

УДК 004.056.5

ИССЛЕДОВАНИЕ ГРАНИЦ ПРИМЕНЕНИЯ СХЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ОСНОВАННОЙ НА РС-КОДАХ

В. М. Деундяк, В. В. Мкртичян

Аннотация. Рассматривается вопрос о защите легально тиражируемой цифровой продукции от несанкционированного распространения. Построена математическая модель схемы специального ширококвещательного шифрования на основе кодов Рида — Соломона и декодера Гурусвами — Судана. Проведено исследование возможности её применения в случае превышения пороговой мощности коалиции злоумышленников.

Ключевые слова: обобщённый код Рида — Соломона, списочное декодирование, ширококвещательное шифрование, коалиционная атака.

Введение

При решении ряда актуальных проблем защиты информации от несанкционированного доступа в последние годы интенсивно применяется теория помехоустойчивого кодирования и, в частности, современные методы списочного декодирования [6, 10]. Представляет интерес применение этой теории в задаче защиты легально тиражируемой цифровой продукции от несанкционированного копирования. В [9] рассмотрен некоторый перспективный способ такой защиты, называемый там схемой специального ширококвещательного шифрования (ССШШ). Согласно [9] защищаемые данные тиражируются свободно в зашифрованном виде, а каждому легальному пользователю выдаётся уникальный набор ключей, причём в случае обнаружения нелегального использования такого набора его хозяин может быть идентифицирован контролёром. ССШШ допускает атаки следующего вида: злоумышленники, являющиеся легальными пользователями, могут объединяться в коалиции мощности s и, комбинируя специальным образом ключи из своих наборов, конструировать новые (пиратские) наборы, которые можно использовать для

расшифрования данных, причём эти пиратские наборы злоумышленники могут нелегально распространять, уклоняясь от обнаружения. Для борьбы с такими коалиционными атаками предложен основанный на хешировании метод обнаружения членов коалиций, который, однако, является весьма затратным по времени, так как использует переборные алгоритмы.

В [2, 8, 11, 12] найдено значительное усиление ССШШ, содержащее теоретические результаты о возможности применения в ССШШ некоторых классов помехоустойчивых кодов и быстрых методов списочного декодирования. Целесообразность применения помехоустойчивого кодирования связана с тем, что пиратские наборы можно рассматривать как результат «запумления» легальных наборов. Идея применения списочных декодеров в ССШШ состоит в том, что, во-первых, ввиду большой степени запумлённости обычные детерминированные декодеры не срабатывают, а во-вторых, на выходе списочный декодер способен генерировать список, содержащий не только одного, но нескольких злоумышленников, а при выполнении ряда условий — вообще всех.

В [11] доказано, что для возможности эффективного поиска всей коалиции мощности $s \geq 2$ или, по крайней мере, её непустого подмножества, можно применять обобщённые коды Рида — Соломона (ОРС-коды) и списочный декодер Гурусвами — Судана с параметрами, зависящими от величины s , которая предполагается известной. Вопрос о степени защищённости ССШШ с такими параметрами от атак коалиций мощности, превышающей предусмотренный порог, ранее не рассматривался и представляется с практической точки зрения весьма актуальным. Дело в том, что в случае превышения мощностью коалиции предусмотренного порога система обнаружения коалиции злоумышленников может дать сбой и контролёр посчитает данные невиновного пользователя данными злоумышленника, т. е. система может осуществить компрометацию невиновного пользователя.

В нашей статье исследованы условия применения ССШШ, основанной на кодах Рида — Соломона и списочном декодере Гурусвами — Судана, в случае превышения мощности коалиции s порога. С этой целью построена иерархия множеств компрометации легальных пользователей и доказаны соответствующие оценки для s (разд. 2, 3), позволяющие определить степень компрометации невиновных пользователей в ходе проверки контролёром. Вспомогательный разд. 1 посвящён построению для рассматриваемой схемы защиты информации математической модели, с помощью которой проведено указанное исследование. Полученные

теоретические результаты частично анонсированы в [1], программной реализации математической модели ССШШ посвящены работы [3, 4].

1. Математическая модель ССШШ

Элементами математической модели ССШШ являются: математическая модель распространения данных (п. 1.1), математическая модель коалиционной атаки (п. 1.2) и математическая модель эффективной защиты от коалиционных атак (п. 1.4). Основой для модели ССШШ являются помехоустойчивые коды Рида — Соломона и списочный декодер Гурусвами — Судана, необходимые сведения о которых содержатся в п. 1.3.

1.1. Математическая модель распространения данных. Напомним, что под шифром понимается пятёрка (X, K, Y, E, D) , где X, K, Y — множества всевозможных открытых текстов, ключей и шифртекстов соответственно, $E = \{E_k\}_{k \in K}$ — множество правил шифрования $E_k : X \rightarrow Y$, $E_k(X)$ — множество всех шифрограмм на ключе k , $D = \{D_k\}_{k \in K}$ — множество правил расшифрования $D_k, E_k(X) \rightarrow X$. При этом предполагается, что $Y = \bigcup_{k \in K} E_k(X)$ и $D_k(E_k(x)) = x$ для

всех $x \in X$, $k \in K$. Для множества A через A^b , где b — натуральное число, обозначим b -кратное декартово произведение множества A на себя.

В математической модели распространения данных ССШШ с N возможными пользователями предполагается, что поставщик цифровой продукции разбивает защищаемые тиражируемые данные на блоки и выбирает два базовых шифра (X', K', Y', E', D') и (X, K, Y, E, D) для защиты блоков и блоковых ключей соответственно. Далее выбираются натуральное число r , степень q некоторого простого числа и код S из линейного r -мерного пространства Хемминга \mathbb{F}_q^r над полем $\mathbb{F}_q = \{\alpha_1, \dots, \alpha_q\}$ такие, что $qr < |K|$, $N < |S| < q^r$. (Здесь и далее мощность произвольного конечного множества A будем обозначать через $|A|$.) Отметим, что в силу того, что величины $|K|$ для современных шифросистем достаточно велики, легко выбрать q и r , удовлетворяющие не только второй, но и первой оценке. Для каждого $i \in \{1, \dots, r\}$ поставщик выбирает вектор различных ключей $(k_{i,j})_{j \in \mathbb{F}_q} \in K^r$ и формирует упорядоченный набор из r векторов разрешённых ключей в виде матрицы: $\Lambda = (k_{i,j})_{i \in \{1, \dots, r\}, j \in \mathbb{F}_q}$, при этом полагается, что на поле \mathbb{F}_q введён линейный порядок. Матрицу Λ поставщик хранит в секрете.

Каждому легальному пользователю u поставщик данных выдаёт уникальный вектор $J_u = (j_1, \dots, j_r) \in S$, называемый *вектор-номером* поль-

зователя, и соответствующий ему уникальный упорядоченный набор частичных ключей $K_u = (\kappa_1, \dots, \kappa_r)$, где $\kappa_i = k_{i,j_i}$, называемый *вектор-ключом* пользователя.

Рассмотрим действия поставщика по передаче данных. Очередной блок $M \in X'$ поставщик шифрует на блоковом ключе $s \in K'$ с помощью правила шифрования $E'_s : e' = E'_s(M)$. Затем ключ s преобразуется согласно одной из схем разделения секрета, имеющих возможность разделения ключа s на r частей (различные схемы разделения секрета содержатся, например, в разд. 3.7 [7]). Именно, в соответствии с выбранной схемой ключу s по правилу разделения секрета сопоставляется вектор $\sigma(s) = (s_1, \dots, s_r) \in X^r$, каждая из координат которого необходима для восстановления s , причём по вектору (s_1, \dots, s_r) ключ s вычисляется с помощью правила восстановления секрета: $s = \sigma^{(-1)}(s_1, \dots, s_r)$. Далее каждая координата s_i шифруется на элементах i -го вектора разрешённых ключей из матрицы Λ по правилам

$$e_{i,1} = E_{k_{i,1}}(s_i), \dots, e_{i,q} = E_{k_{i,q}}(s_i).$$

Шифрограммы e' и $Y_0 = (e_{i,j})_{i \in \{1, \dots, r\}, j \in \{1, \dots, q\}}$ поставщик передаёт пользователям по открытому каналу.

Имеющаяся у легального пользователя u ключевая пара J_u, K_u обеспечивает ему доступ к защищённым данным, который реализует следующий

АЛГОРИТМ 1

ШАГ 1. Расшифровать части блокового ключа:

$$D_{\kappa_i}(e_{i,j_i}) = D_{\kappa_{i,j_i}}(E_{\kappa_{i,j_i}}(s_i)) = s_i \quad (i \in \{1; \dots; r\}).$$

ШАГ 2. Вычислить блоковый ключ $s = \sigma^{(-1)}(s_1, \dots, s_r)$.

ШАГ 3. Расшифровать блок защищённых данных

$$D'_s(e') = D'_s(E'_s(M)) = M.$$

В случае несанкционированного распространения пользователем u своей ключевой пары J_u, K_u он может быть по базе идентифицирован контролёром ввиду уникальности этой пары. Отметим также, что в матрице Λ следует избегать повторов элементов, чтобы противостоять переборным атакам на ключ пользователя.

1.2. Математическая модель коалиционной атаки. Являющиеся легальными пользователями злоумышленники могут объединяться в

коалиции с целью генерации новых (пиратских) ключевых пар, подходящих для доступа к защищённым данным. При этом коалиции могут нелегально распространять сгенерированные пиратские ключевые пары без боязни быть выявленными по базе. Рассмотрим математическую модель таких коалиционных атак.

Пусть \mathbb{N} — множество натуральных чисел, $\mathbb{N}_1 = \mathbb{N} \setminus \{1\}$. Непустое подмножество C_0 кода $S(\subseteq \mathbb{F}_q^r)$ назовём *c-коалицией*, если $|C_0| \leq c$. Пусть $\text{coal}_c(S)$ — множество всех *c-коалиций*. Зафиксируем линейный код $S \subseteq \mathbb{F}_q^r$, и пусть $C_0 \in \text{coal}_c(S)$. Через

$$K(C_0) = \{(k_{1,j_1}, \dots, k_{r,j_r}) \in K^r : (j_1, \dots, j_r) \in C_0\}$$

обозначим множество вектор-ключей, соответствующих элементам коалиции C_0 , а через $C_{0,i}$ — множество *i-х* координат вектор-номеров её элементов. Вектор $w = (w_1, \dots, w_r) \in \mathbb{F}_q^r$ будем называть *потомком коалиции* C_0 , если $w_i \in C_{0,i}$ для всех i . В этом случае будем говорить, что C_0 — коалиция, создающая потомка w . Пусть $\text{desc}(C_0)$ — множество всех потомков коалиции C_0 . Векторы из $\text{desc}(C_0)$, не содержащиеся в C_0 , будем называть *пиратскими вектор-номерами коалиции* C_0 . Пусть

$$\text{desc}_c(S) = \bigcup_{C_i \in \text{coal}_c(S)} \text{desc}(C_i).$$

Ясно, что

$$S = \text{desc}_1(S) \subseteq \text{desc}_2(S) \subseteq \text{desc}_3(S) \subseteq \dots \subseteq \text{desc}_{|S|}(S) \subseteq \mathbb{F}_q^r.$$

Математическую модель коалиционной атаки описывает

Лемма 1. Для произвольных $c \in \mathbb{N}_1$, коалиции $C_0 \in \text{coal}_c(S)$ и пиратского вектор-номера $w = (w_1, \dots, w_r) \in \text{desc}(C_0) \setminus C_0$ можно построить такой вектор-ключ $K_w \in K^r$, что ключевая пара (w, K_w) обеспечивает нелегальному пользователю доступ к защищённым данным.

ДОКАЗАТЕЛЬСТВО. Для пиратского вектор-номера $w = (w_1, \dots, w_r)$ и произвольного $i \in \{1, \dots, r\}$ в силу определения потомка существует такой вектор-номер $J_{u(i)} = (j_1, \dots, j_r) \in C_0$, что $j_i = w_i$. Пусть

$$K_{u(i)} = (\kappa_1^{u(i)}, \dots, \kappa_r^{u(i)}) \in K(C_0)$$

— вектор-ключ, соответствующий вектор-номеру $J_{u(i)}$. Тогда

$$D_{\kappa_i^{u(i)}}(e_{i,w_i}) = D_{\kappa_{i,j_i}}(e_{i,j_i}) = s_i$$

(см. шаг 1 алгоритма). Положим $K_w = (\kappa_1^{u(1)}, \dots, \kappa_r^{u(r)})$. Таким образом, по коалиции C_0 и множеству $K(C_0)$ составлена пиратская пара (w, K_w) , позволяющая восстановить блочный ключ и с помощью него расшифровать защищённые данные. Лемма 1 доказана.

1.3. Выбор помехоустойчивых кодов и алгоритмов декодирования для ССШШ. Рассмотренным в п. 1.2 атакам можно противодействовать. В [11, 12] исследован вопрос о применении некоторых помехоустойчивых кодов и списочных декодеров в ССШШ с целью такого противодействия. Представим в удобном виде необходимые для дальнейшего полученные там результаты. Пусть $c \in \mathbb{N}_1$, $C(\subseteq \mathbb{F}_q^r)$ — линейный код. Множество номеров координат совпадения векторов $x=(x_1, \dots, x_r)$, $y=(y_1, \dots, y_r)$ из \mathbb{F}_q^r обозначим через $I(x, y)$. Метрика Хемминга $d(x, y)$ в \mathbb{F}_q^r и множество $I(x, y)$ связаны равенством $d(x, y) = r - |I(x, y)|$.

Говорят, что код C обладает *c-FP-свойством* (англ. *framerproof* — «рамочная защита») [12], если

$$\forall C_0 \in \text{coal}_c(C) \forall z \in C : z \in \{C \setminus C_0\} \Rightarrow z \notin \text{desc}(C_0) \setminus C_0.$$

Замечание 1. Отметим, что код обладает *c-FP-свойством* тогда и только тогда, когда никакая коалиция злоумышленников мощности не более c не может осуществить прямую компрометацию легального пользователя, не входящего в неё, путём создания его вектор-номера.

Говорят, что код C обладает *c-ТА-свойством* (англ. *traceability* — «возможность отследить») [12], если

$$\forall C_0 \in \text{coal}_c(C) \forall w \in \text{desc}(C_0) \setminus C_0 \exists u \in C_0 : \forall z \in C \setminus C_0 |I(z, w)| < |I(w, u)|.$$

Замечание 2. Отметим, что код C обладает *c-ТА-свойством* тогда и только тогда, когда для любого пиратского вектор-номера $w \in \text{desc}_c(C)$ ближайшим кодовым словом является элемент u , входящий в каждую из создающих его коалиций. Этот элемент в [12] предлагается находить переборным декодером.

Известно, что *c-ТА-свойство* влечёт *c-FP-свойство* [12, лемма 1.3].

Код длины r и размерности k будем называть (r, k) -кодом. Напомним, что (r, k) -код с минимальным расстоянием d называется *МДР (r, k) -кодом*, если в неравенстве Синглтона $d \leq r - k + 1$ достигается равенство [6]:

$$d = r - k + 1. \quad (1)$$

Из теоремы 4.4 в [12] вытекает, что если для (r, k) -кода C выполняется неравенство $d > r - r/c^2$, то код обладает *c-ТА-свойством*. Из этого результата, равенства (1) и целочисленности величины c легко вывести, что

МДР (r, k) -код C обладает c -ТА-свойством, если для него выполняется условие

$$c \leq B_0(C) := \lceil \sqrt{r/(k-1)} \rceil - 1. \quad (2)$$

В [11] предлагается использовать в ССШШ обобщённые коды Рида — Соломона (ОРС-коды). Напомним необходимые определения [6]. Пусть $\mathbb{F}_q^{(l)}[x]$ — пространство полиномов степени не выше l с коэффициентами из \mathbb{F}_q , $\alpha_1, \dots, \alpha_q$ — фиксированное упорядочение элементов поля \mathbb{F}_q , $r \in \mathbb{N}$ и $r \leq q$, $a_1, \dots, a_r \in \mathbb{F}_q \setminus \{0\}$, $k \in \{2, 3, \dots, r\}$. *Обобщённый код Рида — Соломона* длины r размерности k $((r, k)$ -ОРС-код), определяется кодирующим отображением $\varphi: \mathbb{F}_q^{(k-1)}[x] \rightarrow \mathbb{F}_q^r$ по правилу

$$\varphi(p) = (a_1 p(\alpha_1), \dots, a_r p(\alpha_r)).$$

Для кодового слова v через p_v будем обозначать полином из $\mathbb{F}_q^{(k-1)}[x]$ такой, что $\varphi(p_v) = v$. Известно, что (r, k) -ОРС-коды являются МДР-кодами.

Далее нам понадобится алгоритм списочного декодирования Гурсвами — Судана для ОРС-кодов (АСДГС) [10]. Напомним, что АСДГС имеет полиномиальную сложность работы и её входными параметрами являются r , k и управляющий параметр $t \in \{\lfloor \sqrt{r(k-1)} + 1 \rfloor, \dots, r\}$. При декодировании на вход подаётся вектор y из \mathbb{F}_q^r и АСДГС производит поиск всех кодовых слов в пределах шара $B(y, r-t)$ радиуса $r-t$ с центром в точке y . Множество полученных на выходе декодера слов называют *списком*. Величину $r-t$ естественно назвать *радиусом работы списочного декодера*. В силу оценки $t > \sqrt{r(k-1)}$ его наибольшее значение равно

$$r_{00} = r - \lceil \sqrt{r(k-1)} \rceil - 1. \quad (3)$$

В [11] идёт речь о целесообразности использования АСДГС в ССШШ.

Лемма 2 [11, разд. 3]. Пусть C — (r, k) -ОРС-код над полем \mathbb{F}_q , для параметра c выполняется оценка (2), r_{00} — определено в (3). Тогда

$$\forall C_0 \in \text{coal}_c(C) \forall w \in \mathbb{F}_q^r : w \in \text{desc}(C_0) \setminus C_0 \Rightarrow \emptyset \neq B(w, r_{00}) \subseteq C_0 \quad (4)$$

и если $r \geq \log_2 q$, то радиус работы АСДГС с управляющим параметром $t = \lceil r/c \rceil$ равен r_{00} .

Смысл этой леммы заключается в следующем. Если в ССШШ применяется (r, k) -ОРС-код C над полем \mathbb{F}_q , а мощность коалиции злоумышленников удовлетворяет оценке (2), то для организации поиска элементов коалиции C_0 контролёру целесообразно применять алгоритм списочного

декодирования Гурусвами — Судана (АСДГС), так как на выходе декодера сгенерируется непустой список злоумышленников, хотя, быть может, и не всех.

1.4. Математическая модель эффективной защиты от коалиционных атак. Применим ОРС-коды и АСДГС для построения математической модели эффективной защиты от коалиционных атак в ССШШ. Далее предполагается, что мощность s коалиции не превышает порога $B_0(C)$ (см. (2)). В п. 1.3 отмечено, что в силу (2) код C обладает s -ТА-свойством. Пусть C — (r, k) -ОРС-код над полем Галуа \mathbb{F}_q , $r \geq \log_2 q$. Для гарантированной защиты от атак коалиций мощности не более s в математической модели распространения данных из 1.1 рассмотрим код C . Под математической моделью защиты от коалиционных атак будем понимать алгоритм 1 действий контролёра, направленный на поиск злоумышленников из коалиции при обнаружении факта несанкционированного распространения ключевой пары $(w, K_w) \in \text{desc}_c(C) \times K^r$.

АЛГОРИТМ 2

ШАГ 1. Осуществить поиск w по базе вектор-номеров легальных пользователей.

ШАГ 2. Если w обнаружен в базе, то w — вектор-номер злоумышленника; иначе подать w на вход АСДГС с управляющим параметром $t = \lceil r/c \rceil$.

ШАГ 3. На выходе АСДГС получить $\{u_i\}$ — непустой контрольный список легальных вектор-номеров злоумышленников из коалиции.

В результате таких действий контролёра злоумышленники из коалиции будут найдены. Корректность модели вытекает из п. 1.3.

Отметим, что необходимость организации эффективного поиска злоумышленников в ССШШ обуславливается большим количеством возможных пиратских вектор-номеров. Если C — (r, k) -ОРС-код над полем Галуа \mathbb{F}_q , $c \in \{2, \dots, q\}$, то $\max_{C_0 \in \text{coal}_c(C)} \{|\text{desc}(C_0)|\} = c^r$.

Из того, что коды с s -ТА-свойством обладают и s -ФР-свойством, следует, что помимо возможности эффективного поиска злоумышленников в модели исключается возможность прямой компрометации невиновных пользователей.

2. Исследование ССШШ в случае превышения пороговой мощности коалиции. Формулировка основных результатов

В случае превышения мощностью коалиции порога $B_0(C)$ (см. (2)), корректная работа модели не гарантируется. При обнаружении контро-

лёмом факта несанкционированного распространения ключевой пары $(w, K_w) \in \text{desc}_c(C) \times K^r$ и запуске алгоритма 1 возможны следующие ситуации.

(i) Вектор-номер w нелегальный ($w \in \text{desc}_c(C) \setminus C$), полученный контрольный список непуст, однако, в нём оказались вектор-номера невиновных пользователей. Это событие, вызывающее сбой на шаге 3 алгоритма 2, назовём *компрометацией невиновного пользователя «списочным декодером»* и обозначим через $A_{1,c}$.

Заметим, что если существует возможность нарушения оценки (2), то контролёру имеет смысл в качестве вектор-номера злоумышленника рассматривать в первую очередь ближний к w элемент контрольного списка, так как при создании w находящийся ближе к w вносит в него большее количество координат. В соответствии с этим выделим следующий подслучай первой ситуации.

(ii) Ближайшим к w является вектор-номер невиновного пользователя. Это событие назовём *компрометацией невиновного пользователя «переборным декодером»* (см. замечание 2) и обозначим через $A_{2,c}$.

(iii) Вектор-номер w нелегальный, однако полученный контрольный список пуст. Это событие, хотя и вызывает сбой на шаге 3 алгоритма 2, не приводит к компрометации невиновного пользователя.

(iv) Вектор-номер w легальный, но создан некоторой коалицией ($w \in \text{desc}_c(C) \cap C$). Это событие, вызывающее сбой на шаге 2 алгоритма 2, назовём *прямой компрометацией* невиновного пользователя и обозначим через $A_{3,c}$.

В случае (iv) контролёр не имеет возможности обнаружить факт коалиционной атаки. В случае (iii) контролёр обнаружит факт коалиционной атаки с превышением мощностью коалиции допустимого порога $B_0(C)$, но предпринять каких-либо действий не может. В случаях (i), (ii) контролёр рассмотрит список вектор-номеров, в котором в качестве вектор-номера злоумышленника имеет смысл рассматривать вектор-номер, ближайший к w .

Выясним при каких значениях мощности c коалиции, возможны рассмотренные события $A_{1,c}$, $A_{2,c}$ и $A_{3,c}$, характеризующие различные типы компрометации невиновного пользователя. Для этого введём понятие множеств компрометации. Пусть

$$\Omega_1(C) = \{c \in \mathbb{N}_1 \mid \exists v \in C \exists C_0 \in \text{coal}_c(C \setminus \{v\}) \exists w \in \text{desc}(C_0) \setminus C_0 : d(v, w) \leq r_{00}\} \quad (5)$$

— множество мощностей таких коалиций, при которых для некоторого кодового слова существует коалиция, у которой хотя бы один из потомков расположен на расстоянии не далее r_{00} от данного кодового слова (3). Очевидно, что $\Omega_1(C)$ — множество таких значений $c \in \mathbb{N}_1$, при которых для кода C существует возможность компрометации некоторого невиновного пользователя в результате применения списочного декодера Гурусвами — Судана к потомку коалиции. Пусть

$$\Omega_2(C) = \{c \in \mathbb{N}_1 \mid \exists v \in C \exists C_0 \in \text{coal}_c(C \setminus \{v\}) \\ \exists w \in \text{desc}(C_0) \setminus C_0 \forall u \in C_0 : d(v, w) \leq d(w, u)\} \quad (6)$$

— множество таких значений $c \in \mathbb{N}_1$, для которых код C не обладает c -ТА-свойством (см. замечание 2). Пусть

$$\Omega_3(C) = \{c \in \mathbb{N}_1 \mid \exists v \in C \exists C_0 \in \text{coal}_c(C \setminus \{v\}) : v \in \text{desc}(C_0) \setminus C_0\} \quad (7)$$

— множество таких $c \in \mathbb{N}_1$, для которых код C не обладает c -ФР-свойством (см. замечание 1). Нетрудно видеть, что вероятность события $A_{i,c}$ положительна тогда и только тогда, когда $c \in \Omega_i(C)$, где $i \in \{1, 2, 3\}$.

Замечание 3. Сдвиг двух точек пространства \mathbb{F}_q^r на некоторый вектор сохраняет расстояние между ними, а сдвиг множества потомков любой коалиции на произвольный кодовый вектор образует множество потомков сдвинутой на тот же вектор коалиции. Отсюда вытекает, что для каждого i множество $\Omega_i(C)$ на самом деле состоит из таких $c \in \mathbb{N}_1$, при которых возможна соответствующая компрометация не только одного, но и нескольких пользователей.

Очевидно, что множество компрометации $\Omega_i(C)$ — целочисленный отрезок вида $\{R_i(C), R_i(C) + 1, \dots, |C|\}$. Величину $R_i(C)$ будем называть *рубежом множества компрометации* $\Omega_i(C)$, причём непосредственно из определений вытекает вложение $\Omega_3(C) \subseteq \Omega_2(C)$, а из доказанной ниже теоремы вытекает вложение $\Omega_2(C) \subseteq \Omega_1(C)$. Таким образом, для рубежей множеств компрометации выполняется условие

$$R_1(C) \leq R_2(C) \leq R_3(C).$$

В силу того, что степень защищённости ССШШ в случае превышения величиной c границы $B_0(C)$ ранее не исследовалась, представляет интерес вопрос о вычислении $R_i(C)$. Действительно, если мощность c коалиции злоумышленников превышает рубеж $R_1(C)$, то возможна компрометация невиновного пользователя «списочным декодером» (событие $A_{1,c}$). Если c превышает рубеж $R_2(C)$, то возможна компрометация

невиновного пользователя «переборным декодером» (событие $A_{2,c}$). Если s превышает $R_3(C)$, то возможна прямая компрометация невиновного пользователя (событие $A_{3,c}$). При этом если мощность s превышает рубеж $R_i(C)$, то вероятность компрометации невиновного пользователя (событие $A_{i,c}$) строго больше нуля, а если не превышает $R_i(C)$, то вероятность компрометации невиновного равна нулю. Следовательно, в зависимости от конкретных условий, при которых проектируется ССШП, вычисление рубежей $R_i(C)$ позволяет уточнить параметры используемого кода и декодера для того, чтобы уменьшить негативные последствия возможного превышения пороговой мощности коалиции злоумышленников.

Ранее рубежи $R_i(C)$ не вводились и не вычислялись. Непосредственный расчёт $R_i(C)$ является достаточно непростой комбинаторной задачей, поэтому если $R_i(C)$ для некоторого i вычислить не удаётся, то интерес представляет задача получения границ для значений $R_i(C)$. Для решения этих задач введём следующие величины:

$$\varepsilon_{r,k} = 1 - [\lceil \sqrt{r(k-1)} \rceil - \sqrt{r(k-1)}] \in \{0; 1\}, \quad (8)$$

$$B_1(C) = B_0(C) + 1 + \varepsilon_{r,k}, \quad B_2(C) = \left\lceil \frac{r+k-1}{2(k-1)} \right\rceil, \quad B_3(C) = \lceil r/(k-1) \rceil, \quad (9)$$

где $B_0(C)$ определено в (2). Прямыми вычислениями проверяется

Лемма 3. Для произвольного (r, k) -кода C

$$2 \leq B_1(C) \leq B_2(C) \leq B_3(C),$$

при этом $B_1(C) = B_2(C)$ тогда и только тогда, когда $r \leq 3(k-1)$, а $B_2(C) = B_3(C)$ тогда и только тогда, когда $r \leq 2(k-1)$.

Сформулируем основной результат работы о рубежах $R_i(C)$ множеств компрометации $\Omega_i(C)$.

Теорема. Пусть C — (r, k) -ОПС-код. Тогда

$$R_1(C) = B_1(C) \leq R_2(C) \leq B_2(C) \leq B_3(C) = R_3(C).$$

Доказательство теоремы представлено в следующем разделе.

Таким образом, для случаев $i = 1$ и $i = 3$ удалось вычислить значения рубежей $R_i(C)$. Доказано, что $B_1(C)$ — нижняя граница для рубежа $R_2(C)$, а $B_2(C)$ — верхняя граница для этого рубежа, более точная чем $R_3(C)$. Из леммы 3 и теоремы видно, что при $r \leq 3(k-1)$ выполняется

условие $R_1(C) = R_2(C) = B_2(C)$, а при $r \leq 2(k-1)$ кроме того имеет место равенство $R_3(C) = B_2(C)$.

В [2] отмечается, что существуют q -ичные коды длины r со скоростью $R := \log_q |C|/r = 1/4$, обладающие 2-ТА-свойством, а вопрос их существования для $R > 1/4$ остаётся открытым. Из теоремы вытекает, что не существуют (r, k) -ОРС-коды со скоростью $R \geq 1/3 + 1/r$, обладающие 2-ТА-свойством. Более того, имеет место

Следствие. Для любого $c \in \mathbb{N}_1$ не существуют (r, k) -ОРС-коды со скоростью $R \geq 1/(2c-1) + 1/r$, обладающие c -ТА свойством.

ДОКАЗАТЕЛЬСТВО. Пусть C — (r, k) -ОРС-код, $R \geq 1/(2c-1) + 1/r$, $c \in \mathbb{N}_1$. Тогда

$$\begin{aligned} k/r \geq 1/(2c-1) + 1/r &\iff c \geq (r+k-1)/2(k-1) \\ &\iff c \geq \lceil (r+k-1)/2(k-1) \rceil = B_2(C). \end{aligned}$$

По теореме $B_2(C) \geq R_2(C)$, значит, $c \geq R_2(C)$. Таким образом, если $R \geq 1/(2c-1) + 1/r$, то код C не обладает c -ТА свойством по определению $\Omega_2(C)$. Следствие доказано.

Полученные теоретические результаты можно использовать в ходе проектирования ССШШ при выборе значений параметров r и k применяемого ОРС-кода. Именно, соотношения из теоремы позволяют делать вывод о возможности различных типов компрометации контролёром невиновных пользователей в случае атаки коалиции мощности c , превосходящей порог $B_0(C)$ (см. (2)). В [5] проведено экспериментальное исследование ССШШ для конкретных кодов и произвольных значений c . (Исследование выполнено на сорока компьютерах с процессором 2,5 ГГц и ОЗУ 512 Мб, что позволило добиться точности 0,005 и доверительной вероятности 0,95 в случае (19,3)-ОРС-кода и (101,2)-ОРС-кода.) Проведённые эксперименты позволили оценить вероятности событий $A_{1,c}$, $A_{2,c}$, $A_{3,c}$, характеризующих тип компрометации невиновного пользователя в случае, если мощностью коалиции c будет превышена не только величина $B_0(C)$, но и рубежи $R_i(C)$. Эксперименты, в частности, показывают, что применение длинных кодов значительно сокращает вероятность компрометации невиновных пользователей даже при значительном превышении предполагаемого числа злоумышленников [5].

3. Доказательство основных результатов

Рассмотрим несколько вспомогательных лемм.

Лемма 4. Пусть C — (r, k) -ОРС-код над полем \mathbb{F}_q . Тогда

$$\begin{aligned} \forall c \in \mathbb{N}_1 \quad \forall v \in C \quad \forall C_0 \in \text{coal}_c(C \setminus \{v\}) \\ \forall w \in \text{desc}(C_0) \setminus C_0 : |I(w, v)| \leq \min\{(k-1)c, r\}, \end{aligned}$$

причём

$$\begin{aligned} \forall c \in \mathbb{N}_1 \quad \forall v \in C \quad \exists C_0 \in \text{coal}_c(C \setminus \{v\}) \\ \exists w \in \text{desc}(C_0) \setminus C_0 : |I(w, v)| = \min\{(k-1)c, r\}. \end{aligned}$$

Лемма 5. Пусть $B_3(C)$ определено в (9). Тогда $R_3(C) = B_3(C)$.

ДОКАЗАТЕЛЬСТВО. Пусть c' — произвольное целое такое, что $c' \geq B_3(C)$. Чтобы доказать оценку $R_3(C) \leq B_3(C)$ достаточно показать, что $c' \in \Omega_3(C)$ (см. (7)). По лемме 4

$$\forall c \geq r/(k-1) \quad \forall v \in C \quad \exists C_0 \in \text{coal}_c(C \setminus \{v\}) \quad \exists w \in \text{desc}(C_0) \setminus C_0 : |I(v, w)| = r.$$

Последнее означает, что $v = w \in \text{desc}(C_0) \setminus C_0$. Тогда из $c \geq r/(k-1)$ следует, что $c \in \Omega_3(C)$. Следовательно, $c' \in \Omega_3(C)$ и $R_3(C) \leq B_3(C)$.

Противоположное неравенство верно для произвольных МДР-кодов и содержится в [1]. Таким образом, $R_3(C) = B_3(C)$. Лемма 5 доказана.

Из определений $\Omega_3(C)$ и $\Omega_2(C)$ следует, что $R_2(C) \leq R_3(C)$, а по лемме 5 $R_3(C) = B_3(C)$. Значит, $B_3(C)$ — верхняя граница для $R_2(C)$. Можно получить более точную верхнюю оценку для $R_2(C)$.

Лемма 6. Пусть $B_2(C)$ определено в (9). Тогда $B_2(C) \geq R_2(C)$.

ДОКАЗАТЕЛЬСТВО. Достаточно показать, что если c — произвольное целое такое, что $c \geq B_2(C)$, то $c \in \Omega_2(C)$, где $\Omega_2(C)$ определено в (6). В силу того, что $B_3(C)$ — верхняя граница для $R_2(C)$, можно ограничиться случаем

$$\left\lceil \frac{r+k-1}{2(k-1)} \right\rceil = B_2(C) \leq c < B_3(C) = \lceil r/(k-1) \rceil.$$

Так как $c \in \mathbb{N}_1$, для $\delta = k-1$ получим

$$(r+\delta)/2 \leq c\delta < r. \tag{10}$$

Пусть $v = (v_1, \dots, v_r) \in C$ — произвольное кодовое слово. Рассмотрим построенные в лемме 4 (см. (12)) $C_0 = \{u_1, \dots, u_c\} \in \text{coal}_c(C \setminus \{v\})$ и $w \in \text{desc}(C_0) \setminus C_0$. Согласно определению $\Omega_2(C)$ для проверки искомого соотношения $c \in \Omega_2(C)$ достаточно показать, что

$$|I(w, u_i)| \leq |I(v, w)| \quad \forall i \in \{1, \dots, c\}. \quad (11)$$

Прежде всего заметим, что в силу леммы 4 выполняется неравенство

$$|I(v, w)| \geq \delta c \quad (12)$$

(w в отличие от v и u_i ($i \in \{1, \dots, c\}$) кодовым словом не является).

Докажем неравенство

$$|I(w, u_i)| \leq r - (c - 1)\delta. \quad (13)$$

Отметим, что $I(v, u_i) \supseteq \{(i - 1)\delta + 1, \dots, i\delta\}$ для любого $i \in \{1, \dots, c\}$, а так как $v, u_i \in C$, ввиду (1) получим $I(v, u_i) = \{(i - 1)\delta + 1, \dots, i\delta\}$. Пусть $I_S(u, v) = \{i \in S : u_i = v_i\}$ для произвольного $S \subseteq \{1, \dots, r\}$, $A = \{1, \dots, \delta c\}$. Очевидно, что $I(v, u_i) \subset A$. Покажем, что $|I_A(w, u_i)| = \delta$. По построению w выполняется неравенство $|I_A(w, u_i)| \geq \delta$. Предположим, что $|I_A(w, u_i)| > \delta$, т.е. существует такой номер $j' \in A \setminus I(v, u_i)$, что $u_{i,j'} = w_{j'}$. Так как $w_j = v_j$ для всех $j \in A$, то $u_{i,j'} = v_{j'}$. Тогда $|I(v, u_i)| \geq \delta + 1$, а значит, ввиду (1) и того, что $u_i, v \in C$, получаем

$$d(u_i, v) \leq r - (k - 1) = d,$$

где d — минимальное расстояние кода C , чего быть не может. Следовательно, $I_A(u_i, w) = \delta$. Отсюда ввиду того, что

$$I(w, u_i) = I_A(w, u_i) \cup I_{\{1, \dots, r\} \setminus A}(w, u_i),$$

получаем

$$|I(w, u_i)| \leq \delta + (r - c\delta) = r - (c - 1)\delta.$$

Таким образом, оценка (13) доказана.

Из левой части оценки (10) вытекает $c\delta \geq r - \delta(c - 1)$. Отсюда в силу (12) и (13) вытекает оценка (11):

$$|I(w, u_i)| \leq r - (c - 1)\delta \leq c\delta \leq |I(v, w)|.$$

Лемма 6 доказана.

Пусть r_{00} — наибольший радиус работы АСДГС.

Лемма 7. Пусть C — (r, k) -ОРС-код, $B_1(C)$ определено в (9). Тогда $R_1(C) = B_1(C)$.

ДОКАЗАТЕЛЬСТВО разобьём на два случая.

(i) Пусть $\varepsilon_{r,k} = 1$, т. е. $\sqrt{r/(k-1)} \notin \mathbb{N}$, где $\varepsilon_{r,k}$ определено в (8). Тогда

$$B_1(C) = B_0(C) + 1 = \lceil \sqrt{r/(k-1)} \rceil.$$

Для проверки неравенства $R_1(C) \leq B_1(C)$ достаточно показать, что для произвольного $c \geq B_1(C)$ выполняется условие $c \in \Omega_1(C)$. Пусть $v \in C$ — произвольное кодовое слово. По лемме 4 найдётся потомок $w \in \text{desc}(C \setminus \{v\})$ такой, что $d(v, w) = \max\{0, r - (k-1)c\}$. Пусть $r - (k-1)c < 0$. Тогда $d(v, w) = 0$. Если $r - (k-1)c \geq 0$, то

$$d(v, w) = r - (k-1)c. \quad (14)$$

Ввиду того, что $c \in \mathbb{N}$, неравенство $c \geq \lceil \sqrt{r/(k-1)} \rceil$ эквивалентно неравенству $c \geq \sqrt{r/(k-1)}$. Значит,

$$d(v, w) \leq r - (k-1)\sqrt{r/(k-1)} = r - \sqrt{r(k-1)}.$$

Так как $\sqrt{r/(k-1)} \notin \mathbb{N}$, из (3) следует, что $r_{00} = \lfloor r - \sqrt{r(k-1)} \rfloor$. Ввиду того, что $d(v, w) \in \mathbb{N}$, получаем

$$d(v, w) \leq r - \sqrt{r(k-1)} \iff d(v, w) \leq \lfloor r - \sqrt{r(k-1)} \rfloor = r_{00}.$$

(Очевидно, последнее верно и для случая $r - (k-1)c < 0$.) Таким образом,

$$\forall v \in C \exists C_0 \in \text{coal}_c(C \setminus \{v\}) \exists w \in \text{desc}(C_0) \setminus C_0 : d(v, w) \leq r_{00}. \quad (15)$$

Значит, согласно определению (5) выполняется условие $c \in \Omega_1(C)$.

Для проверки неравенства $B_1(C) \leq R_1(C)$ достаточно показать, что если $c < B_1(C)$, то $c \notin \Omega_1(C)$. Так как $c < B_1(C)$, имеем

$$c \leq B_1(C) - 1 = B_0(C).$$

Стало быть, выполняется условие (4). Однако из определения (5) следует, что

$$\forall c \in \Omega_1(C) \exists C_0 \in \text{coal}_c(C) \exists w \in \text{desc}(C_0) \setminus C_0 : B(w, r_{00}) \not\subset C_0. \quad (16)$$

Значит, $c \notin \Omega_1(C)$. Таким образом, если $\varepsilon_{r,k} = 1$, то выполняется равенство $R_1(C) = B_1(C)$.

(ii) Пусть $\varepsilon_{r,k} = 0$, т. е. $\sqrt{r/(k-1)} \in \mathbb{N}$. Тогда

$$B_1(C) = B_0(C) + 2 = \lceil \sqrt{r/(k-1)} \rceil + 1.$$

Для проверки неравенства $R_1(C) \leq B_1(C)$ достаточно показать, что для $c \geq B_1(C)$ выполняется условие $c \in \Omega_1(C)$. Пусть $v \in C$ — произвольное кодовое слово, тогда в силу (14) найдётся потомок $w \in \text{desc}(C \setminus \{v\})$ такой, что $d(v, w) = r - (k-1)c$. Ввиду того, что $c \in \mathbb{N}$, неравенство

$$c \geq \lceil \sqrt{r/(k-1)} \rceil + 1$$

эквивалентно неравенству $c \geq \sqrt{r/(k-1)} + 1$. Значит,

$$\begin{aligned} d(v, w) &\leq r - (k-1)(\sqrt{r/(k-1)} + 1) = r - \sqrt{r(k-1)} - (k-1) \\ &\leq r - \sqrt{r(k-1)} - 1. \end{aligned}$$

Так как $\sqrt{r/(k-1)} \in \mathbb{N}$, из (3) следует, что $r_{00} = r - \sqrt{r(k-1)} - 1$. Таким образом, выполняется условие (15). Тем самым $c \in \Omega_1(C)$ согласно определению (5).

Для проверки неравенства $B_1(C) \leq R_1(C)$ достаточно показать, что если $c < B_1(C)$, то $c \notin \Omega_1(C)$. Так как $c < B_1(C)$, получим

$$c \leq B_1(C) - 1 = B_0(C) + 1.$$

Пусть $c \leq B_0(C)$, тогда выполняется условие (4). Однако из определения (5) следует, что выполняется условие (16). Значит, $c \notin \Omega_1(C)$. Пусть $c = B_0(C) + 1 = \lceil \sqrt{r/(k-1)} \rceil$. Пусть $v \in C$ — произвольное кодовое слово, $w \in \text{desc}(C \setminus \{v\})$ — произвольный потомок. По лемме 4 выполняется неравенство

$$d(v, w) \geq \max\{0, r - (k-1)c\}.$$

Пусть $r - (k-1)c < 0$, тогда ввиду $c = B_0(C) + 1$ выполняется неравенство $\lceil \sqrt{r/(k-1)} \rceil > r/(k-1)$, чего быть не может. Пусть $r - (k-1)c \geq 0$, тогда $d(v, w) \geq r - (k-1)c$. Значит, $d(v, w) \geq r - (k-1)\lceil \sqrt{r/(k-1)} \rceil$. При этом

$$r_{00} = r - (k-1)\sqrt{r/(k-1)} - 1 \leq r - (k-1)\lceil \sqrt{r/(k-1)} \rceil - 1.$$

Следовательно,

$$\forall v \in C \forall C_0 \in \text{coal}_c(C \setminus \{v\}) \forall w \in \text{desc}(C_0) \setminus C_0 \ d(v, w) > r_{00},$$

т. е. $c \notin \Omega_1(C)$. Стало быть, если $c < B_1(C)$, то $c \notin \Omega_1(C)$. Таким образом, если $\varepsilon_{r,k} = 0$, то равенство $R_1(C) = B_1(C)$ тоже выполняется. Лемма 7 доказана.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ. Согласно (2) если

$$c \leq B_0(C) = \lfloor \sqrt{r/(k-1)} \rfloor - 1,$$

то код C обладает c -ТА-свойством и $c \notin \Omega_2(C)$. Отсюда $B_0(C) < R_2(C)$, следовательно, $B_1(C) \leq R_2(C)$. Теорема является прямым следствием этого неравенства и лемм 3, 5, 6 и 7. Теорема доказана.

ЛИТЕРАТУРА

1. Деундяк В. М., Мкртичян В. В. Математическая модель эффективной схемы специального широковещательного шифрования и исследование границ её применения // Изв. вузов. Северо-Кавказский регион. Естеств. науки. — 2009. — № 1. — С. 5–8.
2. Кабатянский Г. А. Коды для защиты авторских прав: случай двух пиратов // Проблемы передачи информации. — 2005. — Т. 41, № 2. — С. 123–127.
3. Мкртичян В. В. Компьютерная модель схемы специального широковещательного шифрования на основе кодов Рида — Соломона и списочного декодера Гурусвами — Судана // Мат. IX международной научно-практической конф. «Информационная безопасность». Ч. 2. — Таганрог: ЮФУ, 2007. — С. 111–115.
4. Мкртичян В. В. Компьютерные модели списочных декодеров Гурусвами — Судана для обобщённых кодов Рида — Соломона и конкатенированных кодов // Вестн. ДГТУ. — 2007. — Т. 7, № 4. — С. 384–394.
5. Мкртичян В. В. Об экспериментальном исследовании надёжности и применении схемы специального широковещательного шифрования // Изв. ЮФУ. Техн. науки. — 2008. — №8. — С. 203–210.
6. Сидельников В. М. Теория кодирования. — М.: Физматлит, 2008. — 324 с.
7. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. — М.: Триумф, 2002. — 816 с.
8. Barg A., Blakley G. R., Kabatiansky G. A. Digital fingerprinting codes: problem statements, constructions, identification of traitors // IEEE Trans. Inf. Theory. — 2003. — Vol. 49. — P. 852–865.
9. Chor B., Fiat A., Naor M. Tracing traitors // Proc. Advances in cryptology — Crypto'94. — 1994. — P. 257–270. (Lect. Notes Comp. Sci.; Vol. 839.)
10. Guruswami V. List decoding of error-correcting codes. — New York: Springer-Verl., 2005. — 350 p.

11. **Silverberg A., Staddon J., Walker J.** Application of list decoding to tracing traitors // Proc. Advances in cryptology — ASIACRYPT 2001. — 2001. — P. 175–192. (Lect. Notes Comp. Sci.; Vol. 2248.)
12. **Staddon J. N., Stinson D. R., Wei R.** Combinatorial properties of frameproof and traceability codes // IEEE Trans. Inf. Theory. — 2001. — Vol. 47. — P. 1042–1049.

Деундяк Владимир Михайлович,
e-mail: vlade@math.rsu.ru

Мкртичан Вячеслав Виталиевич,
e-mail: realdeal@bk.ru

Статья поступила
7 апреля 2010 г.

Переработанный вариант —
3 марта 2011 г.