УДК 621.391:519.2

АСИМПТОТИЧЕСКИЕ СООТНОШЕНИЯ ДЛЯ ВЕРОЯТНОСТЕЙ ЧИСЛА НЕСКОМПРОМЕТИРОВАННЫХ КЛЮЧЕЙ В СХЕМАХ РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ, ПОСТРОЕННЫХ НА ОСНОВЕ БЛОЧНЫХ КОДОВ

Антон Алексейчук, Сергей Конюшок

СФ СБ Украины в составе ВИТИ НТУУ "КПИ"

Аннотация: **Рассматривается вероятностная модель процесса компрометаций корреспондентов в определенных схемах широковещательного распределения ключей, построенных на основе ортогональных таблиц силы 1 или 2. Получены точные оценки биномиальных моментов и асимптотические выражения вероятностей числа нескомпрометированных ключей в этих схемах после компрометации случайного равновероятного t-подмножества корреспондентов.**

Summary: **It is considered the probabilistic model of the correspondents compromising process in some broadcast key distribution schemes, built on base of orthogonal arrays of strength 1 or 2. As a result, we obtain proper bounds for binomial moments and asymptotic expressions of probability of the number non-compromising keys in these schemes under condition of random equiprobable t- subset correspondents compromising.**

Ключевые слова: **Схема распределения ключей, компрометация корреспондентов, ортогональная таблица, распределение Пуассона.**

I. Введение

Одним из перспективных направлений современной криптографии является разработка методов построения и анализа свойств схем распределения ключей (СРК) в телекоммуникационных системах, имеющих безусловную стойкость относительно компрометации корреспондентов [1 – 7]. Стойкость указанных СРК основывается на принципиальной невозможности получения противником информации о ключах, используемых корреспондентами для ведения засекреченной связи, что обычно достигается путем применения для распределения ключей определенных комбинаторных конфигураций [8], а также увеличением количества вспомогательной секретной информации, используемой корреспондентами телекоммуникационной системы для вычисления общих сеансовых ключей.

В [4, 5] предложены конструкции безусловно стойких схем распределения ключей на основе широковещательного шифрования информации, которые могут быть использованы в случае динамически изменяющегося множества скомпрометированных корреспондентов. В схеме распределения ключей, описанной в [5], применяется так называемая процедура динамического управления ключами, в соответствии с которой осуществляется широковещательная передача зашифрованных сеансовых ключей корреспондентам $1, 2, \ldots, v$ из центра распределения ключей (ЦРК). При этом предполагается, что на множестве корреспондентов задана некоторая комбинаторная конфигурация (система подмножеств) D так, что каждому блоку $B \subseteq \{1, 2, \ldots, v\}$ этой конфигурации соответствует определенный секретный ключ, которым обладают корреспонденты, принадлежащие множеству B (и только они). Секретные ключи заранее доставляются корреспондентам из ЦРК по защищенным каналам связи и используются ими в дальнейшем для расшифрования сообщений (сеансовых ключей), передаваемых из центра распределения ключей по открытому широковещательному каналу.

В [5 – 7] получены аналитические оценки ряда числовых параметров, характеризующих эффективность описанной выше, а также близкой к ней, схемы распределения ключей в том частном случае, когда в качестве комбинаторной конфигурации D используется произвольная симметричная неполная сбалансированная блок-схема [8].

В настоящей статье вводятся в рассмотрение схемы широковещательного распределения ключей, построенные на основе конфигураций, являющихся блочными кодами над произвольным конечным алфавитом. С использованием вероятностных методов исследуется асимптотическое поведение распределения случайной величины (СВ), равной числу нескомпрометированных ключей в кодовой СРК при компрометации случайного равновероятного t-подмножества корреспондентов.

II. Постановка задачи

Пусть F – конечное множество мощности $q \geq 2$, G – код длины n над алфавитом F (то есть произвольное подмножество множества F^n[9]), состоящий из $v = q^k$ слов ((n, q^k)-код), $k \geq 2$. Запишем кодовые слова, принадлежащие G, в виде прямоугольной таблицы размера $v \times n$. Далее будем отождествлять эту таблицу с кодом G и обозначать ее тем же символом. Напомним [9], что G называется ортогональной таблицей силы $l \geq 1$, если каждый l-мерный вектор над алфавитом F содержится одинаковое число (равное q^{k-l}) раз в произвольных фиксированных l столбцах таблицы G.

Для данного кода G построим схему распределения ключей D_G на множестве v корреспондентов, отождествляя их со словами, принадлежащими коду G, а распределяемые этим корреспондентам ключи – с множествами

$$B_i(a) = \{x = (x_1,...,x_n) \in G : x_i = a\},\ i \in \overline{1,n},\ a \in F. \tag{1}$$

По определению, компрометация корреспондента $x \in G$ означает, что из схемы D_G удаляются все множества $B_i(a)$ вида (1), содержащие слово x. Назовем ключи, соответствующие указанным множествам, скомпрометированными ключами (в результате компрометации корреспондента x) в СРК D_G.

Для любого натурального t зададим на множестве всех t-подмножеств кода G равномерное распределение вероятностей p_t, полагая для любого $A \subseteq G$ такого, что $|A| = t$,

$$p_t(A) = \binom{v}{t}^{-1}. \tag{2}$$

Обозначим через ξ_t случайную величину, равную числу ключей, являющихся нескомпрометированными в результате компрометации корреспондентов СРК D_G, принадлежащих случайному множеству A, распределенному по закону (2).

Основной задачей, решаемой в настоящей статье, является построение точных оценок биномиальных моментов $E\binom{\xi_t}{l}$ случайной величины ξ_t, $l = 0, 1, ...,$ и исследование асимптотического поведения распределения этой случайной величины при $t, q \to \infty$.

III. Основная часть

Получим представление СВ ξ_t в виде суммы индикаторов. Заметим, что

$$\xi_t = \sum_{i=1}^{n} \xi_t^{(i)}, \tag{3}$$

где $\xi_t^{(i)}$ – число элементов алфавита F, отсутствующих в i-м столбце и строках с номерами из множества A таблицы G. Введем случайные величины $\xi_{i,a}$, полагая $\xi_{i,a} = 1$, если на пересечении i-го столбца и строк с номерами из множества A, соответствующих скомпрометированным корреспондентам СРК D_G, отсутствует элемент a; $\xi_{i,a} = 0$ – в противном случае, $i \in \overline{1,n}$, $a \in F$. В силу равенства (3) получим, что

$$\xi_t = \sum_{(i,a) \in \overline{1,n} \times F} \xi_{i,a}. \tag{4}$$

Предположим, что код G является ортогональной таблицей силы 1. Тогда на основании соотношений (2), (4)

$$E\xi_t = \sum_{(i,a) \in \overline{1,n} \times F} P(\xi_{i,a} = 1),$$

$$P(\xi_{i,a}=1)=\binom{q^k}{t}^{-1}\binom{q^k-q^{k-1}}{t},\ i\in\overline{1,n},\ a\in F,$$

где последнее равенство вытекает из формулы (2) и того факта, что каждый элемент алфавита F встречается в любом фиксированном столбце таблицы G ровно q^{k-1} раз. Отсюда находим

$$E\xi_t=nq\binom{q^k}{t}^{-1}\binom{q^k-q^{k-1}}{t}. \tag{5}$$

Предположим теперь, что $t,q\to\infty$ таким образом, что

$$t=o(q),\ q\to\infty. \tag{6}$$

Принимая во внимание неравенство $k\ge 2$, получим, что при условии (6)

$$\binom{q^k}{t}\sim\frac{q^{kt}}{t!},\ \binom{q^k-q^{k-1}}{t}\sim\frac{(q^k-q^{k-1})^t}{t!},\ t,q\to\infty,$$

откуда на основании (5) следует, что

$$E\xi_t\sim nq(1-q^{-1})^t\sim nq\exp\{-t/q\},\ t,q\to\infty. \tag{7}$$

Непосредственно из соотношений (6), (7) и неравенства Маркова вытекает следующий результат.

Утверждение 1. Пусть $(n,\ q^k)$-код G является ортогональной таблицей силы 1, $k\ge 2$. Обозначим через $\eta_t=1-(nq)^{-1}\xi_t$ относительное число скомпрометированных ключей в результате случайных и равновероятных компрометаций t корреспондентов СРК D_G, соответствующей коду G. Тогда при выполнении условия (6) последовательность СВ $\{\eta_t : t=1,2,...\}$ сходится к нулю по вероятности:

$$P(\eta_t\ge\varepsilon)\le\varepsilon^{-1}E\eta_t=o(1),\ t\to\infty$$

для любого $\varepsilon>0$.

Получим точные оценки биномиальных моментов СВ ξ_t. Далее будем предполагать, что код G является ортогональной таблицей силы 2.

Пусть l – фиксированное натуральное число. Справедливо равенство

$$E\binom{\xi_t}{l}=\sum_{\{(i_1,a_1),...,(i_l,a_l)\}}P(\xi_{i_1,a_1}=...=\xi_{i_l,a_l}=1), \tag{8}$$

где суммирование в (8) осуществляется по всем l-подмножествам множества $\overline{1,n}\times F$.

Зафиксируем произвольное подмножество $U_l=\{(i_1,a_1),...,(i_l,a_l)\}\subseteq\overline{1,n}\times F$ и получим двусторонние оценки вероятности $P(\xi_{i_1,a_1}=...=\xi_{i_l,a_l}=1)$, соответствующей этому подмножеству.

Обозначим через I мультимножество $\{i_1,...,i_l\}$ и через a вектор $(a_1,...,a_l)$. Предположим, что среди чисел $i_1,...,i_l$ имеется ровно s различных, скажем, $i_1,...,i_s$, где $1\le s\le l$. Пусть, далее, α_j есть кратность вхождения элемента i_j в мультимножество I, $a_1^{(j)},...,a_{\alpha_j}^{(j)}$ – те и только те координаты вектора a, для которых выполняется условие $(i_j,a_1^{(j)}),...,(i_j,a_{\alpha_j}^{(j)})\in U_l$, где $j\in\overline{1,s}$. Очевидно, что $\alpha_1,...,\alpha_s\ge 1$, $\alpha_1+...+\alpha_s=l$, и для любого $j\in\overline{1,s}$ элементы $a_1^{(j)},...,a_{\alpha_j}^{(j)}$ алфавита F попарно различны.

Обозначим через $N(U_l)$ число таких слов $x=(x_1,...,x_n)$ кода G, для которых выполняются условия $x_{i_1}\notin\{a_1^{(1)},...,a_{\alpha_1}^{(1)}\}$, ..., $x_{i_s}\notin\{a_1^{(s)},...,a_{\alpha_s}^{(s)}\}$. Справедливо равенство

$$P(\xi_{i_1,a_1} = \ldots = \xi_{i_l,a_l} = 1) = \binom{q^k}{t}^{-1} \binom{N(U_l)}{t}. \tag{9}$$

Получим оценки параметра $N(U_l)$. Заметим, что, поскольку код G является ортогональной таблицей силы 2, то на основании неравенств Бонферрони [10] имеют место следующие соотношения:

$$N(U_l) = q^k - \#\bigcup_{j=1}^{s}\{x \in G : x_{i_j} \in \{a_1^{(j)},\ldots,a_{\alpha_j}^{(j)}\}\} \le q^k - \sum_{j=1}^{s}\#\{x \in G : x_{i_j} \in \{a_1^{(j)},\ldots,a_{\alpha_j}^{(j)}\}\} +$$

$$+ \sum_{1\le j(1)<j(2)\le s} \#\{x \in G : x_{i_{j(1)}} \in \{a_1^{j(1)},\ldots,a_{\alpha_{j(1)}}^{j(1)}\}, x_{i_{j(2)}} \in \{a_1^{j(2)},\ldots,a_{\alpha_{j(2)}}^{j(2)}\}\} =$$

$$= q^k - (\sum_{j=1}^{s}\alpha_j)q^{k-1} + (\sum_{1\le j(1)<j(2)\le s}\alpha_{j(1)}\alpha_{j(2)})q^{k-2}. \tag{10}$$

На основании равенства (10) и соотношений

$$\alpha_1 + \ldots + \alpha_s = l,\ l^2 = (\alpha_1 + \ldots + \alpha_s)^2 = \alpha_1^2 + \ldots + \alpha_s^2 + 2\sum_{1\le j(1)<j(2)\le s}\alpha_{j(1)}\alpha_{j(2)} \ge 2\sum_{1\le j(1)<j(2)\le s}\alpha_{j(1)}\alpha_{j(2)}$$

справедлива оценка

$$N(U_l) \le q^k - lq^{k-1} + \tfrac{1}{2}l^2q^{k-2}. \tag{11}$$

Кроме того, имеет место оценка

$$N(U_l) = q^k - \#\bigcup_{j=1}^{s}\{x \in G : x_{i_j} \in \{a_1^{(j)},\ldots,a_{\alpha_j}^{(j)}\}\} \ge q^k - \left(\sum_{j=1}^{s}\alpha_j\right)q^{k-1} = q^k - lq^{k-1}. \tag{12}$$

Итак, на основании соотношений (9), (11), (12) для любого l-подмножества $U_l = \{(i_1,a_1),\ldots,(i_l,a_l)\}$ множества $\overline{1,n}\times F$ выполняются следующие неравенства:

$$\binom{q^k}{t}^{-1}\binom{q^k - lq^{k-1}}{t} \le P(\xi_{i_1,a_1} = \ldots = \xi_{i_l,a_l} = 1) \le \binom{q^k}{t}^{-1}\binom{q^k - lq^{k-1} + \frac{1}{2}l^2q^{k-2}}{t}. \tag{13}$$

Из равенства (8) и неравенств (13) вытекает следующее утверждение, устанавливающее точные оценки биномиальных моментов случайной величины ξ_t.

Утверждение 2. Пусть $(n,\ q^k)$-код G является ортогональной таблицей силы 2, $k \ge 2$. Тогда для любого натурального l справедливы неравенства

$$\binom{nq}{l}\binom{q^k}{t}^{-1}\binom{q^k - lq^{k-1}}{t} \le E\binom{\xi_t}{l} \le \binom{nq}{l}\binom{q^k}{t}^{-1}\binom{q^k - lq^{k-1} + \frac{1}{2}l^2q^{k-2}}{t}. \tag{14}$$

Исходя из оценок (14), с использованием метода моментов [10] нетрудно убедиться в справедливости следующего утверждения.

Утверждение 3. Пусть в условиях утверждения 2 параметры n, q и t изменяются таким образом, что

$$nq\exp\{-t/q\} \to \lambda > 0,\ t,q \to \infty, \tag{15}$$

и параметр k принимает любые натуральные (не обязательно фиксированные) значения, больше либо равные 2. Тогда для любого $l = 0, 1, \ldots$

$$\lim_{t\to\infty} P(\xi_t = l) = e^{-\lambda}\frac{\lambda^l}{l!}, \tag{16}$$

то есть последовательность распределений СВ $\{\xi_t : t = 1, 2, \ldots\}$ сходится по распределению к распределению Пуассона с параметром λ.

IV. Выводы

Как следует из утверждений 1, 3, асимптотическое поведение распределения вероятностей случайной величины ξ_t, равной числу нескомпрометированных ключей в СРК D_G при случайной и равновероятной компрометации t корреспондентов, определяется предельным значением функции $nq\exp\{-t/q\}$ при $t,q\to\infty$, где n – длина кода G над алфавитом F (равная количеству ключей, хранящихся у каждого корреспондента СРК D_G), $q=|F|$ – число различных сообщений, которые необходимо передать из ЦРК по широковещательному каналу связи всем корреспондентам при инициализации процедуры динамического управления ключами. Так, при выполнении условия (15) предельный при $t,q\to\infty$ закон распределения последовательности СВ $\{\xi_t : t=1,2,...\}$ совпадает с законом распределения Пуассона с параметром λ. Если же имеет место равенство (6), то последовательность СВ $\{\eta_t=1-(nq)^{-1}\xi_t : t=1,2,...\}$ сходится по вероятности к нулю.

В целом, полученные выше результаты вероятностного анализа числа нескомпрометированных ключей в СРК, построенных на основе ортогональных таблиц силы 1 или 2, могут быть использованы на этапах проектирования или оценки эффективности кодовых схем распределения ключей в телекоммуникационных системах. С практической точки зрения, представляют интерес задачи вероятностного анализа числа нескомпрометированных корреспондентов и наименьшего числа сообщений, передаваемых этим корреспондентам из ЦРК, при случайной и равновероятной компрометации t корреспондентов кодовой схемы распределения ключей.

Литература: ***1.*** *Blom R.. An Optimal Class of Symmetric Key Generation System // Lekture Notes in Computer Science. – 1985. – № 209. – P.335 – 338.* ***2.*** *Stinson D. R. On Some Methods for Unconditionally Secure Key Distribution and Broadcast Encryption // Designs, Codes and Cryptography. – 1997. – № 12. – P.215 – 243.* ***3.*** *Blundo B., De Santis A., Herzberg A., Kutten S., Vaccaro U., Yung M.. Perfectly Secure Key Distribution for Dynamic Conferences // Lecture Notes in Computer Science. – 1993. – № 740. – P.471 – 486.* ***4.*** *Fiat A., Naor M.. Broadcast Encryption // Lekture Notes in Computer Science. – 1994. – № 773. – P.480 – 491.* ***5.*** *Korjik V., Ivkov M., Merinovich Y., Bang A., Van Tilborg H.. A Broadcast Key Distribution Scheme Based on Block Designs // Lecture Notes in Computer Science. – 1995. – № 1025. – P.12 – 21.* ***6.*** *Алексейчук А.Н., Паничек В.Г. Анализ стойкости ключевых сетей относительно компрометации корреспондентов // Збірник наукових праць КВІУЗ. Вип. 3. Київ. 1998. С. 76 – 83.* ***7.*** *Конюшок С. М. Алгоритм оцінки параметрів оптимальних ключових структур, побудованих на основі неповних урівноважених блок-схем // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – Київ: 2003. – Вип. 6. – С. 79 – 83.* ***8.*** *Холл М. Комбинаторика. Пер. с англ. – М.: Мир, 1970. – 427 с.* ***9.*** *Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А. Теория кодов, исправляющих ошибки: Пер. с англ. М.: Связь, 1979. – 743 с.* ***10.*** *Сачков В.Н. Введение в комбинаторные методы дискретной математики. – М.: Наука, 1982. – 384 с.*