Kosolapov Yury Vladimirovich
Federal State-Owned Educational Establishment of Higher Vocational Education «Southern Federal University».
E-mail: itaim@mail.ru.
8a, Milchakova street, Rostov-on-Don, 344090, Russia.
Phone: +79061833020.

Chekunov Evgeny Sergeevich
E-mail: echekunov@gmail.com.
Phone: +79054782547.

УДК 004.056.5

В.В. Мкртичян

СХЕМА СПЕЦИАЛЬНОГО ШИРОКОВЕЩАТЕЛЬНОГО ШИФРОВАНИЯ, ОСНОВАННАЯ НА НЕКОТОРЫХ КОНКАТЕНИРОВАННЫХ КОДАХ, И ИССЛЕДОВАНИЕ ГРАНИЦЫ ЕЕ ПРИМЕНЕНИЯ

Исследуется проблема защиты легально тиражируемой цифровой продукции от несанкционированного распространения. Строится математическая модель схемы специального широковещательного шифрования на основе обобщенных кодов Рида–Соломона конкатенированных с кодами Адамара и декодера Гурусвами–Судана. Разрабатывается программная реализация математической модели. Проводится исследование возможности ее применения в случае превышения допустимого числа членов коалиции злоумышленников.

Коды Рида–Соломона, конкатенированные коды; списочное декодирование; широковещательное шифрование; поиск злоумышленников.

V.V. Mkrtichan

BROADCAST ENCRYPTION SCHEME BASED ON SOME CONCATENATED CODES, RESEARCH OF BOUND OF THE SCHEME APPLYING

The problem of protecting legally replicated digital products from unauthorized distribution.ьConstruct a mathematical model of Skye special broadcast encryption scheme based on generalized Reed-Solomon concatenated with Hadamard codes and deco-dera Guruswami-Sudan.ьDeveloped software implementation of mathematical models.ьWe study its possible use in case of exceeding the allowable number of members of the coalition attackers.

Reed–Solomon codes; concatenated codes; list decoding; broadcast encryption; tracing traitors.

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 [1] доказано, что для эффективного поиска всей коалиции или, по крайней мере, ее непустого подмножества можно применять обобщенный код Рида–Соломона (ОРС-код), специальным образом конкатенированный с кодом Адамара (КОРСА-код). При этом в качестве алгоритма декодирования предлагается использовать эффективный алгоритм списочного декодирования Гурусвами–Судана [2]. В [3] представлена математическая модель и теоретическое исследование эффективной ССШШ для ОРС-кода, в [4], [5] проведено экспериментальное исследование этой схемы. В [6] построена компьютерная модель списочного декодера Гурусвами–Судана для КОРСА-кода, выступающая наиболее сложным элементом

ССШШ. Целью настоящей работы является построение и исследование математической модели эффективной ССШШ на основе КОРСА-кода и списочного декодера Гурусвами–Судана для КОРСА-кода.

2. КОРСА-коды и списочное декодирование. Пусть p – простое, m – натуральное, F_p – поле Галуа, $z_1, \ldots, z_{p^m}$ – фиксированное упорядочение элементов линейного векторного пространства F_p^m. Код Адамара над полем F_p с инициализирующим параметром m задается кодирующим отображением

$$\psi_m: \quad F_p^m \to F_p^{p^m}; \psi_m(a) = (< a, z_1 >, \ldots, < a, z_{p^m} >),$$

где $< a, z_i >$ – скалярное произведение векторов a и z_i Далее этот код будем обозначать как (p^m, m)-А-код.

Для удобного в дальнейшем представления КОРСА-кодов введем ряд обозначений. Пусть p – простое, m – натуральное,

$$r \in \{p^m; 2p^m; 3p^m; \ldots; p^{2m}\}, k \in \{m; 2m; 3m; \ldots; rm/p^m\}, \quad (1)$$

μ_m – биективное отображение, сопоставляющее элементу пространства F_p^m элемент поля F_{p^m} в соответствии с полиномиальным представлением поля

$$k_0 = k/m, r_0 = r/p^m. \quad (2)$$

Рассмотрим биективное отображение:

$$\chi_{m,k}: F_p^k \to F_{p^m}^{k_0-1}[x];$$
$$\chi_{m,k}(a) = \mu_m(a^{(0)}) + \mu_m(a^{(1)})x + \ldots + \mu_m(a^{(k_0-1)})x^{k_0-1},$$

где $a = (a_0, \ldots, a_{k-1})$, $a^{(i)} = (a_{im}, \ldots, a_{(i+1)m-1})$, $i \in \{0; \ldots; k_0 - 1\}$. Очевидно, что отображение $\chi_{m,k}^{-1}$ определяется формулой

$$\chi_{m,k}^{-1}: F_{p^m}^{k_0-1}[x] \to F_p^k; \chi_{m,k}^{-1}\big(p(x)\big) = \Big(\mu_m^{-1}(p_0), \mu_m^{-1}(p_1), \ldots, \mu_m^{-1}\big(p_{k_0-1}\big)\Big),$$

где $p(x) = p_0 + p_1 x + \ldots + p_{k_0-1}x^{k_0-1}$. Рассмотрим отображение:

$$\psi_m^0: F_{p^m} \to F_p^{p^m}; \ \psi_m^0(a) = \psi_m(\mu_m^{-1}(a)),$$

где ψ_m – кодирующее отображение (p^m, m)-А-кода. Пусть $\alpha_1, \ldots, \alpha_{p^m}$ – фиксированное упорядочение элементов F_{p^m}. Рассмотрим также (r_0, k_0)-ОРС-код.

КОРСА-код над полем F_p, получаемый специальным конкатенированием (r_0, k_0)-ОРС-кода над полем F_{p^m} и (p^m, m)-А-кода над полем F_p, имеет инициализирующие параметры m, k, r (см. (1), (2)) и задается кодирующим отображением:

$$\gamma_{m,k,r}: F_p^k \to F_p^r; \gamma_{m,k,r}(a) = (\psi_m^0(p_a(\alpha_1)), \ldots, \quad \psi_m^0(p_a(\alpha_{r_0}))),$$

где $p_a(x) = \chi_{m,k}(a)$ – представление сообщения $a \in F_p^k$ в виде полинома степени не выше $k_0 - 1$ над полем F_{p^m}. При этом "внешним" кодом является (r_0, k_0)-ОРС-код, а "внутренним" кодом – (p^m, m)-А-код.

Отметим, что в приведенном выше определении КОРСА-кода содержится и метод кодирования.

В работе [2] показана теоретическая возможность списочного декодирования КОРСА-кодов, при этом схематично описан метод декодирования, однако точного алгоритма не приводится. В [6] представлен формализованный алгоритм декодирования, на который далее будем ссылаться как на алгоритм 1. Входными параметрами алгоритма являются параметры КОРСА-кода C: параметры полей p и m,

длина r и размерность k кода, упорядочения $\alpha_1,\dots,\alpha_{p^m}$ и $z_1,\dots,z_{p^m}$ элементов F_{p^m} и F_p^m соответственно. При декодировании на вход алгоритма подается слово $y=(y_1,\dots,y_r)\in F_p^r$. Декодер производит поиск всех кодовых слов в пределах сферы, центром которой является y, радиусом – величина

$$E=(1-1/p)(r-\sqrt{rp^m(k/m-1)}\,. \qquad (3)$$

Выходом алгоритма является список всех информационных векторов $b(\in F_p^k)$, удовлетворяющих условию: $d(\gamma_{m,k,r}(b),y)\le E$, где $\gamma_{m,k,r}$ – кодирующее отображение кода C, $d(x,y)$ – метрика Хемминга в F_q^r. Оценка эффективности работы алгоритма 1 списочного декодирования КОРСА-кодов составляет $O(r^2)$.

3. Математическая модель ССШШ, основанной на КОРСА-кодах и списочном декодере для них. Для получения доступа к распространяемым данным пользователь ССШШ получает, в частности, так называемый вектор-номер, являющийся словом помехоустойчивого кода C (см. [1], [3], [5]). 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

$$\mathrm{desc}(C_0)=\{w=(w_1,\dots,w_r)\in F_q^r:\forall i\in\{1;\dots;r\}\ w_i\in C_{0,i}\},$$

где $C_{0,i}$ – множество координат всех вектор-номеров C_0; множество пиратских вектор-номеров коалиции C_0 определяется правилом $\mathrm{desc}(C_0)\backslash C_0$. Пиратские вектор-номера можно применять для нелегального доступа к тиражируемым данным.

Для защиты от коалиционных атак в качестве C используется КОРСА-код такой длины r и размерности k (далее (r,k)-КОРСА-код), над полем F_q такой, что выполняется условие:

$$c\le B_0(C)=\lfloor qr/(q(k/m-1)(q-1)+r)\rfloor,$$

где $q=p^m$, p – простое, m – натуральное, $\alpha_1,\dots,\alpha_{p^m}$ и $z_1,\dots,z_{p^m}$ – фиксированные упорядочения элементов F_{p^m} и F_p^m соответственно. При обнаружении пиратского вектор-номера w применяется следующий порядок действий котроллера: подать p,m,r,k, $\alpha_1,\dots,\alpha_{p^m}$, $z_1,\dots,z_{p^m}$ и вектор w на вход алгоритма 1, и на выходе получить список $b(\subseteq C)$ легальных вектор-номеров из коалиции.

4. Исследование границы применения ССШШ. Выше отмечено, что условие $c\le B_0(C)$ является необходимым условием корректной работы эффективной ССШШ. Аналогично [3] введем классификацию различных случаев его нарушения. Пусть $\mathbf{N}$ – множество натуральных чисел, $N_1=\mathbf{N}\{1\}$, C – (r,k)-КОРСА-код, E – определено в (3). Множество номеров координат совпадения векторов $x=(x_1,\dots,x_r)$, $y=(y_1,\dots,y_r)$ из F_q^r обозначим $I(x,y)$. Метрика Хемминга $d(x,y)$ в F_q^r и множество $I(x,y)$ связаны следующим равенством: $d(x,y)=r-I(x,y)$. 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, у которых имеется возможность компрометации 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.

Очевидно, $\Omega_i(C)$ – целочисленный отрезок вида $\Omega_i(C) = \{R_i(C); \ldots; |C|\}$, где $R_i(C)$ – величина, называемая рубежом области компрометации $\Omega_i(C)$. Непосредственно из определений вытекает справедливость вложения $\Omega_3(C) \subseteq \Omega_2(C)$.

Для рубежа $R_3(C)$ удалось получить верхнюю оценку.

Теорема. Пусть C – (r,k)-КОРСА-код, над полем F_q, где $q = p^m$, p – простое, m – натуральное. Рассмотрим величину

$$\widetilde{R_3}(C) = \lceil r/(p^m(k/m - 1)) \rceil.$$

Тогда для рубежа $R_3(C)$ выполняется оценка $R_3(C) \le \widetilde{R_3}(C)$.

Замечание. Полученные теоретические результаты можно использовать при выборе значений параметров r, k и m применяемого КОРСА-кода при проектировании ССШШ. Именно вычисленное значение границы $\widetilde{R_3}(C)$ позволяет оценить качественную характеристику возможной компрометации невиновных пользователей в случае атаки коалиции мощности c для конкретных параметров r, k и m.

Для доказательства теоремы рассмотрим две вспомогательные леммы. В леммах 1, 2 и доказательстве теоремы в качестве кодирующего отображения (r,k)-КОРСА-кода C будем использовать следующее отображение:

$$\gamma_{m,k_0,r} : F_{p^m}^{k_0-1}[x] \to F_p^r;\ \gamma_{k_0,r}(p(x)) = (\psi(p(\alpha_1)), \ldots, \psi(p(\alpha_{r_0}))),$$

где ψ – кодирующее отображение (p^m, m)-А-кода, $\alpha_1, \ldots, \alpha_{p^m}$ – фиксированные упорядочения элементов поля F_{p^m}, а k_0 и r_0 определены в (2).

Лемма 1. Пусть C – (r,k)-КОРСА-код, над полем F_q. Пусть $p_v(x) \in F_{p^m}^{k_0-1}[x]$, $v = \gamma_{m,k_0,r}(p_v(x))$ – сообщение и соответствующее ему кодовое слово и пусть

$$p_u(x) = p_v(x) - (x - \alpha_{i_1}) \cdot \ldots \cdot (x - \alpha_{i_\delta}),\ u = \gamma_{k_0,r}(p_u(x)),$$

где $\delta = k_0 - 1$, $\{i_1, \ldots, i_\delta\} \subset \{1; \ldots, r_0\}$. Тогда выполняются соотношения

$$v \ne u,\ |I(v,u)| \ge q\delta,\ I(v,u) \supseteq \{I_{i_1}^1; \ldots; I_{i_\delta}^\delta\},$$

где $I_{i_j}^j = \{q(i_j - 1) + 1; \ldots; qi_j\}$, $j \in \{1; \ldots; \delta\}$.

Доказательство. Заметим, что $v \ne u$, так как $p_v(x) - p_u(x) = (x - \alpha_{i_1}) \cdots (x - \alpha_{i_\delta})$ – ненулевой информационный полином. Так как элементы $p_v(\alpha_{i_j})$ и $p_u(\alpha_{i_j})$ поля F_{p^m} совпадают для любого $j \in \{1; \ldots; \delta\}$, то совпадают и векторы $\psi(p_v(\alpha_{i_j}))$ и $\psi(p_u(\alpha_{i_j}))$, а значит выполняется вложение $I(v,u) \supseteq \{I_{i_1}^1; \ldots; I_{i_\delta}^\delta\}$ и неравенство $|I(v,u)| \ge q\delta$.

Лемма 2. Пусть C – (r,k)-КОРСА-код, над полем F_q, где $q = p^m$. Тогда

$$\forall c \in N_1\ \forall v \in C\ \exists C_0 \in \mathrm{coal}_c(C \backslash \{v\})\ \exists w \in \mathrm{desc}(C_0) : |I(v,w)| \ge \min\{p^m(k/m - 1)c, r\}.$$

Доказательство. Чтобы для $c \in N_1$ и $v = (v_1, \dots, v_r) \in C$ построить коалицию $C = \{u_1; \dots; u_c\} \in \text{coal}_c(C \backslash \{v\})$ и элемент $w \in \text{desc}(C_0) \backslash C_0$, рассмотрим два случая.

1. Сначала рассмотрим случай $c < r/(p^m(k/m-1))$. Пусть

$$p_{u_i}(x) = p_v(x) - (x - \alpha_{\delta(i-1)+1}) \cdots (x - \alpha_{\delta i}),$$

где $p_v(x)$ такой, что $\gamma_{m,k_0,r} p_v(x) = v$, $\delta = k_0 - 1$. По лемме 1 для каждого $i \in \{1; \dots; c\}$ выполняется вложение $I(\gamma_{m,k_0,r}(p_{u_i}(x)), v) \supseteq \{I^1_{\delta(i-1)+1}; \dots; I^{\delta}_{\delta i}\}$, где для любого $j \in \{1; \dots; \delta\}$

$$I^j_{\delta(i-1)+j} = \{q(\delta(i-1) + j - 1) + 1; \dots; q(\delta(i-1) + j)\}.$$

Отсюда вытекает, что для каждого $i \in \{1; \dots; c\}$ выполняется вложение

$$I(\gamma_{m,k_0,r}(p_{u_i}(x)), v) \supseteq \{q\delta(i-1) + 1; \dots; q\delta i\},$$

а значит и неравенство $|I(\gamma_{m,k_0,r}(p_{u_i}(x)), v)| \geq q\delta$, причем $u_i = (\gamma_{m,k_0,r}(p_{u_i}(x)) \neq v$. Таким образом, построена коалиция $C = \{u_1; \dots; u_c\} \in \text{coal}_c(C \backslash \{v\})$, для которой

$$\begin{cases} u_i = (v_1, \dots, v_{q\delta}, u_{1,q\delta+1}, \dots u_{1,r}), \\ \dots, \\ u_i = (u_{i,1}, \dots, u_{1,q\delta(i-1)}, v_{q\delta(i-1)+1}, \dots, v_{q\delta i}, u_{i,q\delta i+1}, \dots, u_{i,r}), \\ \dots, \\ u_c = (u_{c,1}, \dots, u_{c,qc(i-1)}, v_{c,qc(i-1)+1}, \dots, v_{q\delta c}, u_{c,q\delta c+1}, \dots, u_{c,r}). \end{cases}$$

Определим

$$w = (v_1, \dots, v_{q\delta c}, w_{q\delta c+1}, \dots w_r),$$

где для каждого $j \in \{q\delta c + 1; \dots; c\}$ координата w_j задается как произвольный элемент из $\{u_{1,j}, \dots, u_{c,j}\}$. Ясно, что $w \in \text{desc}(C_0) \backslash C_0$. По построению выполняется неравенство $|I(v,w)| \geq q\delta c$, а так как $q\delta c = \min\{q\delta c, r\}$, то выполняется неравенство $|I(v,w)| \geq \min\{p^m(k/m-1)c, r\}$.

2. Рассмотрим случай $c \geq r/(p^m(k/m-1))$. Способом, описанным выше, построим первые $\lfloor r/(p^m(k/m-1)) \rfloor$ элементов коалиции C_0. Если $\lfloor r/(p^m(k/m-1)) \rfloor \neq r/(pm(k/m-1))$, то элемент коалиции с номером $r/(pm(k/m-1))$ определим как $\gamma_{m,k_0,r}(p_{u_{\lfloor r/(p^m(k/m-1)) \rfloor}}(x))$,

где $p_{u_{\lfloor r/(p^m(k/m-1)) \rfloor}} = p_v(x) - (x - \alpha_{q\delta(\lfloor r/(p^m(k/m-1)) \rfloor - 1)+1}) \cdot \dots \cdot (x - \alpha_r)$.

Оставшиеся $c - \lfloor r/(p^m(k/m-1)) \rfloor$ элементов коалиции выберем как произвольные кодовые слова, не равные v. Таким образом, построена коалициия $C_0 = \{u_1; \dots; u_c\} \in \text{coal}_c(C \backslash \{v\})$. В качестве $w \in \text{desc}(C_0) \backslash C_0$ выберем $(v_1, \dots, v_r)$. Так как $r = \min\{q\delta c, r\}$, то выполняется неравенство $|I(v,w)| \geq \min\{p^m(\frac{k}{m} - 1)c, r\}$.

Доказательство теоремы. Для проверки неравенства $R_3(C) \leq \widetilde{R_3}(C)$ достаточно показать, что для произвольного $c \geq \widetilde{R_3}(C)$ выполняется условие $c \in \Omega_3(C)$. По определению

$$\Omega_3(C) = \{c \in N_1 : \exists v \in C \; \exists C_0 \in \text{coal}_c(C \backslash \{v\}) : v \in \text{desc}(C_0) \backslash C_0\}.$$

По лемме 2 при $c \geq r/(p^m(k/m-1))$

$$\forall v \in C\ \exists C_0 \in \mathrm{coal}_c(C\backslash\{v\})\ \exists w \in \mathrm{desc}(C_0)\colon |I(v,w)| = r, \text{т. е. } w = v.$$

Значит из неравенства $c \geq r/(p^m(k/m-1))$ следует условие $c \in \Omega_3(C)$. А так как $\widetilde{R_3}(C) = \lceil r/(p^m(k/m-1))\rceil \geq r/(pm(k/m-1))$, то и из неравенства $c \geq \widetilde{R_3}(C)$ следует условие $c \in \Omega_3(C)$. Таким образом, $R_3(C) \leq \widetilde{R_3}(C)$.

4. Программная реализация и экспериментальное исследование ССШШ. Наличие математической модели сделало возможным построение программной реализации ССШШ. Реализация выполнена на языке C++ в среде Microsoft Visual Studio 2008 с использованием библиотеки теоретико-числовых методов WinNTL-5_4_1 [7] и может работать под управлением операционной системы Windows 2000/XP/Vista/7. Программная реализация математической модели ССШШ исследована экспериментально. Результаты экспериментов подтвердили корректность математической модели ССШШ.

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. *Guruswami V.* List Decoding of Error-Correcting Codes. – New York: Springer-Verlag Inc. (LNCS 3282). 2005. – 350 p.
3. *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.
4. *Мкртичян В.В.* Экспериментальное исследование надежности схемы специального широковещательного шифрования в случае превышения допустимого числа злоумышленников // 'Материалы X Международной научно-практической конференции "Информационная безопасность". Ч.2. – Таганрог, 2008. – С. 149-152.
5. *Мкртичян В.В.* Об экспериментальном исследовании надежности и применении схемы специального широковещательного шифрования // Известия ЮФУ. Технические науки. – 2008. – № 8 (85). – С. 203-210.
6. *Мкртичян В.В.* Компьютерные модели списочных декодеров Гурусвами–Судана для обобщенных кодов Рида–Соломона и конкатенированных кодов // Вестник ДГТУ. – 2007. – Т. 7, № 4. – С. 384-394.
7. Библиотека классов WinNTL-5_4_1. [Электронный ресурс]: 2008. – Режим доступа: shoup.net/ntl.

Мкртичян Вячеслав Виталиевич
ФГНУ НИИ "Спецвузавтоматика", г. Ростов-на-Дону.
E-mail: sva@rsu.ru.
344007, г. Ростов-на-Дону, пер. Газетный, 51.
Тел: +79044417791.

Mkrtichan Vyacheslav Vitalievich
Federal State Scientific Establishment "Scientific Research Institute "Specialized Security Computing Devices and Automation", Rostov-on-Don.
E-mail: sva@rsu.ru.
51, Gazetniy line, Rostov-on-Don, 344007, Russia.
Phone: +79044417791.