Владикавказский математический журнал
2014, Том 16, Выпуск 2, С. 38–45

УДК **004.056**

УСЛОВИЯ ПРИМЕНЕНИЯ q-ИЧНЫХ КОДОВ РИДА — МАЛЛЕРА В СПЕЦИАЛЬНЫХ СХЕМАХ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

С. А. Евпак, В. В. Мкртичян

В работе исследуется специальная схема защиты легально тиражируемых данных от несанкционированного доступа. Для q-ичных кодов Рида — Маллера получены условия, при которых их применение в схемах специального широковещательного шифрования (ССШШ) оправдано и не оправдано с точки зрения задачи поиска злоумышленников, объединяющихся в коалицию для создания пиратских ключей.

Ключевые слова: помехоустойчивые коды, схема специального широковещательного шифрования, коалиция, потомки, TA-коды, IPP-коды, q-ичные коды Рида — Маллера.

Проблема защиты легально тиражируемых цифровых данных от несанкционированного доступа является актуальной. Будем рассматривать ситуацию, в которой поставщик распространяет цифровую продукцию. При этом доступ к распространяемой продукции должны получать только покупающие ее легальные пользователи. Для решения этой задачи в [1] рассмотрена схема специального широковещательного шифрования (ССШШ).

1. Схема специального широковещательного шифрования, постановка задачи. В этой схеме защищаемые данные тиражируются свободно в зашифрованном виде, а каждому легальному пользователю выдается уникальный набор ключей, причем в случае обнаружения нелегального использования такого набора его владелец может быть идентифицирован контроллером. Однако ССШШ допускает атаки следующего вида: злоумышленники, являющиеся легальными пользователями, могут объединяться в коалиции мощности c и, комбинируя специальным образом ключи из своих наборов, конструировать новые (пиратские) наборы, которые можно использовать для расшифрования данных, причем эти пиратские наборы злоумышленники могут нелегально распространять, уклоняясь от обнаружения. Для борьбы с такими коалиционными атаками в [2] предложен основанный на помехоустойчивом кодировании метод обнаружения членов коалиций. В частности, доказано, что для эффективного поиска всей коалиции мощности c, или по крайней мере ее непустого подмножества, можно применять обобщенные коды Рида — Соломона (ОРС-коды) с параметрами, зависящими от c.

Целью настоящей работы является исследование условий возможности применения q-ичных кодов Рида — Маллера в схемах специального широковещательного шифрования.

2. Сведения о кодах, применяемых в схемах специального широковещательного шифрования. Пусть $\mathbb{N}$ — множество натуральных чисел, $\mathbb{N}_1 = \mathbb{N}\backslash\{1\}$, $|A|$ — мощность произвольного конечного множества A, C_m^n — количество сочетаний из m по n.

© 2014 Евпак С. А., Мкртичян В. В.

Далее i-ую координату произвольного вектора $\mathbf{x}$ будем обозначать $\mathbf{x}_i$, а линейное n-мерное пространство Хемминга над полем Галуа $\mathbf{F}_q$ обозначим через $\mathbf{F}_q^n$, где $q = p^l$, p — простое число, $l \in \mathbb{N}$. Пусть $C(\subseteq \mathbf{F}_q^n)$ — произвольный код длины n с минимальным расстоянием d над полем $\mathbf{F}_q$. Множеством c-коалиций $\mathrm{coal}_c(C)$ кода C, где $c \in \mathbb{N}$, назовем множество всех его непустых подмножеств мощности не более c. Очевидно, что

$$|\mathrm{coal}_c(C)| = \sum_{i=1}^{c} C_{|C|}^i.$$

Под множеством потомков коалиции $C_0 \in \mathrm{coal}_c(C)$ будем понимать

$$\mathrm{desc}(C_0) = \big\{\mathbf{w} \in \mathbf{F}_q^n : \mathbf{w}_i \in \{\mathbf{a}_i : \mathbf{a} \in C_0\} \quad \forall\, i \in \{1, \ldots, n\}\big\}.$$

Для потомка $\mathbf{w}$ коалицию C_0 будем называть порождающей. Пиратским вектор-номером коалиции $C_0 \in \mathrm{coal}_c(C)$ назовем элемент множества $\mathrm{desc}(C_0) \setminus C_0$. Под множеством c-потомков кода C будем понимать

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

Через $Z_c(C)$ будем обозначать максимальное число нулей в пиратском вектор-номере, который может быть порожден коалицией размера c из множества $C \setminus \{0\}$. Для величины $Z_c(C)$ выполняются неравенства

$$n - d \leqslant Z_c(C) \leqslant \min\{c(n-d), n\}. \tag{1}$$

Действительно, ввиду того, что минимальный вес слова кода C равен d, произвольная коалиция мощности 1 из $\mathrm{coal}_c(C)$ может породить пиратский вектор-номер, содержащий не более чем $n-d$ нулей. Значит, произвольная коалиция мощности c из $\mathrm{coal}_c(C)$ может породить пиратский вектор-номер, содержащий не более чем $c(n-d)$ нулей. При этом такая коалиция породить пиратский вектор-номер, содержащий более чем n нулей, не может.

Пусть $c \in \mathbb{N}_1$, C — произвольный код. Код C является c-TA-кодом тогда и только тогда, когда

$$(\forall\, C_i \in \mathrm{coal}_c(C))\ (\forall\, \mathbf{w} \in \mathrm{desc}(C_i))\ (\forall\, \mathbf{z} \in C \setminus C_i)\ (\exists\, \mathbf{y} \in C_i) \quad d(\mathbf{w}, \mathbf{y}) < d(\mathbf{w}, \mathbf{z}).$$

Отметим, что код является c-TA-кодом тогда и только тогда, когда ближайшим кодовым словом к любому потомку является элемент породившей его коалиции [3].

Пусть $c \in \mathbb{N}_1$, C — произвольный код. Код является c-IPP-кодом тогда и только тогда, когда

$$(\forall\, \mathbf{w} \in \mathrm{desc}_c(C)) \qquad \bigcap_{\{C_i (\in \mathrm{coal}_c(C)) :\, \mathbf{w} \in \mathrm{desc}(C_i)\}} C_i \neq \varnothing.$$

Отметим, что код является c-IPP-кодом тогда и только тогда, когда для любого потомка пересечение всех порождающих коалиций не пусто [3]. Сформулируем лемму, содержащую необходимые далее результаты работы [3] о c-TA-кодах и c-IPP-кодах.

Лемма 1 [3, раздел 1.3]**.** *Пусть $c \in \mathbb{N}_1$, 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;*

2) *если выполняется условие $q \leqslant c < N$, то код C не является c-IPP-кодом;*

3) *если код является c-TA-кодом, то код является c-IPP-кодом.*

Для построения математической модели эффективной ССШШ удобно использовать c-ТА-коды [4]. В работе [5, раздел 3.1] доказывается следующая

Теорема 1 [5, раздел 3.1]**.** *Пусть $c \in \mathbb{N}_1$, $C(\subseteq \mathbf{F}_q^n)$ — линейный код длины n с минимальным расстоянием d над полем $\mathbf{F}_q$. И пусть выполняется неравенство*

$$n - Z_c(C) + 1 < q. \tag{2}$$

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

$$c < \frac{n}{Z_c(C)}. \tag{3}$$

Из раздела 3.2 работы [5] вытекает

Следствие. *Пусть $c \in \mathbb{N}_1$, $C(\subseteq \mathbf{F}_q^n)$ — циклический код длины n с минимальным расстоянием d над полем $\mathbf{F}_q$. Тогда для кода C выполняется условие*

$$Z_c(C) = \min\{c(n-d), n\}.$$

Далее определим q-ичные коды Рида — Маллера. Пусть $\mathbf{F}_q[X_1, X_2, \ldots, X_m]$ — кольцо полиномов m переменных с коэффициентами из поля Галуа $\mathbf{F}_q$, $\mathbf{F}_q^r[X_1, X_2, \ldots, X_m]$ — подпространство полиномов степени не выше r кольца $\mathbf{F}_q[X_1, X_2, \ldots, X_m]$, степень монома

$$X_1^{t_1} X_2^{t_2} \ldots X_m^{t_m} (\in \mathbf{F}_q[X_1, X_2, \ldots, X_m])$$

есть $\sum_{i=1}^m t_i$, а степень $\deg(f)$ полинома $f \in \mathbf{F}_q[X_1, X_2, \ldots, X_m]$ есть максимальная из степеней входящих в него мономов. Пусть, кроме того, $\mathbf{P_1}, \mathbf{P_2}, \ldots, \mathbf{P_n}$ — фиксированное упорядочение элементов пространства Хемминга $\mathbf{F}_q^m = \mathbf{F}_q \times \ldots \times \mathbf{F}_q$, где $n = q^m$. Тогда q-ичный код Рида — Маллера $\mathrm{RM}_q(r, m)$ порядка r определяется следующим образом [6]:

$$\mathrm{RM}_q(r, m) = \big\{(f(\mathbf{P_1}), f(\mathbf{P_2}), \ldots, f(\mathbf{P_n})) : f \in \mathbf{F}_q^r[X_1, X_2, \ldots, X_m]\big\}.$$

Из леммы 2 работы [7] вытекает, что для произвольного набора параметров r, q и m код $\mathrm{RM}_q(r, m)$ совпадает с кодом $\mathrm{RM}_q(r', m)$, для порядка r' которого выполняется условие $r' \leqslant m(q-1)$. Таким образом, не теряя общности, можно считать, что для кода $\mathrm{RM}_q(r, m)$ выполняется оценка

$$r \leqslant m(q-1). \tag{4}$$

3. Основные результаты. В работе [7] представлена следующая

Теорема 2. *Пусть $c \in \mathbb{N}_1$, $r, m (\in \mathbb{N})$ такие, что выполняется условие $r < q$, а C — $\mathrm{RM}_q(r, m)$-код над полем $\mathbf{F}_q$. Если выполняется условие $c < \sqrt{\frac{q}{r}}$, то код C является c-TA-кодом.*

Доказательство теоремы 2 опубликовано в [7] и основывается, в частности, на лемме 1 и результатах работы [6]. Из леммы 1 вытекает, что при $q \leqslant c < N$ код не является c-ТА-кодом. Таким образом, открытым остается вопрос о том, будет ли код $\mathrm{RM}_q(r, m)$ являться либо не являться c-ТА-кодом в случае $c \in \{\lceil\sqrt{\frac{q}{r}}\rceil, \ldots, q-1\}$ для параметров q и r, удовлетворяющих условию $r < q$, и будет ли код $\mathrm{RM}_q(r, m)$ являться либо не являться c-ТА-кодом в случае $c \in \{2, 3, \ldots, q-1\}$ для параметров q и r, удовлетворяющих условию $r \geqslant q$. В теореме 3 представлен ответ на этот вопрос для случая $r \geqslant q$. В теореме 4

представлен ответ для случая $r < q$ при $c \in \{\frac{q}{r}, \dots, q-1\}$. Сформулируем леммы, содержащие необходимые далее результаты.

Лемма 2. *Пусть $c \in \mathbb{N}_1$, $r, m (\in \mathbb{N})$, C — $\mathrm{RM}_q(r,m)$-код над полем $\mathbf{F}_q$. Тогда для кода C выполняется условие*

$$Z_c(C) = \min\{c(n-d), n\}.$$

$\lhd$ В соответствии с работой [6] код C является расширением циклического кода $C^* = \mathrm{RM}_q^*(r,m)$, где

$$\mathrm{RM}_q^*(r,m) = \big\{(f(\mathbf{P_2}), \dots, f(\mathbf{P_n})) : f \in \mathbf{F}_q^r[X_1, X_2, \dots, X_m]\big\},$$

а $\mathbf{P_1}, \mathbf{P_2}, \dots, \mathbf{P_n}$ — фиксированное упорядочение элементов пространства Хемминга $\mathbf{F}_q^m$ такое, что $\mathbf{P_1} = (0,0,\dots,0) \in \mathbf{F}_q^m$, $n = q^m$. Из следствия теоремы 1 для кода C^* выполняется равенство $Z_c(C^*) = \min\{c(\acute{n} - \acute{d}), \acute{n}\}$, где $\acute{n}$ — длина кода C^*, а $\acute{d}$ — его минимальное расстояние. Код C получается из кода C^* добавлением в начало одной координаты, равной $f(\mathbf{P_1}) \in \mathbf{F}_q$. Отсюда вытекает, что $n = \acute{n} + 1$. Кроме того, из [6] следует, что для кода C минимальное расстояние d равно $\acute{d}+1$. В общем случае величина $f(\mathbf{P_1})$ может быть равной или не равной 0 (например, для $f(X_1, \dots, X_m) = X_1 + X_2 + \dots + X_m$ или $f(X_1, \dots, X_m) = 2$ соответственно). Тогда выполняются неравенство $Z_c(C) \geqslant Z_c(C^*)$ и равенство

$$Z_c(C^*) = \min\big\{c(\acute{n} - \acute{d}), \acute{n}\big\} = \min\big\{c(n-1-(d-1)), n-1\big\} = \min\big\{c(n-d), n-1\big\}.$$

Кроме того, в силу (1) выполняется оценка $Z_c(C) \leqslant \min\{c(n-d), n\}$. Рассмотрим случай, при котором выполняется равенство $\min\{c(n-d), n-1\} = c(n-d)$. Тогда, во-первых, выполняется неравенство $Z_c(C) \geqslant c(n-d)$, а, во-вторых, выполняется неравенство $Z_c(C) \leqslant c(n-d)$. Значит, если выполняется равенство $\min\{c(n-d), n-1\} = c(n-d)$, то выполняется равенство

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

Рассмотрим случай, при котором выполняется равенство $\min\{c(n-d), n-1\} = n-1$. Пусть $\varphi^* : \mathbf{F}_q^r[X_1, X_2, \dots, X_m] \to \mathbf{F}_q^{n-1}$ является кодирующим отображением кода C^*, а $\varphi : \mathbf{F}_q^r[X_1, X_2, \dots, X_m] \to \mathbf{F}_q^n$ является кодирующим отображением кода C, т. е.

$$\varphi^*(f) = (f(\mathbf{P}_2), \dots, f(\mathbf{P}_n)), \quad \varphi(f) = (f(\mathbf{P}_1), \dots, f(\mathbf{P}_n)).$$

Пусть $C_0 = \{\mathbf{v_1}, \dots, \mathbf{v_c}\} (\in \mathrm{coal}_c(C^*))$ — такая коалиция кода C^*, что максимальное число нулей в порождаемом ей пиратском вектор-номере равно $n-1$, где $\mathbf{v_i} = \varphi^*(f_i)$, $f_i \in \mathbf{F}_q^r[X_1, X_2, \dots, X_m]$, $i \in \{1, \dots, c\}$. В коде C рассмотрим коалицию $C_1 = \{\mathbf{u_1}, \dots, \mathbf{u_c}\} (\in \mathrm{coal}_c(C))$ следующего вида:

$$\mathbf{u_i} = \varphi(X_1 f_i \bmod X_1^q),$$

где $i \in \{1, \dots, c\}$. Тогда выполняются равенства $\mathbf{u}_{\mathbf{1},0} = 0, \dots, \mathbf{u}_{\mathbf{c},0} = 0$. Значит, если выполняется равенство $Z_c(C^*) = \min\{c\,(n-d), n-1\} = n-1$, то выполняется равенство $Z_c(C) = n$.

Если $c(n-d) \geqslant n$, то выполняется равенство $\min\{c\,(n-d), n\} = n$, а, значит, $\min\{c\,(n-d), n-1\} = n-1$. Тогда выполняется равенство $Z_c(C) = n$. Если же $c\,(n-d) < n$, то выполняется равенство $\min\{c\,(n-d), n\} = c\,(n-d)$ и, в то же время, выполняется равенство $\min\{c\,(n-d), n-1\} = c(n-d)$. Тогда выполняется равенство $Z_c(C) = c\,(n-d)$. Таким образом, имеет место равенство $Z_c(C) = \min\{c\,(n-d), n\}$. $\rhd$

Лемма 3. *Пусть $r, m(\in \mathbb{N})$, C — $\mathrm{RM}_q(r,m)$-код над полем $\mathbf{F}_q$ с минимальным расстоянием d. Тогда*

1) *если $r < q$, то выполняется условие $d = q^m - rq^{m-1}$;*

2) *если $r \geqslant q$, то выполняется оценка $d \leqslant (q-1)\, q^{m-2}$.*

$\lhd$ Согласно [6] минимальное расстояние q-ичного кода Рида — Маллера $\mathrm{RM}_q(r,m)$ можно вычислить следующим образом:

$$d = (\eta + 1)\, q^{\mu}, \tag{5}$$

где η — остаток от деления $m(q-1)-r$ на $q-1$ с частным μ, т. е. $m(q-1)-r = \mu(q-1)+\eta$, где $\eta < q-1$.

Рассмотрим отдельно каждое из двух условий леммы. Пусть $r < q$. Тогда при делении $m(q-1)-r$ на $q-1$ с остатком получим $m(q-1)-r = (m-1)(q-1)+q-1-r$. Значит, $\eta = q-1-r$, а $\mu = m-1$ и, соответственно,

$$d = (q-r)\, q^{m-1} = q^m - rq^{m-1}.$$

Пусть $r \geqslant q$. Тогда в силу (4) получим

$$q \leqslant r \leqslant m(q-1),$$

$$(q-1)+1 \leqslant r \leqslant (m-1)(q-1)+q-1,$$

Так как $r \geqslant q$, то r представимо в виде $r = x(q-1)+y$. Тогда

$$(q-1)+1 \leqslant x(q-1)+y \leqslant (m-1)(q-1)+q-1,$$

где x и y такие, что выполняются неравенства

$$1 \leqslant x \leqslant m-1, \quad 1 \leqslant y \leqslant q-1.$$

Так как $r = x(q-1)+y$, то

$$m(q-1)-r = (m-x-1)(q-1)+q-1-y.$$

Пусть $\alpha = m-x-1$, $\beta = q-1-y$. Так как выполняется $1 \leqslant y \leqslant q-1$, то $\beta \in \{0, \ldots, q-2\}$, а, значит, β — остаток от деления $m(q-1)-r$ на $q-1$ с частным α. Таким образом, в силу (5) минимальное расстояние кода вычисляется по формуле

$$d = (q-y)\, q^{m-x-1}.$$

В силу неравенств $1 \leqslant x \leqslant m-1$ и $1 \leqslant y \leqslant q-1$ получим

$$d \leqslant (q-1)\, q^{m-2}. \rhd$$

Теорема 3. *Пусть $c \in \mathbb{N}_1$, $r \geqslant q$, $C = \mathrm{RM}_q(r,m)$-код над полем $\mathbf{F}_q$. Тогда код C не является c-ТА-кодом.*

$\lhd$ Согласно лемме 3 для минимального расстояния d кода C в случае $r \geqslant q$ выполняется оценка

$$d \leqslant (q-1)\, q^{m-2}.$$

Отсюда следует

$$c(q^m - q^{m-1} + q^{m-2}) \leqslant c(n-d). \tag{6}$$

Оценим величину $n - Z_c(C) + 1$.

По лемме 2 для кода C выполняется равенство

$$Z_c(C) = \min\{c(n-d), n\}.$$

В случае $Z_c(C) = n$ выполняется равенство $n - Z_c(C) + 1 = 1$, а значит, по теореме 1 код C не является c-ТА-кодом.

Рассмотрим случай, когда выполняется равенство $Z_c(C) = c(n-d)$. Ввиду (6) получим равенство

$$n - Z_c(C) + 1 = q^m - c(n-d) + 1 \leqslant q^m - c(q^m - q^{m-1} + q^{m-2}) + 1. \tag{7}$$

Проверим выполнение неравенства

$$q^m - c(q^m - q^{m-1} + q^{m-2}) + 1 < q.$$

Последнее эквивалентно

$$1 < \frac{1}{q^{m-1}} - \frac{1}{q^m} + c\left(1 - \frac{1}{q} + \frac{1}{q^2}\right). \tag{8}$$

Так как третье слагаемое возрастает при возрастании величины q, и его минимальное значение равно $1,5$ при $q = 2$, и так как второе слагаемое меньше первого, то неравенство (8) выполняется при любых $c \in \mathbb{N}_1$, $q \geqslant 2$ и $m \in \mathbb{N}$. Тогда из оценок (7) и (8) следует, что для любых $c \in \mathbb{N}_1$, $q \geqslant 2$ и $m \in \mathbb{N}$ выполняется неравенство (2). Из теоремы 2 работы [7] следует, что условие (3) для кода C не выполняется. Таким образом, согласно теореме 1 код C не является c-ТА-кодом. $\triangleright$

Теорема 4. *Пусть $c \in \mathbb{N}_1$, $r < q$, $C = \mathrm{RM}_q(r, m)$-код над полем $\mathbf{F}_q$. Если выполняется условие $c \geqslant \frac{q}{r}$, то код C не является c-ТА-кодом.*

$\triangleleft$ Согласно лемме 3 минимальное расстояние d кода C при $r < q$ вычисляется по формуле $d = q^m - rq^{m-1}$. Тогда $n - d = rq^{m-1}$, где n — длина кода C.

Аналогично доказательству теоремы 3 рассмотрим два случая:

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

Очевидно, что для случая $Z_c(C) = n$ по теореме 1 код C не является c-ТА-кодом.

Рассмотрим случай, при котором выполняется равенство $Z_c(C) = c(n-d)$. Тогда выполняется равенство

$$n - Z_c(C) + 1 = q^m - c(n-d) + 1 = q^m - crq^{m-1} + 1. \tag{9}$$

Поставив формулу (9) в формулу (2), получим:

$$q^m - crq^{m-1} + 1 < q.$$

Последнее неравенство эквивалентно

$$1 < \frac{1}{q^{m-1}} - \frac{1}{q^m} + \frac{cr}{q},$$

которое выполняется для любого $c \in \mathbb{N}_1$, удовлетворяющего условию $c \geqslant \frac{q}{r}$, и фиксированного $q \geqslant 2$, $m \in \mathbb{N}$. Значит, для $c(\in \mathbb{N}_1) \geqslant \frac{q}{r}$ условие (2) выполняется.

Пусть для $c(\in \mathbb{N}_1) \geqslant \frac{q}{r}$ выполняется и условие (3). Тогда из равенства для $Z_c(C)$ следует, что

$$c < \frac{n}{c(n-d)}. \tag{10}$$

Так как выполняется условие $c \geqslant \frac{q}{r}$, то из (10) следует

$$\frac{q}{r} \leqslant c < \sqrt{\frac{n}{n-d}}.$$

Однако по условию теоремы выполняется условие $r < q$, значит,

$$\frac{q}{r} < \sqrt{\frac{n}{n-d}} = \sqrt{\frac{q}{r}},$$

чего быть не может. Следовательно, для $c(\in \mathbb{N}_1) \geqslant \frac{q}{r}$ условие (3) не выполняется. Таким образом, при $c(\in \mathbb{N}_1) \geqslant \frac{q}{r}$ для любых значений $Z_c(C)$ кода C условие (2) выполняется, а условие (3) не выполняется, а, значит, по теореме 1 код C не является c-ТА-кодом. ▷

Таким образом, найдены условия, при которых q-ичные коды Рида — Маллера являются c-ТА-кодами, и условия, при которых q-ичные коды Рида — Маллера не являются c-ТА-кодами. Основной результат может быть представлен на рис. 1. Отметим, что в работе [8] опубликованы ключевые теоремы настоящей работы без доказательств.

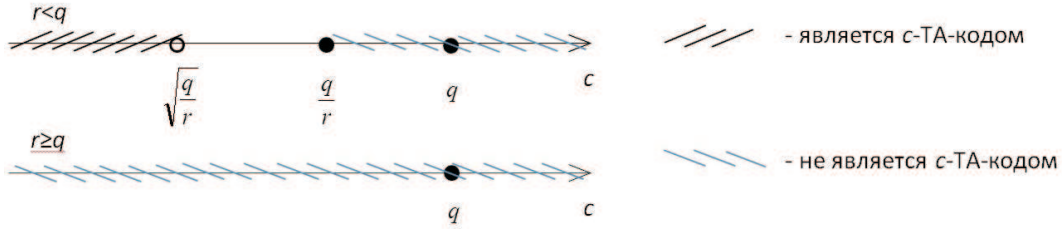

Рис. 1. Условия наличия c-ТА-свойства.

Литература

1. *Chor B., Fiat A., Naor M.* Tracing Traitors // Advances in Cryptology — Crypto 1994.—1994.—P. 257–270.—(Lecture Notes in Computer Science. Vol. 839).
2. *Silverberg A., Staddon J., Walker J.* Application of list decoding to tracing traitors // Advances in Cryptolo — Asiacrypt 2001.—2001.—P. 175–192.—(Lecture Notes in Computer Science. Vol. 2248).
3. *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.
4. *Деундяк В. М., Мкртичян В. В.* Математическая модель эффективной схемы специального широковещательного шифрования и исследование границ ее применения // Изв. вузов. Сев.-Кавк. регион. Естественные науки.—2009.—№ 1.—С. 5–8.
5. *Fernandez M., Cotrina J., Sorario M., Domingo N.* A note about the traceability properties of linear codes // Information Security and Cryptology — ICISC 2007.—2007.—P. 251–258.—(Lecture Notes in Computer Science. Vol. 4817).
6. *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.
7. *Евпак С. А., Мкртичян В. В.* Исследование возможности применения q-ичных кодов Рида — Маллера в схемах специального широковещательного шифрования // Изв. вузов. Сев.-Кавк. регион. Естественные науки.—2011.—№ 5.—С. 11–15.
8. *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.

Статья поступила 16 апреля 2013 г.

Евпак Сергей Александрович
Южный федеральный университет,
аспирант кафедры алгебры и дискретной математики
факультета математики, механики и компьютерных наук
РОССИЯ, 344090, Ростов-на-Дону, ул. Мильчакова, 8 а
E-mail: sergej-evpak@yandex.ru

Мкртичян Вячеслав Виталиевич
ФГАНУ НИИ «Спецвузавтоматика»,
старший научный сотрудник
РОССИЯ, 344002, Ростов-на-Дону, пер. Газетный, 51
E-mail: realdeal@bk.ru

APPLICABILITY CONDITIONS FOR q-ARY REED–MULLER CODES IN TRAITOR TRACING

Yevpak S. A., Mkrtichan V. V.

The special information protection scheme is investigated. The scheme prevents unauthorized distribution to digital products. The paper introduces the applicability conditions for q-ary Reed–Muller codes in the scheme. These codes help to search malefactors who attack the scheme.

Key words: noise-resistant code, traitor tracing, traceability codes (TA-codes), identifiable parent property (IPP), coalition, descendants, q-ary Reed–Muller codes.