С. А. Евпак, **В. В. Мкртичян** (Ростов-на-Дону, ФГНУ НИИ «Спецвузавтоматика»). **Об исследовании возможности применения q-ичных кодов Рида–Маллера в специальных схемах защиты информации от несанкционированного доступа.**

В работе [1] рассматривается схема специального широковещательного шифрования (ССШШ), применяемая на практике для защиты легально тиражируемых цифровых данных от несанкционированного доступа. Известно, что злоумышленники, являющиеся легальными пользователями ССШШ, могут объединяться в коалиции мощности c и пытаться атаковать ССШШ. В [2] представлена математическая модель эффективной ССШШ на основе кодов Рида–Соломона, для построения которой удобно использовать c-ТА-коды [1]. В работе, представленной данным докладом, исследованы условия возможности применения q-ичных кодов Рида–Маллера в качестве c-ТА-кодов для построения ССШШ.

Теорема 1. *Пусть $c \in \mathbf{N}\backslash\{1\}$, $C = \mathbf{RM}_q(r, m)$ — q-ичный код Рида–Маллера над полем $\mathbf{F}_q$, $r < q$. Если выполняется условие*

$$c < \sqrt{q/r}, \tag{1}$$

то код C является c*-ТА-кодом.*

Теорема 2. *Пусть $c \in \mathbf{N}\backslash\{1\}$, $C = \mathbf{RM}_q(r, m)$ — q-ичный код Рида–Маллера над полем $\mathbf{F}_q$, $r < q$. Если выполняется условие $c \geqslant q/r$, то код C не является c-ТА-кодом.*

Теорема 3. *Пусть $c \in \mathbf{N}\backslash\{1\}$, $C = \mathbf{RM}_q(r, m)$ — q-ичный код Рида–Маллера над полем Галуа $\mathbf{F}_q$, $r \geqslant q$. Тогда код C не является c-ТА-кодом.*

Теорема 4. *Пусть $C = \mathbf{RM}_q(r, m)$ — q-ичный код Рида–Маллера над полем Галуа $\mathbf{F}_q$, $c \in \mathbf{N}\backslash\{1\}$, $r < q$, для параметра c выполняется оценка* (1)*, $E = \lceil n - \sqrt{n(n-d)} - 1 \rceil$, тогда*

$$\forall C_0 \in \mathrm{coal}_c(C)\ \forall w \in \mathrm{desc}(C_0)\backslash C_0\colon\ \varnothing \neq (B(w, E) \cap C) \subseteq C_0.$$

Доказательства теорем 1 и 4 основываются на результатах работ [1], [3], а теорем 2 и 3 — на результатах работы [4].

Таким образом, найдены условия, при которых q-ичные коды Рида–Маллера являются c-ТА-кодами, и доказано, что множество кодовых слов, находящихся в пределах расстояния E от потомка, не пусто и вложено в создающую его коалицию. Полученные результаты используются при выборе параметров математической модели эффективной ССШШ на основе q-ичных кодов Рида–Маллера [5].

СПИСОК ЛИТЕРАТУРЫ

1. *Silverberg A.*, *Staddon J.*, *Walker J.* Application of list decoding to tracing traitors. — In: Advances in Cryptology — ASIACRYPT 2001 (LNCS 2248), 2001, p. 175–192.
2. *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.
3. *Staddon J. N.*, *Stinson D. R.*, *Wei R.* Combinatorial properties of frameproof and traceability codes. — IEEE Trans. Inf. Theory, 2001, v. 47, p. 1042–1049.
4. *Fernandez M.*, *Cotrina J.*, *Sorario M.*, *Domingo N.* A note about the traceability properties of linear codes. — In: Information Security and Cryptology — ICISC 2007 (LNCS 4817), 2007, p. 251–258.
5. *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: изд-во ЮФУ, 2010, с. 93–99.