Раздел IV. Методы и средства криптографии и стеганографии

УДК 004.056.5

С.А. Евпак, В.В. Мкртичян

О СВЯЗИ ГРАНИЦ ПРИМЕНЕНИЯ СПЕЦИАЛЬНОЙ СХЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ОСНОВАННОЙ НА *Q*-ИЧНЫХ КОДАХ РИДА–МАЛЛЕРА

Целью работы является исследование условий применения схемы защиты легально тиражируемой цифровой продукции от несанкционированного распространения. Задачами работы являются, во-первых, исследование новых границ применения схемы защиты, а во-вторых, построение условий связи границ применения этой схемы. В соответствии с целью в работе проведено исследование условий применения схемы специального широковещательного шифрования (ССШШ), основанной на перспективных q-ичных кодах Рида–Маллера, и современных методах списочного декодирования в случае превышения допустимого числа членов коалиции злоумышленников. В соответствии с задачами в работе получены новые границы применения этой схемы, а также условия, представляющие связь как новых, так и исследованных ранее границ применения этой схемы. Полученные теоретические результаты можно использовать в ходе проектирования ССШШ при выборе значений параметров применяемого в ССШШ q-ичного кода Рида–Маллера и управляющих параметров применяемого в ССШШ списочного декодера.

q-коды Рида–Маллера; списочное декодирование; широковещательное шифрование; поиск злоумышленников.

S.A. Yevpak, V.V. Mkrtichan

ABOUT THE LINK BETWEEN THE BOUNDS OF APPLYING OF THE SPECIAL INFORMATION PROTECTION SCHEME BASED ON THE Q-ARY REED–MULLER CODES

The purpose of the article is to study conditions of applying of a scheme of legally circulated digital products protection from unauthorized distribution. The objectives are to study new bounds of the scheme and to build a conditions of connections between the bounds of the scheme. According to the purpose an study of special broadcast encryption scheme (SBES), based on perspective q-ary Reed–Muller codes and modern methods of list decoding is carried out in case of exceeding of possible size of coalition members. According to the objectives a new bounds of applying of the scheme are constructed and a link between the bounds and a bounds constructed in previous works are deduced. This theoretical results can be applied during engineering of SBES, particularly during selecting a parameters of applied Reed-Muller code and parameters of applied list decoder.

q-ary Reed-Muller codes; list decoding; broadcast encryption; traitor tracing.

1. Введение и постановка задачи. В работе [1] рассмотрен перспективный способ защиты легально тиражируемой цифровой продукции от несанкционированного распространения, называемый схемой специального широковещательного шифрования (ССШШ). Известно, что злоумышленники, являющиеся легальными пользователями ССШШ, могут объединяться в коалиции и пытаться атаковать ССШШ. В [2], [3] доказано, что для эффективного поиска всей коалиции, или, по

крайней мере, ее непустого подмножества, можно применять q-ичные коды Рида–Маллера. В [4] представлена математическая модель эффективной ССШШ на основе q-ичных кодов Рида–Маллера и списочного декодера Пелликаана для q-ичных кодов Рида-Маллера. Целью настоящей работы является исследование математической модели эффективной ССШШ на основе q-ичных кодов Рида-Маллера и списочного декодера Пелликаана для q-ичных кодов Рида–Маллера в случае превышения допустимого числа членов коалиции злоумышленников.

2. Определение q-ичных кодов Рида-Маллера и списочное декодирование. Пусть $\mathbf{N}$ – множество натуральных чисел, $N_1 = \mathbf{N}\backslash\{1\}$, $\mathbf{F}_q[X_1, X_2, \dots, X_m]$ – кольцо полиномов m переменных с коэффициентами из поля Галуа $\mathbf{F}_q$, $\mathbf{F}_q^r[X_1, X_2, \dots, X_m]$ – подпространство полиномов степени не выше r кольца $\mathbf{F}_q[X_1, X_2, \dots, X_m]$, степень монома $X_1^{t_1}X_2^{t_2} \dots X_m^{t_m} \in (\mathbf{F}_q[X_1, X_2, \dots, X_m])$ есть $\sum_{i=1}^{m} t_i$, а степень $\deg(f)$ полинома f из $\mathbf{F}_q[X_1, X_2, \dots, X_m]$ есть максимальная из степеней входящих в него мономов. Пусть, кроме того, $\boldsymbol{P}_1, \boldsymbol{P}_2, \dots, \boldsymbol{P}_n$ – фиксированное упорядочение элементов пространства Хемминга $\mathbf{F}_q^m = \mathbf{F}_q \times \dots \times \mathbf{F}_q$, где $n = q^m$. Тогда q-ичный код Рида–Маллера $\mathrm{RM}_q(r, m)$ порядка r определяется следующим образом [5]:

$$\mathrm{RM}_q(r, m) = \{(f(\boldsymbol{P}_1), f(\boldsymbol{P}_2), \dots, f(\boldsymbol{P}_n)) | f \in \mathbf{F}_q^r[X_1, \dots, X_m]\}.$$

Из леммы 2 работы [2] вытекает, что для кода $\mathrm{RM}_q(r, m)$ выполняется оценка

$$r \le m(q-1).$$

В работе [5] представлен алгоритм списочного декодирования q-ичного кода Рида–Маллера, на который далее будем ссылаться как на Алгоритм 1. Входными параметрами алгоритма являются параметры q, r и m кода $\mathrm{RM}_q(r, m)$. При декодировании на вход алгоритма подается слово $y = (y_0, y_1 \dots, y_{n-1}) \in \mathbf{F}_q^n$, где $n = q^m$ – длина кода $\mathrm{RM}_q(r, m)$. Декодер производит поиск всех кодовых слов в пределах сферы, центром которой является y, радиусом – величина

$$E = \left\lfloor n - \sqrt{n(n-d)} - 1 \right\rfloor, \quad (1)$$

где d – минимальное расстояние кода $\mathrm{RM}_q(r, m)$. Выходом алгоритма является список всех информационных векторов $b \in \mathrm{RM}_q(r, m)$, удовлетворяющих условию: $d(b, y) \le E$. Оценка эффективности работы алгоритма 1 списочного декодирования q-ичного кода Рида-Маллера составляет $O(n)$ операций в поле $\mathbf{F}_q$ и $O(n^3)$ операций в поле $\mathbf{F}_{q^m}$.

3. Математическая модель схемы специального широковещательного шифрования, основанной на q-ичных кодах Рида–Маллера и списочном декодере для них. Для получения доступа к распространяемым данным пользователь ССШШ получает от распространителя данных ключевую пару, включающую, в частности, так называемый вектор-номер, являющийся словом помехоустойчивого кода C ([1], [4], [6]). Злоумышленники могут объединить свои вектор-номера в коалицию и строить потомков коалиции. Множество всевозможных коалиций кода C мощности не более $c(\ge 2)$ обозначается через $\mathrm{coal}_c(C)$; множество потомков коалиции $C_0 \in \mathrm{coal}_c(C)$ обозначается через $\mathrm{desc}(C_0)$ и определяется правилом

$$\mathrm{desc}(C_0) = \{w = (w_1, \dots, w_n) \in \mathbf{F}_q^n : \forall i \in \{1; \dots; n\}\ w_i \in C_{0,i}\},$$

где $C_{0,i}$ – множество i-х координат всех вектор-номеров коалиции C_0; множество пиратских вектор-номеров коалиции C_0 определяется правилом $\mathrm{desc}(C_0)\backslash C_0$. Под множеством-потомков кода C будем понимать

$$\mathrm{desc}_c(C) = \bigcup_{C_i \in \mathrm{coal}_c(C)} \mathrm{desc}(C_i).$$

Пиратские вектор-номера можно применять для нелегального доступа к тиражируемым данным.

Через $Z_c(C)$ будем обозначать максимальное число нулей в пиратском вектор-номере, который может быть порожден коалицией мощности c из множества $C\backslash\{0\}$. Нетрудно видеть, что

$$(n-d) \le Z_c(C) \le c(n-d).$$

Пусть $c \in N_1$, C – произвольный код. Код C является c-FP-кодом тогда и только тогда, когда

$$\forall C_i \in \mathrm{coal_c}(C)\ \forall z \in C\colon\ z \in \{C\backslash C_i\} \Rightarrow z \notin \mathrm{desc}(C_i)\backslash C_i.$$

Отметим, что код является c-FP-кодом тогда и только тогда, когда никакая коалиция злоумышленников мощности не более c не может осуществить прямую компрометацию легального пользователя, не входящего в нее, путем создания его вектор-номера.

Пусть $c \in N_1$, C – произвольный код. Код C является c-IPP-кодом тогда и только тогда, когда

$$\forall w \in \mathrm{desc_c}(C)\ \bigcap_{\{i:w\in \mathrm{desc}(C_i)\}} C_i \neq \emptyset.$$

Отметим, что код является c-IPP-кодом тогда и только тогда, когда для любого потомка пересечение всех порождающих коалиций не пусто [7].

Пусть $c \in N_1$, C – произвольный код. Код C является c-TA-кодом тогда и только тогда, когда

$$\forall C_i \in \mathrm{coal_c}(C) \forall w \in \mathrm{desc}(C_i) \forall z \in C\backslash C_i \exists y \in C_i\colon d(w,y) \le d(w,z).$$

Отметим, что код C является c-TA-кодом тогда и только тогда, когда для любого пиратского вектор-номера $w \in \mathrm{desc}_c(C)$ ближайшим кодовым словом является элемент y, входящий в каждую из создающих его коалиций. Этот элемент в [7] предлагается находить переборным декодером.

Сформулируем лемму, содержащую необходимые далее результаты работы [7] о c-TA-кодах и c-IPP-кодах.

Лемма 1 ([7], раздел 1.3). Пусть $c \in N_1$, C – произвольный код длины n с минимальным расстоянием d и мощностью N над полем Галуа $\mathbf{F}_q$. Тогда

1) если для кода C выполняется условие

$$d > n - \frac{n}{c^2},$$

то код C является c-TA-кодом и выполняется условие

$$\forall C_0 \in \mathrm{coal}_c(C) \forall w \in \mathbf{F}_q^n\colon w \in \mathrm{desc}(C_0)\backslash C_0 \Rightarrow$$

$$\emptyset \neq \left(B\left(w, n - \frac{n}{c}\right) \cap C\right) \subseteq C_0,$$

2) если выполняется условие

$$q \le c < N,$$

то код C не является c-IPP-кодом;

3) если код C является c-TA-кодом, то код C является c-IPP-кодом;

4) если код C является c-TA-кодом, то код C является c-FP-кодом.

Для построения ССШШ используют, в частности, c-IPP-коды и c-TA-коды [2], [4], [6], [7].

Лемма 2 ([8], раздел 3.1). Пусть $c \in N_1$, C – линейный код длины n с минимальным расстоянием d над полем Галуа $\mathbf{F}_q$ и пусть выполняется равенство

$$n - Z_c(C) + 1 \le q.$$

Код C является c-TA-кодом тогда и только тогда, когда выполняется неравенство

$$c < \frac{n}{Z_c(C)}.$$

Следствие ([8], раздел 3.2). Пусть $c \in N_1$, C – циклический код длины n с минимальным расстоянием d над полем Галуа $\mathbf{F}_q$. Тогда для кода C выполняется условие

$$Z_c(C) = c(n-d).$$

Для построения эффективной ССШШ удобно использовать c-ТА-коды [4], [6].

Теорема 1 ([4], раздел 3). Пусть $c \in N_1$, r, m ($\in \mathbf{N}$) такие, что выполняется условие $r < q$, а $C - \mathrm{RM}_q(r,m)$-код над полем $\mathbf{F}_q$, E – определено в (1). Если выполняется условие

$$c \le B_0(C) = \left\lfloor \sqrt{\frac{q}{r}} \right\rfloor, \tag{2}$$

то, во-первых, код C является c-ТА-кодом, а во-вторых

$$\forall C_0 \in \mathrm{coal}_c(C) \forall w \in \mathbf{F}_q^n : w \in \mathrm{desc}(C_0) \backslash C_0 \Rightarrow \emptyset \neq (B(w,E) \cap C) \subseteq C_0.$$

Рассмотрим q-ичный код Рида-Маллера с параметрами такими, что выполняется условие (2). Тогда по теореме 1 код C является c-ТА-кодом и может быть использован для защиты от коалиционных атак [2]. При этом при обнаружении пиратского вектор-номера w применяется следующий порядок действий котроллера: подать q, r и m и вектор w на вход Алгоритма 1 и на выходе получить список $b(\subseteq C)$ легальных вектор-номеров из коалиции. Из того, что c-ТА-коды является и c-FP-кодами, следует, что помимо возможности эффективного поиска злоумышленников в модели исключается возможность прямой компрометации невиновных пользователей. Под компрометацией пользователя контроллером будем понимать существование такого потомка из $\mathrm{desc}_c(C)$, что применение к нему декодера дает список, включающий вектор-номер данного пользователя.

4. Исследования схемы специального широковещательного шифрования, основанной на q-ичных кодах Рида–Маллера и списочном декодере для них, в случае превышения пороговой мощности коалиции. Формулировка основных результатов. Выше отмечено, что условие $c \le B_0(C)$ является необходимым условием корректной работы эффективной ССШШ. В случае превышения мощности коалиции порога $B_0(C)$ корректная работа модели не гарантируется. Согласно [9] возможны следующие ситуации результата работы контроллера.

1. Для пиратского вектор-номера w получен непустой список $b(\subseteq C)$ легальных вектор-номеров из коалиции, однако, в нем оказались вектор-номера невиновных пользователей. Это событие назовем компрометацией невиновного пользователя списочным декодером Пелликаана (см. Алгоритм 1).

2. Ближайшим к w является вектор-номер невиновного пользователя. Это событие назовем компрометацией невиновного пользователя переборным декодером.

3. Вектор-номер w нелегальный, однако полученный от контроллера список пуст. Это событие не приводит к компрометации невиновного пользователя.

4. Вектор-номер w легальный, но создан некоторой коалицией ($w \in \mathrm{desc}_c(C) \cap C$). Это событие назовем прямой компрометацией невиновного пользователя.

В случае 4 контроллер не имеет возможности обнаружить факт коалиционной атаки. В случае 3 контроллер обнаружит факт коалиционной атаки с превышением мощности коалиции допустимого порога $B_0(C)$, но предпринять каких-либо действий не сможет. В случаях 1 и 2 контроллер рассмотрит список вектор-номеров, в котором в качестве вектор-номера злоумышленника имеет смысл рассматривать вектор-номер, ближайший к w.

Аналогично [6] введем классификацию различных случаев нарушения (1). Пусть $\mathbf{N}$ – множество натуральных чисел, $N_1 = \mathbf{N} \backslash \{1\}$, $r, m \in \mathbf{N}$, $C - \mathrm{RM}_q(r,m)$-код, $E = \left\lfloor n - \sqrt{n(n-d)} - 1 \right\rfloor$. Рассмотрим множества $\Omega_i(C)$, называемые областями компрометации кода C. Пусть

$$\Omega_1(C) = \{c \in N_1 : \exists v \in C\ \exists C_0 \in \mathrm{coal_c}(C \backslash \{v\})\ \exists w \in \mathrm{desc}(C_0) \backslash C_0 : d(v,w) \le E\}.$$

Область $\Omega_1(C)$ кода C это множество мощностей таких коалиций, при которых для некоторого кодового слова существует коалиция, у которой хотя бы один из потомков расположен на расстоянии не далее E от данного кодового слова. Очевидно, что $\Omega_1(C)$ – множество таких значений $c \in N_1$, при которых для кода C существует возможность компрометации некоторого невиновного пользователя в результате применения Алгоритма 1 к потомку коалиции. Пусть

$$\Omega_2(C) = \{c \in N_1 : \exists v \in C\ \exists C_0 \in \mathrm{coal_c}(C \backslash \{v\}) \exists w \in \mathrm{desc}(C_0) \backslash C_0 \forall u \in C_0 : d(v,w) \le d(w,u)\}.$$

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

$$\Omega_3(C) = \{c \in N_1 : \exists v \in C\ \exists C_0 \in \mathrm{coal_c}(C \backslash \{v\}) : v \in \mathrm{desc}(C_0) \backslash C_0\}.$$

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. Пусть

$$\Omega_4(C) = \{c \in N_1 : \exists w \in \mathrm{desc_c}(C) \bigcap_{\{i : w \in \mathrm{desc}(C_i)\}} C_i = \emptyset\}.$$

Область $\Omega_4(C)$ кода C это множество мощностей таких коалиций, у которых не имеется возможности определить ни одного члена коалиции по некоторому ее потомку.

Отметим, что сдвиг двух точек пространства $\mathbf{F}_q^n$ 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 $\Omega_i(C)$ состоит из таких $c \in N_1$, при которых возможна соответствующая компрометация не только одного, но и нескольких пользователей.

Очевидно, $\Omega_i(C)$ – целочисленный отрезок вида: $\Omega_i(C) = \{R_i(r,m); \ldots; |C|\}$, где $R_i(r,m)$ – величина, называемая рубежом областей компрометации $\Omega_i(C)$. Далее будем использовать следующие обозначения:

$$R_i(r, \max) = \max_{m \in \mathbf{N}} R_i(r,m);\ R_i(r, \min) = \min_{m \in \mathbf{N}} R_i(r,m).$$

Непосредственно из определений вытекает справедливость вложения

$$\Omega_3(C) \subseteq \Omega_2(C).$$

В зависимости от конкретных условий, при которых проектируется ССШШ, вычисление рубежей $R_i(r,m)$ позволяет уточнить параметры используемого кода и декодера для того, чтобы уменьшить негативные последствия возможности превышения пороговой мощности коалиции злоумышленников. Действительно, если мощность c коалиции злоумышленников превышает рубеж $R_1(r,m)$, то возможна компрометация невиновного пользователя списочным декодером. Если мощность c коалиции злоумышленников превышает рубеж $R_2(r,m)$, то возможна компрометация невиновного пользователя переборным декодером. Если мощность c коалиции злоумышленников превышает рубеж $R_3(r,m)$, то возможна прямая компрометация невиновного пользователя.

Непосредственный расчет рубежей $R_i(r,m)$ является достаточно непростой комбинаторной задачей, поэтому если $R_i(r,m)$ для некоторого i вычислить не удается, то интерес представляет задача получения границ для значений $R_i(r,m)$. Для решения этих задач введем следующие величины:

$$B_1(q,r) = \left\lceil \sqrt{\frac{q}{r}} \right\rceil,\ B_2(q,r,m) = \left\lceil \frac{q}{r} - \frac{1}{rq^{m-2}} + \frac{1}{rq^{m-1}} \right\rceil,\ B_4(q) = q.$$

Очевидно, выполняются неравенства

$$B_1(q,r) \le B_2(q,r,m) \le B_4(q).$$

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

Теорема 2. Пусть $c \in N_1$, $r, m \in \mathbf{N}$, а $C = \mathrm{RM}_q(r,m)$ – q-ичный код Рида-Малера. Если выполняется условие $r < q$, то рубежи $R_1(r,m)$, $R_2(r,m)$, $R_3(r,m)$ и $R_4(r,m)$ имеют следующие границы

$$B_1(q,r) \le R_1(r,\min),\ R_2(r,\max) \le B_2(q,r,m) \le R_3(r,\min),$$
$$R_4(r,\max) \le R_3(r,\min),\ R_4(r,\max) \le B_4(q).$$

Если выполняется условие $r \ge q$, то выполняется равенство

$$R_2(r,m) = 2.$$

Если выполняется условие $9r \le q$, $C \ne \mathrm{RM}_2(1,1)$, тогда выполняется неравенства

$$R_1(r,m) \le R_2(r,m).$$

Доказательство теоремы 2 основывается на результатах работ [2], [3] и [6] и публикуется отдельно. Полученные теоретические результаты можно использовать в ходе проектирования ССШШ при выборе значений параметров r и q применяемого в ССШШ q-ичного кода Рида-Маллера. Представленные границы позволяют делать вывод о возможности различных типов компрометации контроллером невиновных пользователей в случае атаки коалиции мощности c, превосходящей порог $B_0(C)$.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Silverberg A., Staddon J., Walker J.* Application of list decoding to tracing traitors // In Adv. in Cryptology – ASIACRYPT 2001 (LNCS 2248). – 2001. – P. 175-192.
2. *Евпак С.А., Мкртичян В.В.* Исследование возможности применения *q*-ичных кодов Рида-Маллера в схемах специального широковещательного шифрования // Известия вузов. Северо-Кавказский регион. Естественные науки. – 2011. – № 5. – С. 11-15.
3. *Евпак С.А., Мкртичян В.В.* Об исследовании возможности применения *q*-ичных кодов Рида-Маллера в специальных схемах защиты информации от НСД // Обозрение Прикладной и Промышленной Математики. – 2011. – Т. 18. Вып. 2. – С. 268-269.
4. *Евпак С.А., Мкртичян В.В.* Применение *q*-ичных кодов Рида-Маллера в схемах специального широковещательного шифрования // Труды научной школы И.Б. Симоненко. – Ростов-на-Дону: ЮФУ, 2010. – С. 93-99.
5. *Pellikaan R., Wu X.-W.* List decoding of *q*-ary Reed-Muller Codes // IEEE Trans. On Information Theory. – 2004. – Vol. 50 (4). – P. 679-682.
6. *Деундяк В.М., Мкртичян В.В.* Математическая модель эффективной схемы специального широковещательного шифрования и исследование границ ее применения // Известия вузов. Северо-Кавказский регион. Естественные науки. – 2009. – № 1. – С. 5-8.
7. *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.
8. *Fernandez M., Cotrina J., Sorario M. and Domingo N.* A note about the traceability properties of linear codes // In Information Security and Cryptology – ICISC 2007 (LNCS 4817). – 2007. – P. 251-258.
9. *Деундяк В.М., Мкртичян В.В.* Исследование границ применения схемы защиты информации, основанной на РС-кодах // Дискретный анализ и исследование операций. – 2011. – Т. 18, № 1. – С. 21-38.

Статью рекомендовал к опубликованию к.т.н., доцент Н.С. Могилевская.

Евпак Сергей Александрович – Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Южный федеральный университет»; e-mail: sergej-evpak@yandex.ru; 344029, г. Ростов-на-Дону, пр. Маршала Жукова, 30/95, кв. 365; тел.: 89094142919; кафедра алгебры и дискретной математики факультета математики, механики и компьютерных наук; аспирант.

Мкртичян Вячеслав Виталиевич – ФГАНУ НИИ "Спецвузавтоматика"; e-mail: realdeal@bk.ru; 344015, г. Ростов-на-Дону, ул. Малиновского, 72/2, кв. 136; тел.: 88632202486, 89044417791; старший научный сотрудник.

Yevpak Sergey Alexandrovich – Federal State-Owned Autonomy Educational Establishment of Higher Vocational Education “Southern Federal University”; e-mail: sergej-evpak@yandex.ru; 30/95, Marshal Zhukov avenue, 365 flat, Rostov-on-Don, 344029, Russia; phone: +79094142919; the department of the algebra and discrete mathematics of the faculty of mathematics, mechanics and computer sciences; postgraduate student.

Mkrtichan Vyacheslav Vitalievich – FSSI RI "Spetsvuzavtomatika"; e-mail: realdeal@bk.ru; 72/2, Malinovskogo street, 136 flat, Rostov-on-Don, 344015, Russia; phones: +78632202486, +79044417791; senior researcher.

УДК 517.19

Е.А. Михайлова

СИСТЕМА ЗАЩИТЫ МАК-ЭЛИСА В СЛУЧАЙНЫХ СЕТЯХ НА БАЗЕ СЕТЕВОГО КОДА РИДА-СОЛОМОНА*

Рассматривается задача защищенной от помех и наблюдателя передачи одной и той же информации от одного источника некоторому количеству получателей в сети неизвестной структуры. Задача решается на основе предложенного Кёттером и Кшишангом метода случайного сетевого кодирования. В этом методе сеть представляется графом неизвестной структуры, в узлах которого над пришедшими пакетами совершаются случайные линейные преобразования. В работе построена модель сетевого канала, использующего линейное сетевое кодирование, рассмотрены предложенные Кёттером и Кшишангом подпространственные сетевые коды Рида-Соломона, обеспечивающие эффективную помехоустойчивую передачу данных по такому сетевому каналу. Представлены алгоритмы кодирования и декодирования. Построена новая матричная интерпретация кодирования, приведен соответствующий алгоритм. На базе сетевых кодов Рида-Соломона в их матричной интерпретации построена система защиты с открытым ключом, являющаяся некоторым аналогом известной криптосистемы Мак-Элиса. Целью построенной системы защиты является защищенная передача от одного отправителя, знающего открытый ключ, нескольким получателям, владеющим общим секретным ключом, некоторого одинакового набора данных. Приведены алгоритмы шифрования и расшифрования для построенной системы защиты, доказана теорема о корректности работы алгоритмов. В заключение построена симметричная версия системы защиты, изменены соответствующие алгоритмы, отмечены достоинства и недостатки симметричной версии.

Помехоустойчивое кодирование; сетевые коды Рида-Соломона; случайная линейная сеть; система защиты с открытым ключом; криптосистема Мак-Элиса.

E.A. Mikhailova

MCELICE SECURITY SYSTEM IN RANDOM NETWORK BASED ON REED-SOLOMON NETWORK CODE

The problem of error-correction transmission of the same data from one source to several receivers in wiretapped network of unknown structure is considered. The solution based on random network coding technique provided by Koetter and Kschischang. In this method network represent as an unknown structured graph, where each intermediate node creates a random linear combination of the received data and transmits this random combination. The network channel model, using a linear network coding, is constructed. Network subspace Reed-Solomon codes pro-

* Работа подержана грантом ЮФУ на 2013 год ИТ-213.01-24/2013-147.