютерные модели списочных декодеров Гурусвами-Судана для обобщенных кодов Рида-Соломона и конкатенированных кодов // Вестник ДГТУ, 2007. Т.7. №4. – С. 384-394.

10. *Мкртичян В.В.* Особенности реализации программных модулей списочных декодеров Гурусвами-Судана в компьютерной модели схемы специального широковещательного шифрования. В сб. "Интегро-дифференциальные операторы и их приложения." Вып. 8. – Ростов-на-Дону, 2008. – С. 104-116.

11. *Мкртичян В.В.* О программной реализации моделей коалиционной атаки и защиты от коалиционных атак схемы специального широковещательного шифрования. В сб. " Интегро-дифференциальные операторы и их приложения." Вып. 8. – Ростов-на-Дону, 2008. – С. 94-103.

12. *Евпак С.А.*, *Мкртичян В.В.* Особенности программной реализации модели распространения данных схемы специального широковещательного шифрования. В сб. " Интегро-дифференциальные операторы и их приложения." Вып. 8. – Ростов-на-Дону, 2008. – С. 61-71.

13. *Влэдуц С.Г.*, *Ногин Д.Ю.*, *Цфасман М.А.* Алгеброгеометрические коды. Основные понятия. – М.: МЦНМО, 2003. – 504 с.

14. *Мак-Вильямс Ф.Д.*, *Слоэн Н.Дж.* Теория кодов, исправляющих ошибки. – М.: Связь, 1979. – 744 с.

15. *Деундяк В.М.*, *Мкртичян В.В.* Исследование границ применения одной схемы защиты данных. В сб. "Труды участников международной школы-семинара по геометрии и анализу". – Ростов-на-Дону: ЮФУ, 2008.

16. *Чистяков В.П.* Курс теории вероятностей. – М.: Наука, 1982. – 256 с.

УДК 681.03.245

**Е.А. Ищукова**

## ИССЛЕДОВАНИЕ ВЛИЯНИЯ БЛОКОВ ЗАМЕНЫ НА УСТОЙЧИВОСТЬ АЛГОРИТМОВ ШИФРОВАНИЯ*

За последние два десятилетия совершен большой скачок в развитии компьютерной техники. Чтобы убедиться в этом, достаточно сравнить вычислительные мощности, которые были доступны обычному пользователю 20 лет назад и сейчас. Такое бурное развитие компьютерной техники повлекло за собой стремительное развитие других наук так или иначе связанных с вычислительными задачами. Можно сказать, что наибольшее влияние было оказано на криптографию, так как пока не было вычислительно мощных систем задачи криптографии в основном сводились к различного рода головоломкам и использовали в своей основе различные шифры замен и подстановок. Однако в конце XX века вместе с ростом вычислительных ресурсов начала развиваться и криптография. Появились принципиально новые подходы к построению схем шифрования. Широкое развитие получила симметричная криптография в связи с принятием в конце 70-х годов прошлого века в качестве государственного стандарта шифрования данных США алгоритма DES. Также был найден новый подход для шифрования данных, легший в основу асимметричных алгоритмов шифрования.

Вместе с развитием криптографии, то есть вместе с появлением все новых и новых алгоритмов шифрования появилась и необходимость выявления методов их надежности. То есть необходимо было выяснить, насколько использование того

* Работа выполнена при поддержке гранта РФФИ №06-07-89010-а