УДК 621.391:517.95

Системный анализ

А. Н. Алексейчук, С. Н. Конюшок

СХЕМЫ МНОГОАДРЕСНОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ, ОСНОВАННЫЕ НА КОНФИГУРАЦИЯХ СТИНСОНА – ВАН ТРАНГА

Ключевые слова: *схема распределения ключей*, *широковещательное шифрование*, *задача о покрытии*, *комбинаторная конфигурация*, *блок-схема*, *блоковый код*.

Введение

Схема многоадресного распределения ключей (СМРК) представляет собой криптографический протокол, с помощью которого доверенная сторона, выполняющая функции центра распределения ключей (ЦРК), осуществляет передачу некоторой вспомогательной секретной информации абонентам сети связи так, что со временем абоненты, входящие в определенную привилегированную коалицию, могут восстановить общий секретный ключ, который в зашифрованном виде передается из ЦРК по широковещательному каналу связи (по этой причине СМРК называют также схемами широковещательного шифрования – broadcast encryption schemes).

Схемы многоадресного распределения ключей предложены в [1, 2]. На сегодняшний день список публикаций, посвященных исследованию их свойств и методов построения, насчитывает десятки наименований. Отметим обзорные статьи [3, 4] и работы [5 – 7], содержащие, в частности, информацию о различных аспектах практического применения СМРК.

В [8] (и впоследствии, независимо в [5]) предложен общий подход к построению схем многоадресного распределения ключей на основе покрытий множества V абонентов определенными подмножествами. Каждому такому

подмножеству B (блоку покрытия) ставится в соответствие секретный ключ, вырабатываемый в ЦРК. Затем каждому абоненту $x \in V$ по защищенному каналу связи передают набор секретных ключей, соответствующих подмножествам B, содержащим x. Наконец, для передачи общего секретного ключа некоторой привилегированной коалиции $P \subseteq V$ этот ключ зашифровывают на секретных ключах абонентов из P, соответствующих определенным подмножествам $B \subseteq P$, образующим покрытие множества P.

В [8] получены оценки параметров, характеризующих практическую эффективность СМРК, в которых подмножества B определяются как блоки (уравновешенных неполных) блок-схем с множеством элементов V (см. [9, 10]).

Целью данной статьи является исследование характеристик более общего класса схем многоадресного распределения ключей, соответствующих так называемым (v, b, r, λ)-конфигурациям, введенным Д. Стинсоном и Т. ван Трангом [11]. Рассматриваемые СМРК имеют безусловную (теоретико-информационную) стойкость и включают в себя, в качестве частных случаев, СМРК, основанные на блок-схемах [8] и блоковых кодах [12].

Полученные в статье результаты показывают, что, хотя схемы многоадресного распределения ключей, основанные на (v, b, r, λ)-конфигурациях, уступают по своим характеристикам одной из лучших на сегодняшний день безусловно стойких СМРК (так называемой схеме CST) [5], они являются более эффективными по сравнению со схемами [8]. В частности, общее число секретных ключей в СМРК, соответствующей (v, b, r, λ)-конфигурации, может быть меньше числа абонентов сети, что принципиально невозможно для СМРК, основанных на блок-схемах.

Изложенные в статье результаты частично анонсированы в [13].

(v, b, r, λ)-конфигурации

Пусть V – конечное множество мощности v, $B = \{B_1, \ldots, B_b\}$ – совокупность попарно различных непустых подмножеств множества V, r и λ – натуральные числа, $\lambda < r$.

Определение 1 [11]. Упорядоченная пара $D = (V, B)$ называется (v, b, r, λ)-конфигурацией с блоками $B_1, \ldots, B_b$, если каждый элемент $x \in V$ принадлежит ровно r множествам B_j, $j \in \overline{1,b}$, и каждая пара различных элементов x, $y \in V$ принадлежит не более чем λ множествам B_j, $j \in \overline{1,b}$.

Если все блоки (v, b, r, λ)-конфигурации D имеют одинаковую мощность $k < v-1$, и каждая пара различных элементов множества V принадлежит ровно λ блокам, то D называется (уравновешенной неполной) блок-схемой или (b, v, r, k, λ)-конфигурацией. В случае $v = b$ или, что равносильно, $k = r$ (b, v, r, k, λ)-конфигурация D называется симметричной блок-схемой или (v, k, λ)-конфигурацией [10].

Далее слово “конфигурация” используется как синоним термина “(v, b, r, λ)-конфигурация”. При этом предполагается, что λ является наименьшим натуральным числом, для которого выполняется условие, указанное в определении 1.

Параметры произвольной (v, b, r, λ)-конфигурации D связаны соотношениями, обобщающими известные соотношения для параметров блок-схем [9, 10]. В частности, если все блоки конфигурации D имеют одинаковую мощность k, то

$$vr = bk,\ r(k-1) \le \lambda(v-1), \qquad (1)$$

причем последнее неравенство обращается в равенство, если D является блок-схемой (см. [11]).

В [11] предложены способы построения (v, b, r, λ)-конфигураций, отличных от блок-схем, исходя из систем Штейнера, строго универсальных

хэш-семейств и ортогональных таблиц соответственно. Следующая конструкция обобщает последний из указанных способов, позволяя строить конфигурации по произвольным блоковым кодам над конечным алфавитом.

Пусть F – конечное множество мощности $q \geq 2$, $G \subseteq F^n$ – код длины n над алфавитом F с минимальным расстоянием (Хэмминга) $d < n$, состоящий из v кодовых слов ($(n, v, d)_q$-код) [14]. Рассмотрим множества

$$B_{i,a} = \{(x_1,\ldots,x_n) \in G : x_i = a\},\ i \in \overline{1,n},\ a \in F. \qquad (2)$$

Заметим, что каждое слово $x \in G$ принадлежит ровно n множествам вида (2). При этом, поскольку расстояние Хэмминга между любыми двумя различными словами $x, y \in G$ больше либо равно d, то пара $\{x, y\}$ содержится не более чем в $n - d$ указанных множествах. Таким образом, упорядоченная пара (V, B), где $V = G$, $B = \{B_{i,a} : i \in \overline{1,n},\ a \in F, B_{i,a} \neq \varnothing\}$, является (v, b, r, λ)-конфигурацией с параметрами $v = |G|$, $b = |B| \leq nq$, $r = n$, $\lambda = n - d$.

Назовем построенную конфигурацию кодовой конфигурацией, соответствующей коду G, и обозначим ее символом D_G.

По аналогии с понятием разрешимой блок-схемы [9] введем в рассмотрение следующий класс конфигураций.

Определение 2. Назовем (v, b, r, λ)-конфигурацию $D = (V, B)$ разрешимой, если существуют попарно непересекающиеся подмножества $B^{(1)}, \ldots, B^{(r)}$ множества B,

$$B^{(i)} = \{B_{i,1}, \ldots, B_{i,q_i}\},\ i \in \overline{1,r}, \qquad (3)$$

такие, что для любого $i \in \overline{1,r}$

$$\bigcup_{l=1}^{q_i} B_{i,l} = V,\ B_{i,l_1} \cap B_{i,l_2} = \varnothing,\ l_1, l_2 \in \overline{1,q_i},\ l_1 \neq l_2. \qquad (4)$$

Непосредственно из данных определений следует, что каждая кодовая конфигурация разрешима. Справедливо также обратное утверждение (и, следовательно, классы разрешимых и кодовых конфигураций совпадают).

Утверждение 1. Пусть $D = (V, B)$ – разрешимая (v, b, r, λ)-конфигурация. Тогда существует $(r, v, r - \lambda)_q$-код G такой, что $D = D_G$.

Доказательство. Пусть $B = B^{(1)} \cup \ldots \cup B^{(r)}$, где попарно непересекающиеся множества $B^{(i)}$, $i \in \overline{1,r}$, определяются по формуле (3) и удовлетворяют соотношениям (4).

Положим $q = \max\{q_i : i \in \overline{1,r}\}$, $F = \{1, 2, \ldots, q\}$. Для любого $x \in V$ определим вектор $\chi(x) = (x_1, \ldots, x_r)$, полагая $x_i = j$ в том и только в том случае, когда $x \in B_{i,j}$, $i \in \overline{1,r}$, $j \in F$. В силу (4) данное определение корректно. Положим $G = \{\chi(x) : x \in V\}$. Непосредственная проверка показывает, что G является $(r, v, r - \lambda)_q$-кодом, и выполняется равенство $D = D_G$. Утверждение доказано.

Введем ряд дополнительных понятий, используемых ниже при анализе характеристик схем многоадресного распределения ключей.

Пусть $D = (V, B)$ – (v, b, r, λ)-конфигурация с блоками $B_1, \ldots, B_b$. Для любого $x \in V$ обозначим $K_x = \{ j \in \overline{1,b} : x \in B_j \}$.

Определение 3. Конфигурация D называется t-устойчивой ($t = 0, 1, \ldots$) [2, 8], если для любого $C \subseteq V$ такого, что $|C| = t$, блоки B_j, $j \in \overline{1,b}$, содержащиеся во множестве $V \setminus C$, образуют покрытие этого множества.

Назовем наибольшее целое число t, $0 \le t \le v - 1$, для которого D является t-устойчивой конфигурацией, устойчивостью конфигурации D и обозначим это число символом $\tau(D)$.

Определение 4. Назовем конфигурацию $D = (V, B)$ слабо l-однородной ($l = 0, 1, \ldots$), если для любых $x \in V$, $K \subseteq K_x$, где $|K| = l$, существует $y \in V \setminus \{x\}$ такой, что $K \subseteq K_y$.

Обозначим $\Gamma^{(l)}(v)$ совокупность всех слабо l-однородных конфигураций на множестве V мощности v (с произвольными возможными значениями параметров b, r, λ). Справедливы включения

$$\Gamma^{(0)}(v) \supseteq \Gamma^{(1)}(v) \supseteq \ldots \supseteq \Gamma^{(\lambda)}(v) \supseteq \Gamma^{(\lambda+1)}(v) = \varnothing.$$

Отметим, что множество $\Gamma^{(0)}(v)$ состоит из всех (v, b, r, λ)-конфигураций (V, B), а множество $\Gamma^{(1)}(v)$ – из всех конфигураций (V, B) с блоками $B_1, \ldots, B_b$, удовлетворяющими условию $|B_j| \geq 2$, $j \in \overline{1,b}$.

Следующее утверждение вытекает непосредственно из определения кодовой конфигурации и определения 4.

Утверждение 2. Пусть G – $(n, v, d)_q$-код над алфавитом F, где $d < n$, D_G – конфигурация, соответствующая коду G, $l \in \{1, 2, \ldots, \lambda\}$. Тогда $D_G \in \Gamma^{(l)}(v)$ в том и только в том случае, когда частота появления произвольного вектора $\alpha \in F^l$ в любых l различных столбцах $(v \times n)$-таблицы, составленной из слов кода G, отлична от 1. В частности, если G является линейным кодом размерности k над полем $\mathbf{GF}(q)$ или $(n, q^k, d = n - k + 1)_q$-кодом МДР (см. [15]), $2 \leq k \leq n$, то $D_G \in \Gamma^{(k-1)}(q^k)$.

Схемы многоадресного распределения ключей, соответствующие (v, b, r, λ)-конфигурациям

Пусть имеются центр распределения ключей и множество V абонентов сети связи, $|V| = v$. Пусть, далее, $D = (V, B)$ – (v, b, r, λ)-конфигурация с блоками $B_1, \ldots, B_b$, занумерованными определенным образом числами от 1 до b, и $(S, +)$ – конечная абелева группа порядка $|S| > b$.

В соответствии с общим определением СМРК, основанных на покрытиях множества абонентов [5, 8], схема многоадресного распределения ключей, соответствующая конфигурации D, представляет собой криптографический протокол, состоящий из двух этапов.

На первом этапе в центре распределения ключей независимо, случайно и равновероятно генерируют элементы $u_1, \ldots, u_b$ множества S, которые называются секретными ключами абонентов. Ключу u_j присваивают открытый идентификатор j, равный номеру блока B_j конфигурации D, $j \in \overline{1,b}$.

Затем каждому абоненту $x \in V$ по защищенному каналу связи передают набор секретных ключей $(u_j\colon\ j \in K_x)$.

Пусть далее, на втором этапе, требуется передать из ЦРК абонентам, образующим некоторую привилегированную коалицию $P \subseteq V$ мощности $|P| \geq v - \tau(D)$, случайный, равновероятный и не зависящий от $u_1, \ldots, u_b$ общий (групповой) ключ $k_P \in S$ таким образом, чтобы ни один из абонентов, принадлежащих множеству $C = V \setminus P$, не получил никакой информации об этом ключе. С этой целью в ЦРК находят определенное покрытие $\{B_{i(1)}, \ldots, B_{i(m)}\}$ множества P блоками B_j, $j \in \overline{1,b}$, не пересекающимися с C (согласно определению параметра $\tau(D)$ и неравенству $|P| \geq v - \tau(D)$, такие покрытия существуют), и передают всем абонентам сети по широковещательному каналу связи сообщение

$$b_P = (i(1), u_{i(1)} + k_P; \ldots; i(m), u_{i(m)} + k_P). \qquad (5)$$

Каждый абонент $x \in P$ может однозначно восстановить k_P по принятому сообщению (5), используя секретный ключ $u_{i(l)}$ с номером $i(l) \in K_x$, $l \in \overline{1,m}$. При этом в силу независимости и равновероятности ключей $u_1, \ldots, u_b$, k_P абоненты, принадлежащие множеству C, не получат никакой апостериорной информации о ключе k_P.

Отметим, что в соответствии с терминологией [5], описанная схема распределения ключей является однократной ренонс-схемой (one-time revocation scheme), устойчивой относительно компрометации $\tau(D)$ абонентов.

Заметим также, что вместо операции + при формировании сообщения (5) можно использовать произвольную квазигрупповую операцию на множестве S, реализующую табличный шифр гаммирования [16]. Полученная таким образом схема распределения ключей будет иметь ту же (безусловную) стойкость и те же характеристики эффективности, что и исходная СМРК.

В соответствии с [2, 5, 8], основными параметрами, характеризующими эффективность СМРК, соответствующей конфигурации D, являются число r

секретных ключей, передаваемых каждому абоненту из ЦРК на первом этапе, и максимальное число зашифрований ключа k_P, которые необходимо выполнить для формирования сообщения (5), предназначенного произвольной привилегированной коалиции $P \subseteq V$ мощности $v - t$, $t \in \overline{0, \tau(D)}$. Следуя [8], назовем последнюю характеристику t-связностью конфигурации D и обозначим ее $\chi_D(t)$.

Отметим, что t-связность является функцией целочисленного параметра $t \in \overline{0, \tau(D)}$, которая зависит от конкретного алгоритма построения покрытия множества $P \subseteq V$ мощности $v - t$ блоками $B_j \subseteq P$, $j \in \overline{1, b}$. Обычно предполагают, что таким покрытием является произвольное минимальное (по числу блоков) покрытие множества P [8]. Поэтому далее будем считать, что t-звязность совпадает с максимумом мощностей минимальных покрытий привилегированных коалиций, состоящих из $v - t$ абонентов, соответствующими блоками конфигурации D, $t \in \overline{0, \tau(D)}$.

В качестве дополнительного показателя эффективности СМРК, основанной на конфигурации D, примем общее число b секретных ключей, вырабатываемых в ЦРК на первом этапе.

Оценки устойчивости и t-связности (v, b, r, λ)-конфигураций

В [8] получены оценки устойчивости и t-связности произвольной (b, v, r, k, λ)-конфигурации D:

$$r\lambda^{-1} < \tau(D),$$

$$\chi_D(t) \le \frac{v - t}{r - \lambda t}(1 + \ln k),\ 0 \le t < r\lambda^{-1}. \qquad (6)$$

Показано также [8], что в случае, когда D является проективной плоскостью порядка k (симметричной блок-схемой с параметрами ($k^2 + k + 1$, $k + 1$, 1) [9, 10]), $k \ge 2$, справедливы более точные оценки

$$\tau(D) = k,\ \chi_D(t) \le k(t+1),\ t \in \overline{0, \tau(D)}. \qquad (7)$$

Следующие теоремы обобщают и усиливают эти результаты.

Теорема 1. Пусть D – (v, b, r, λ)-конфигурация. Тогда

$$\left\lceil \frac{r-\lambda}{\lambda} \right\rceil \le \tau(D). \qquad (8)$$

Кроме того, если $D \in \Gamma^{(l)}(v)$, то

$$\tau(D) \le \left\lceil \frac{r-\lambda}{l} \right\rceil; \qquad (9)$$

в частности, если $D \in \Gamma^{(\lambda)}(v)$, то $\tau(D) = \left\lceil \frac{r-\lambda}{\lambda} \right\rceil$.

Доказательство. Положим $t = \tau(D) + 1$. Согласно определению параметра $\tau(D)$, существуют элементы $x, z_1, \ldots, z_t$ такие, что $x \ne z_i$, $i \in \overline{1,t}$ и $K_x \subseteq \bigcup_{i=1}^{t} K_{z_i}$. Отсюда в силу соотношений $|K_x| = r$, $|K_x \cap K_{z_i}| \le \lambda$, $i \in \overline{1,t}$, находим $r \le \sum_{i=1}^{t} |K_x \cap K_{z_i}| \le \lambda t = \lambda(\tau(D)+1)$. Следовательно, справедливо неравенство (8).

Для доказательства (9) зафиксируем пару различных элементов $x, y \in V$ таких, что $|K_x \cap K_y| = \lambda$. Не ограничивая общности рассуждений, предположим, что

$$K_x = \{1, 2, \ldots, \lambda, j_1, j_2, \ldots, j_{r-\lambda}\},\ K_y = \{1, 2, \ldots, \lambda, j_1', j_2', \ldots, j_{r-\lambda}'\},$$

где $\{j_1, j_2, \ldots, j_{r-\lambda}\} \cap \{j_1', j_2', \ldots, j_{r-\lambda}'\} = \varnothing$.

Представим множество $\{j_1, j_2, \ldots, j_{r-\lambda}\}$ в виде объединения $t = \left\lceil \frac{r-\lambda}{l} \right\rceil$ попарно непересекающихся множеств $K^{(1)}, \ldots, K^{(t)}$, каждое из которых, за исключением, быть может, последнего, имеет мощность l. Из условия теоремы и определения 4 вытекает, что существуют элементы $z_1, \ldots, z_t \in V$

такие, что $x \neq z_i$, $K_{z_i} \supseteq K^{(i)}$, $i \in \overline{1,t}$. Следовательно, $K_x \subseteq K_y \cup (\bigcup_{i=1}^{t} K_{z_i})$, где $x \notin \{z_1, \ldots, z_t, y\}$. Таким образом, на основании определения 3 $\tau(D) \leq t = \left\lceil \frac{r-\lambda}{l} \right\rceil$. Итак, неравенство (9), а вместе с ним и теорема, доказаны.

Пусть для фиксированных натуральных v и τ_0 задан некоторый класс $A(v, \tau_0)$ конфигураций D на множестве V ($|V| = v$) такой, что $\tau(D) \geq \tau_0$ для любого $D \in A(v, \tau_0)$.

Определение 5. Назовем конфигурацию $D_0 \in A(v, \tau_0)$ с параметрами (v, b_0, r_0, λ_0) ρ-оптимальной в классе $A(v, \tau_0)$, если для любой (v, b, r, λ)-конфигурации $D \in A(v, \tau_0)$ выполняется неравенство $r_0 \leq r$.

Согласно данному определению, схемы многоадресного распределения ключей, основанные на ρ-оптимальных конфигурациях, характеризуются наименьшим (в заданном классе СМРК) числом секретных ключей, хранящихся у абонентов сети связи.

Следующая теорема устанавливает достаточные условия ρ-оптимальности конфигураций в классе $\Gamma^{(l)}(v, \tau_0) \stackrel{\text{def}}{=} \{D \in \Gamma^{(l)}(v): \tau(D) \geq \tau_0\}$.

Теорема 2. Если для данных v, τ_0 и l существует слабо l-однородная конфигурация D_0 с параметрами $(v, b_0, r_0 = l\tau_0 + 1, l)$, то эта конфигурация является ρ-оптимальной в классе $\Gamma^{(l)}(v, \tau_0)$.

Доказательство. По теореме 1 $\tau(D_0) = \left\lceil \frac{r_0 - l}{l} \right\rceil = \tau_0$, откуда следует, что $D_0 \in \Gamma^{(l)}(v, \tau_0)$. С другой стороны, если D – (v, b, r, λ)-конфигурация, $D \in \Gamma^{(l)}(v, \tau_0)$, то на основании формулы (9) $\tau_0 \leq \tau(D) \leq \left\lceil \frac{r-\lambda}{l} \right\rceil$. Отсюда в силу неравенства $l \leq \lambda$, вытекающего из условия непустоты класса $\Gamma^{(l)}(v)$, следует, что $r \geq l\tau_0 + 1 = r_0$. Теорема доказана.

Непосредственно из теоремы 2, утверждения 2 и предшествующего ему замечания вытекают следующие результаты.

Следствие 1. Пусть D_0 – проективная плоскость порядка $\tau_0 \geq 2$. Тогда D_0 является ρ-оптимальной в классе всех ($v = \tau_0^2 + \tau_0 + 1$, b, r, λ)-конфигураций $D = (V, B = \{B_1, \ldots, B_b\})$, удовлетворяющих условиям $\tau(D) \geq \tau_0$, $|B_j| \geq 2$, $j \in \overline{1,b}$.

Следствие 2. Пусть k, τ_0 – натуральные числа, $k \geq 2$, G – линейный код МДР длины $n = (k - 1)\tau_0 + 1$ и размерности k над полем $F = \mathbf{GF}(q)$. Тогда кодовая конфигурация D_G является ρ-оптимальной в классе всех τ_0-устойчивых конфигураций D, соответствующих k-мерным линейным кодам над полем F.

Для доказательства следующих двух теорем потребуется известная верхняя граница мощности минимального покрытия конечного множества.

Лемма 1 [17], с. 136. Пусть A – конечное множество мощности N, $C_1, \ldots, C_m$ – такая система его подмножеств, что каждый элемент $a \in A$ принадлежит не менее чем γm подмножествам этой системы, $\gamma > 0$. Тогда существует покрытие множества A, состоящее не более чем из $\gamma^{-1}(1 + \ln(\gamma N)) + 1$ подмножеств $C_1, \ldots, C_m$.

Теорема 3. Пусть $D = (V, B)$ – (v, b, r, λ)-конфигурация, блоки которой имеют одинаковую мощность $k \geq 2$. Тогда

$$\tau(D) \leq \frac{v-1}{k-1}(1 + \ln \lambda). \qquad (10)$$

Доказательство. Зафиксируем произвольный элемент $x \in V$ и положим в условии леммы 1 $A = K_x$, $C_i = K_i \cap K_x$, $i \in V \setminus \{x\}$, $\gamma = \frac{k-1}{v-1}$. Согласно утверждению леммы, существует покрытие множества K_x, состоящее не более чем из $\frac{v-1}{k-1}(1 + \ln(\gamma r)) + 1$ подмножеств C_i, $i \in V \setminus \{x\}$. Следовательно,

$\tau(D) \le \frac{v-1}{k-1}(1+\ln\frac{r(k-1)}{v-1})$, откуда в силу соотношений (1) вытекает неравенство (10). Теорема доказана.

Отметим, что в ряде случаев верхняя граница (10) является более точной по сравнению с оценкой (9). Рассмотрим, например, слабо $(k-1)$-однородную конфигурацию D_G, соответствующую симплексному коду G з параметрами $n=(q^k-1)(q-1)^{-1}$, $k\ge 2$, $d=q^{k-1}$ над полем $\mathbf{GF}(q)$ [15]. При фиксированном $k\ge 2$ и $q\to\infty$ выражение в правой части (10) имеет порядок $O(q(1+(k-2)\ln q))$, в то время как порядок выражения в правой части (9) равен $O(q^{k-1}(k-1)^{-1})$. Отметим также, что нижняя граница (8) устойчивости конфигурации D_G является величиной порядка $O(q)$.

Теорема 4. Пусть D = (V, B) – (v, b, r, λ)-конфигурация. Тогда для любого $0 \le t < r\lambda^{-1}$ справедливо неравенство

$$\chi_D(t) \le \frac{b-rt+\lambda\binom{t}{2}}{r-\lambda t}\left(1+\ln\frac{(v-t)(r-\lambda t)}{\max\{1,b-rt\}}\right)+1. \qquad (11)$$

Доказательство. Пусть $C \subseteq V$, $|C| = t$, $0 \le t < r\lambda^{-1}$. Обозначим

$$B_C=\{B_j\in B: B_j\cap C=\varnothing, j\in\overline{1,b}\},\ b_C = |B_C|.$$

Заметим, что на основании неравенства (8) $b_C \ge 1$. Далее, справедливо равенство $b_C = b - \left|\bigcup_{x\in C} K_x\right|$, из которого в силу соотношений $|K_x| = r$, $|K_x\cap K_y|\le\lambda$, $x,y\in V$, $x\ne y$, и неравенств Бонферрони [18] вытекают следующие оценки:

$$b-rt\le b_C\le b-rt+\lambda\binom{t}{2}. \qquad (12)$$

Применим лемму 1 к системе B_C подмножеств множества $A = V \setminus C$,

полагая $N = v - t$, $m = b_C$, $\gamma = \dfrac{r - \lambda t}{b_C}$. На основании утверждения леммы получим, что существует покрытие множества $V \setminus C$, состоящее не более чем из $\dfrac{b_C}{r - \lambda t}\left(1 + \ln \dfrac{(v-t)(r-\lambda t)}{b_C}\right) + 1$ блоков конфигурации D, каждый из которых не пересекается с C. Отсюда в силу (12) и определения параметра $\chi_D(t)$ следует неравенство (11). Теорема доказана.

Верхняя оценка *t*-связности кодовых (*v, b, r,* λ)-конфигураций

Получим оценку t-связности произвольной кодовой конфигурации, которая в определенных случаях оказывается более точной по сравнению с оценкой (11).

Пусть D_G – $(v, b, r = n, \lambda = n - d)$-конфигурация, соответствующая $(n, v, d)_q$-коду G над алфавитом F, $q \geq 2$, $d < n$.

Зафиксируем произвольное множество $C \subseteq G$ мощности t, где $0 \leq t < n(n-d)^{-1}$. Запишем кодовые слова, принадлежащие множеству C, в виде прямоугольной таблицы размера $t \times n$. Эту таблицу будем отождествлять с множеством C и обозначать тем же символом.

Обозначим $T_i = \{a \in F: B_{i,a} \cap C \neq \varnothing\}$, где $B_{i,a}$ определяется по формуле (2), $t_i = |T_i|$, $i \in \overline{1,n}$. Отметим, что t_i равно числу различных элементов алфавита F, содержащихся в i-м столбце таблицы C, $i \in \overline{1,n}$.

Предположим, не ограничивая общности рассуждений, что

$$t_1 \geq t_2 \geq \ldots \geq t_n. \tag{13}$$

Докажем ряд вспомогательных утверждений.

Лемма 2. В обозначениях, введенных выше, совокупность множеств

$$\{B_{i,a}: a \in F \setminus T_i,\ i \in \overline{1, t(n-d)+1}\} \tag{14}$$

является покрытием множества $G \setminus C$.

Доказательство. Предположим противное: существует кодовое слово $x=(x_1,\ldots,x_n)\in G\setminus C$ такое, что $x_i\in T_i$, $i\in\overline{1,t(n-d)+1}$. Отсюда следует, что для любого $i\in\overline{1,t(n-d)+1}$ существует слово $(y_1,\ldots,y_n)\in C$ со свойством $x_i=y_i$. Поскольку при этом $|C| = t$, найдется слово $y^{(0)}\in C$, $n - d + 1$ координат которого совпадают с соответствующими координатами слова x. Но это противоречит тому, что d является минимальным расстоянием кода G. Следовательно, совокупность (14) является покрытием множества $G \setminus C$.

Лемма доказана.

Лемма 3. В обозначениях, введенных выше, справедливо неравенство

$$\gamma(C)\overset{\text{def}}{=}\sum_{i=1}^{n}t_i\geq\frac{n^2t}{nt-d(t-1)}. \tag{15}$$

Доказательство. Обозначим $\alpha_{1,i},\ldots,\alpha_{t_i,i}$ частоты встречаемости всех элементов алфавита F, содержащихся в i-м столбце таблицы C, $i\in\overline{1,n}$. Справедливы соотношения $\alpha_{1,i}+\ldots+\alpha_{t_i,i}=t$, $\alpha_{l,i}\geq1$, $l\in\overline{1,t_i}$, $i\in\overline{1,n}$.

Обозначим $d(u,w)$ расстояние Хэмминга между произвольными словами (одинаковой длины) u и w над алфавитом F и оценим значение

$$\delta(C)\overset{\text{def}}{=}\sum_{(x,y)\in C^2}d(x,y)=\sum_{i=1}^{n}\sum_{(x,y)\in C^2}d(x_i,y_i).$$

Поскольку d – минимальное расстояние кода G, и $|C| = t$, то

$$dt(t-1)\leq\delta(C). \tag{16}$$

С другой стороны, нетрудно видеть, что

$$\delta(C)=\sum_{i=1}^{n}\sum_{l=1}^{t_i}\alpha_{l,i}(t-\alpha_{l,i})=t^2n-\sum_{i=1}^{n}\sum_{l=1}^{t_i}\alpha_{l,i}^2. \tag{17}$$

Поскольку $t_i^{-1}(\alpha_{1,i}^2+\ldots+\alpha_{t_i,i}^2)\geq t_i^{-2}(\alpha_{1,i}+\ldots+\alpha_{t_i,i})^2=t_i^{-2}t^2$, $i\in\overline{1,n}$, то на основании (17)

$$\delta(C) \le t^2 n - t^2 \sum_{i=1}^{n} t_i^{-1},$$

откуда, используя неравенство

$$n\left(\sum_{i=1}^{n} t_i^{-1}\right)^{-1} \le n^{-1}\left(\sum_{i=1}^{n} t_i\right) = n^{-1}\gamma(C),$$

получим, что

$$\delta(C) \le t^2 n - \frac{t^2 n^2}{\gamma(C)}. \qquad (18)$$

Из (16), (18) непосредственно следует неравенство (15). Лемма доказана.

Лемма 4. При выполнении условия (13) справедливо неравенство

$$\sum_{i=1}^{t(n-d)+1} t_i \ge \frac{nt(t(n-d)+1)}{nt - d(t-1)}. \qquad (19)$$

Доказательство. Обозначим $m = t(n - d) + 1$,

$$\gamma(C, M) \overset{\text{def}}{=} \sum_{i \in M} t_i,\ M \subseteq N = \{1, 2, \ldots, n\}.$$

Заметим, что среднее арифметическое значений $\gamma(C, M)$ по всем $M \subseteq N$ таким, что $|M| = m$, равно

$$\binom{n}{m}^{-1} \sum_{\substack{M \subseteq N: \\ |M|=m}} \left(\sum_{i \in M} t_i\right) = \binom{n}{m}^{-1} \sum_{i=1}^{n} t_i \sum_{\substack{M \subseteq N: \\ |M|=m,\, i \in M}} 1 = \binom{n}{m}^{-1} \binom{n-1}{m-1} \sum_{i=1}^{n} t_i = \frac{m}{n}\gamma(C),$$

и, согласно (15), больше либо равно $\dfrac{nmt}{nt - d(t-1)}$. Следовательно, существует множество $M_0 \subseteq N$ мощности m такое, что

$$\gamma(C, M_0) \ge \frac{nmt}{nt - d(t-1)}. \qquad (20)$$

Поскольку в силу (13) $\sum_{i=1}^{m} t_i \ge \gamma(C, M_0)$, то из формулы (20) следует неравенство (19). Лемма доказана.

Теорема 5. Для t-связности конфигурации D_G, соответствующей $(n, v, d)_q$-коду G, справедливо следующее неравенство:

$$\chi_G(t) \le (t(n-d)+1)\left(q - \frac{nt}{nt - d(t-1)}\right),\ 0 \le t < n(n-d)^{-1}\ . \qquad (21)$$

Доказательство. Пусть $C \subseteq G$, $|C| = t$, $0 \le t < n(n-d)^{-1}$. На основании леммы 2 совокупность множеств (14) является покрытием множества $G \setminus C$, состоящим из $\chi(C) \overset{\text{def}}{=} (t(n-d)+1)q - \sum_{i=1}^{t(n-d)+1} t_i$ блоков.

Согласно формуле (19), $\chi(C) \le (t(n-d)+1)q - \frac{nt(t(n-d)+1)}{nt - d(t-1)}$ для любого $C \subseteq G$ такого, что $|C| = t$. Следовательно, выполняется неравенство (21). Теорема доказана.

Характеристики эффективности схем многоадресного распределения ключей, соответствующих определенным кодовым конфигурациям или симметричным блок-схемам

С целью наглядной иллюстрации полученных результатов, рассмотрим схемы многоадресного распределения ключей, основанные на симметричных блок-схемах $D(\tau, \lambda)$ с параметрами ($v = \lambda\tau^2 + \tau + 1$, $k = \lambda\tau + 1$, λ), $\tau, \lambda \in \mathbf{N}$, и, соответственно, кодовых конфигурациях $D_{G(\tau,\lambda)}$, где $G(\tau,\lambda)$ – линейный код МДР длины $n = \tau\lambda + 1$ и размерности $\lambda + 1$ над полем $\mathbf{GF}(q)$, $\tau, \lambda \in \mathbf{N}$, q – наименьшее примарное число, удовлетворяющее условию $q \ge n - 1$ (такие коды существуют для любых натуральных τ и λ [15], стр. 309).

По теореме 1 блок-схема $D(\tau, \lambda)$ (при условии ее существования) имеет устойчивость не менее τ, а конфигурация $D_{G(\tau,\lambda)}$ – устойчивость, равную τ. Число секретных ключей у каждого абонента (участника СМРК $D(\tau, \lambda)$ или СМРК $D_{G(\tau,\lambda)}$) равно $\lambda\tau + 1$.

Общее число секретных ключей, вырабатываемых на первом этапе СМРК $D(\tau, \lambda)$, совпадает с числом участников схемы и равно $v = \lambda\tau^2 + \tau + 1$. При этом схема многоадресного распределения ключей, основанная на конфигурации $D_{G(\tau,\lambda)}$, допускает существенно большее число участников $v' = q^{\lambda+1}$ и предполагает генерацию и распределение $b = q(\lambda\tau + 1)$ секретных ключей.

В табл. 1 приведены численные значения верхних границ t-связности конфигураций $D = D(\tau, \lambda)$ и $D_G = D_{G(\tau,\lambda)}$ при $\tau = 1000$, $\lambda = 2$ и $\lambda = 3$. В первом случае $(\lambda = 2)$ число секретных ключей у каждого абонента равно 2001, $v = 2001001$, $v' = 8036054027$, $b = 4008003$, $q = 2003$. Во втором случае $(\lambda = 3)$ каждый абонент имеет 3001 секретный ключ, $v = 3001001$, $v' = 81108054012001$, $b = 9006001$, $q = 3001$.

В табл. 2 приведены численные оценки t-связности конфигураций $D = D(10000, 2)$ и $D_G = D_{G(10000,2)}$. В этом случае число секретных ключей у каждого абонента равно 20001, $v = 200010001$, $v' = 8013207261331$, $b = 400240011$, $q = 20011$. (Отметим, что параметры блок-схем $D(\tau, \lambda)$ при указанных выше значениях τ и λ удовлетворяют условиям теоремы Брука-Райзера-Човла [9], однако авторам статьи не известно, существуют ли в действительности блок-схемы с такими параметрами. Поэтому значения выражений в правых частях неравенств (6) и (11), приведенные в табл. 1, 2, являются оценками t-связности блок-схем лишь при условии их существования).

Таблица 1

λ			$t = 1$	$t = 10$	$t = 100$	$t = 500$	$t = 1000$
2	D	(6)	8610	8688	9556	17189	17202813
		(11)	8602	8602	8649	10702	15493166
	D_G	(11)	32474	32613	34237	51408	27940951
		(21)	6006	41854	384312	1671058	3006752
3	D	(6)	9015	9097	10006	18004	27020111
		(11)	9007	9008	9056	11250	23847330
	D_G	(11)	75134	75572	80553	128667	130701235
		(21)	12000	92723	875911	4003778	7504500

Таблица 2

		$t = 1$	$t = 10$	$t = 100$	$t = 1000$	$t = 5000$	$t = 10000$
D	(6)	109046	109144	110136	121149	218054	2180707521
	(11)	109036	109036	109041	109640	136281	2011181676
D_G	(11)	416411	416589	418404	439543	663484	3481691962
	(21)	60030	420021	4002308	382227646	166790566	300227510

Как видно из табл. 1, 2, для указанных параметров блок-схем оценка (11) является более точной по сравнению с формулой (6). При t, близких к τ, обе оценки t-связности блок-схем становятся тривиальными, поскольку их значения превышают число $v - t$. Для кодовых конфигураций $D_{G(\tau,\lambda)}$ при крайних (близких к 1 или к τ) значениях t более точной оценкой t-связности является формула (21).

В целом, конфигурации, соответствующие кодам МДР, предоставляют больше возможностей для синтеза СМРК с необходимыми значениями показателей эффективности, позволяя строить схемы многоадресного распределения ключей, характеризующиеся большим числом участников и меньшим количеством секретных ключей при заданных устойчивости конфигурации и числе ключей, хранящихся у каждого абонента сети связи.

Список литературы

1. Berkovits S. How to broadcast a secret // Advances in Cryptology – EUROCRYPT’91. – № 547. – Berlin: Springer-Verlag, 1992. – P. 536 – 541.
2. Fiat A., Naor M. Broadcast encryption // Advances in Cryptology – CRYPTO’93. – № 773. – Berlin: Springer-Verlag, 1994. – P. 480 – 491.
3. Stinson D. R. On some methods for unconditionally secure key distribution and broadcast encryption // Designs, Codes and Cryptography. – 1997. – Vol. 12. – P. 215 – 243.
4. Конюшок С. М., Олексійчук А. М. Безумовно стійки схеми розподілу ключів в інформаційних та телекомунікаційних системах з великою кількістю абонентів: I. Схеми попереднього розподілу й узгодження ключів, II. Схеми багатоадресного розподілу ключів // Прикладная радиоэлектроника. – 2006. – Т. 5. – № 1. – С. 83 – 104.
5. Naor D., Naor M., Lotspiech J. Revocation and tracing schemes for stateless receivers // Advances in Cryptology – CRYPTO’01. – № 2139. – Berlin: Springer-Verlag, 2001. – P. 41 – 62.
6. Asano T. A revocation scheme with minimal storage at receivers // ASIACRYPT’02. – № 2501. – Berlin: Springer-Verlag, 2002. – P. 433 – 450.
7. Naor M., Pincas B. Efficient trace and revoke schemes // Financial Cryptogtaphy’00. – № 1962. – Berlin: Springer-Verlag, 2000. – P. 1 – 20.
8. Korjik V., Ivkov M., Merinovich Y., Barg A., van Tilborg H. A broadcast key distribution scheme based on block designs // Cryptography and Coding V. – № 1025. – Berlin: Springer-Verlag, 1995. – P. 12 – 21.
9. Холл М. Комбинаторика: Пер. с англ. – М.: Мир, 1970. – 427 с.
10. Райзер Г. Дж. Комбинаторная математика: Пер. с англ. – М.: Мир, 1966. – 154 с.

11. Stinson D. R., van Trung T. Some new results on key distribution patterns and broadcast encryption // Designs, Codes and Cryptography. – 1998. – Vol. 15. – P. 261 – 279.
12. Алексейчук А. Н., Конюшок С. Н. Асимптотические соотношения для вероятностей числа нескомпрометированных ключей в схемах распределения ключей, построенных на основе блоковых кодов // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – Вип. 8. – Київ, 2004. – С. 85 – 90.
13. Алексейчук А. Н., Конюшок С. Н. Оптимальные схемы многоадресного распределения ключей, основанные на (v, b, r, λ)-конфигурациях // Праці міжнародної конференції “Питання оптимізації обчислень (ПОО – XXXII)”, присвяченої пам’яті акад. В. С. Михалевича. – Київ: Ін-т кібернетики ім. В. М. Глушкова НАН України, 2005. – С. 22 – 23.
14. Дельсарт Ф. Алгебраический подход к схемам отношений теории кодирования: Пер. с англ. – М.: Мир, 1976. – 136 с.
15. Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А. Теория кодов, исправляющих ошибки: Пер. с англ. – М.: Связь, 1979. – 743 с.
16. Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В. Основы криптографии. – М.: Гелиос АРВ, 2001. – 480 с.
17. Дискретная математика и математические вопросы кибернетики / Васильев Ю. Л., Ветухновский Ф. Я., Глаголев В. В. и др. – Т. 1. – М.: Наука, 1974. – 311 с.
18. Сачков В.Н. Введение в комбинаторные методы дискретной математики. – М.: Наука, 1982. – 384 с.