

МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

DOI 10.17223/20710410/20/5

УДК 519.7

КОД АУТЕНТИФИКАЦИИ С СЕКРЕТНОСТЬЮ
НА ОСНОВЕ ПРОЕКТИВНОЙ ГЕОМЕТРИИ

А. Ю. Зубов

*Московский государственный университет им. М. В. Ломоносова, г. Москва, Россия***E-mail:** Zubovanatoly@yandex.ru

Изучается код аутентификации с секретностью на основе проективной геометрии, обеспечивающий стойкую аутентификацию и конфиденциальность для равновероятного источника информации.

Ключевые слова: код аутентификации с секретностью, совершенный шифр, проективная геометрия.

1. Определения и постановка задачи

Код аутентификации (далее — *A-код*) — это тройка $A = (S, E, M)$ конечных множеств, называемых соответственно множествами *состояний источника*, *правил кодирования* и *сообщений*. Правило кодирования $e \in E$ — это инъективное отображение $e: S \rightarrow M$. Для защиты сообщений от активных атак, к которым относятся атаки имитации и подмены, отправитель и получатель выбирают общее (секретное) правило кодирования e . Отправитель вычисляет $m = e(s)$ и направляет сообщение m получателю. Критерием аутентичности полученного сообщения является условие $e^{-1}(m) \neq \emptyset$. Здесь $e^{-1}: M \rightarrow S \cup \{\emptyset\}$ — обратное к e отображение, определяемое формулой

$$e^{-1}(m) = \begin{cases} s, & \text{если } m = e(s), \\ \emptyset, & \text{если } m \notin e(S), \end{cases}$$

где $e(S) = \{e(s): s \in S\}$. Предполагается, что $\emptyset \notin S$. Для удобства выбора правила кодирования индексируются *ключами* из множества K .

Матрицей кодирования A-кода A называется матрица $C(A) = (c(e, m))$ размеров $|E| \times |M|$. Строки матрицы $C(A)$ занумерованы правилами кодирования $e \in E$, столбцы — сообщениями $m \in M$. Элементы матрицы определяются равенством $c(e, m) = e^{-1}(m)$. *Матрица инцидентности A-кода* — это матрица $I(A) = (i(e, m))$ тех же размеров, где

$$i(e, m) = \begin{cases} 1, & \text{если } e^{-1}(m) \neq \emptyset, \\ 0, & \text{если } e^{-1}(m) = \emptyset. \end{cases}$$

Если в каждом столбце матрицы кодирования A -кода имеются вхождения лишь одного состояния источника, то A -код называется *декартовым* или *A-кодом без секретности*. Он характеризуется тем, что $e_1^{-1}(m) = e_2^{-1}(m)$ для любых $m \in M$ и $e_1, e_2 \in E(m)$, где $E(m) = \{e \in E: e^{-1}(m) \neq \emptyset\}$. Это означает, что сообщение однозначно определяет состояние источника, поэтому состояние источника не является секретом для противника. Недекартов A -код называют *A-кодом с секретностью*.

Фактически A -код с секретностью может обеспечивать конфиденциальность состояния источника. В связи с этим можно говорить о криптографической стойкости A -кода.

Стойкость A -кода к активной атаке оценивается величиной вероятности успеха атаки. При имитации противник вводит в канал связи поддельное сообщение (имитируя передачу сообщения от одного пользователя другому), а при подмене — подменяет наблюдаемое сообщение (например, модифицируя его). В обоих случаях противник рассчитывает на то, что поддельное сообщение будет принято как аутентичное. Не зная правила кодирования, противник добьётся успеха при выборе поддельного сообщения лишь с некоторой вероятностью. Если противник сможет определить по наблюдаемому сообщению правило кодирования, то он добьётся успеха в подмене с вероятностью равной 1. При этом противник сможет навязать получателю любое поддельное сообщение. Чем меньше эта вероятность, тем более стойким является A -код.

В простейшем случае речь идёт об атаках на основе не более чем одного наблюдаемого сообщения. В этом случае естественно полагать, что каждое правило кодирования используется для передачи лишь одного состояния источника. Кроме того, имеется в виду атака, в которой противник добивается успеха, когда лишь некоторое (а не выбранное по его усмотрению) сообщение принимается как аутентичное. Другими словами, противник рассчитывает лишь на навязывание «наугад». Только такие атаки рассматриваются в этой работе. Любые другие атаки, в которых противник может использовать имитацию или подмену на основе наблюдения нескольких сообщений, образованных с помощью одного и того же правила кодирования или имеющих целью навязывание выбранного состояния источника, должны рассматриваться отдельно.

Определим вероятности успеха атак. Будем полагать, что состояния источника и правила кодирования выбираются случайно и независимо друг от друга в соответствии с заданными на множествах S и E распределениями вероятностей $P(S) = (p_S(s) : s \in S)$ и $P(E) = (p_E(e) : e \in E)$. Пусть $\bar{S}$ и $\bar{E}$ — соответствующие случайные величины. Они полагаются независимыми и естественным образом индуцируют случайную величину $\bar{M}$ с множеством исходов M . Вероятность $p_M(m)$ вычисляется по формуле

$$p_M(m) = \sum_{e \in E(m)} p_E(e) p_S(e^{-1}(m)).$$

Обычно полагают, что правила кодирования выбираются случайно и равновероятно (в общем случае это не обязательное условие [1, 2]). Будем и мы полагать, что распределение $P(E)$ — равномерное.

Пусть $p_{\Pi}(m)$ — вероятность того, что (при случайном выборе правила кодирования) имитируемое сообщение $m \in M$ будет принято как аутентичное. Ясно, что

$$p_{\Pi}(m) = \sum_{e \in E(m)} p_E(e).$$

Тогда (учитывая равномерность распределения $P(E)$) определим вероятность p_{Π} *успеха имитации* формулой

$$p_{\Pi} = \max_{m \in M} p_{\Pi}(m) = \max_{m \in M} \frac{|E(m)|}{|E|}. \quad (1)$$

Вероятность p_{Π} *успеха подмены* определяется формулой

$$p_{\Pi} = \sum_{m \in M} p_M(m) p_{\Pi}(m),$$

где

$$p_{\Pi}(m) = \max_{n \neq m} p_{\Pi}(n | m),$$

а $p_{\Pi}(n | m)$ — вероятность того, что (для случайно выбранной пары (e, s)) противник добьётся успеха при подмене наблюдаемого $m \in M$ сообщением $n \neq m$. Эта вероятность вычисляется по формуле

$$p_{\Pi}(n | m) = \frac{1}{p_M(m)} \sum_{e \in E(m, n)} p_E(e) p_S(e^{-1}(m)),$$

где $E(m, n) = E(m) \cap E(n)$. Учитывая равномерность распределения $P(E)$, получаем

$$p_{\Pi} = \frac{1}{|E|} \sum_{m \in M} \max_{n \neq m} \sum_{e \in E(m, n)} p_S(e^{-1}(m)). \quad (2)$$

Если распределение $P(S)$ равномерно, то формула (2) принимает вид

$$p_{\Pi} = \frac{1}{|E| \cdot |S|} \sum_{m \in M} \max_{n \neq m} |E(m, n)|. \quad (3)$$

Будем называть ε -стойким A -код, для которого $\max\{p_{\Pi}, p_{\Pi}\} \leq \varepsilon$, где ε — выбранный порог стойкости. В настоящее время достаточной считается величина ε порядка 2^{-128} . Известны (см., например, [3]) достижимые нижние оценки вероятностей p_{Π}, p_{Π} :

$$p_{\Pi} \geq \frac{|S|}{|M|}, \quad p_{\Pi} \geq \frac{|S| - 1}{|M| - 1}, \quad \max\{p_{\Pi}, p_{\Pi}\} \geq \frac{1}{\sqrt{|E|}}.$$

Актуальной является разработка конструкций A -кодов, использующих общий секретный ключ для обеспечения аутентификации и конфиденциальности передаваемых сообщений. Этой теме посвящён целый ряд работ [4–18]. В данной работе предлагается конструкция A -кода на основе проективной геометрии, обеспечивающего ε -стойкую аутентификацию и совершенное шифрование для равновероятного источника.

2. Теорема Зингера

Пусть v, k, λ — натуральные числа. Тогда (v, k, λ) -схемой или блок-схемой называется пара (M, B) , где M — множество мощности v и B — семейство k -подмножеств (блоков) множества M , таких, что любое 2-подмножество множества M содержится точно в λ блоках.

Пусть b — число блоков схемы и r — число блоков, содержащих любой выбранный элемент множества M . Тогда для параметров блок-схемы выполняются следующие соотношения:

$$\begin{cases} b \cdot k = v \cdot r, \\ r \cdot (k - 1) = \lambda \cdot (v - 1). \end{cases} \quad (4)$$

Для блок-схемы выполняется неравенство Фишера $b \geq v$. Блок-схема, для которой $b = v$, называется симметричной. Известно, что для симметричной блок-схемы справедливо равенство $r = k$ и любые два блока имеют ровно λ общих точек.

Пусть F_q — поле из q элементов. Пространство всех векторов $(a_n, \dots, a_0)$, $a_i \in F_q$, называется проективной геометрией размерности n над F_q и обозначается $PG(n, q)$. Вектор $\bar{0} = (0, \dots, 0)$ образует пустое подпространство размерности -1 . Точка — подпространство размерности 0. Это множество векторов $b\bar{x}$, где $\bar{x} = (x_n, \dots, x_0) \neq \bar{0}$,

а b пробегает все элементы из F_q . Если векторы $\bar{y}_0, \dots, \bar{y}_h$ линейно независимы, то множество векторов $\{b_0\bar{y}_0 + \dots + b_h\bar{y}_h : b_i \in F_q\}$ — подпространство S_h размерности h . Подпространство S_{n-1} называется *гиперплоскостью*. Если $(c_n, \dots, c_0) \neq \bar{0}$, то множество всех точек $(x_n, \dots, x_0)$, удовлетворяющих уравнению

$$c_n x_n + \dots + c_0 x_0 = 0,$$

образует гиперплоскость, и обратно, каждая гиперплоскость может быть определена таким образом, причём $(c_n, \dots, c_0)$ и $(sc_n, \dots, sc_0)$, $s \neq 0$, определяют одну и ту же гиперплоскость.

Каждый из $q^{n+1} - 1$ ненулевых векторов определяет точку, и, поскольку $(x_n, \dots, x_0)$ и $(dx_n, \dots, dx_0)$, $d \neq 0$, определяют одну и ту же точку, всего имеется $v = (q^{n+1} - 1)/(q - 1)$ точек. Аналогично, поскольку $(c_n, \dots, c_0)$ и $(sc_n, \dots, sc_0)$, $s \neq 0$, определяют одну и ту же гиперплоскость, имеется v гиперплоскостей. Подпространство S_h содержит $v = (q^{h+1} - 1)/(q - 1)$ точек, а гиперплоскость — $k = (q^n - 1)/(q - 1)$ точек.

С проективной геометрией $PG(n, q)$ ассоциируется симметричная блок-схема. Это следует из теоремы Зингера [19].

Теорема 1. Гиперплоскости геометрии $PG(n, q)$, взятые в качестве блоков, и точки, взятые в качестве элементов, образуют симметричную блок-схему с параметрами

$$v = \frac{q^{n+1} - 1}{q - 1}, \quad k = \frac{q^n - 1}{q - 1}, \quad \lambda = \frac{q^{n-1} - 1}{q - 1}. \quad (5)$$

Эта схема является циклической, и точки в любой гиперплоскости определяют (v, k, λ) -разностное множество.

Симметричная блок-схема называется *циклической*, если она имеет автоморфизм α , который переставляет элементы и блоки по циклу длины v . Автоморфизмом блок-схемы называется взаимно однозначное отображение α множеств элементов и блоков схемы на множества элементов и блоков той же схемы, такое, что если x_i — элемент, а B_j — блок и

$$\begin{cases} \alpha : x_i \rightarrow x'_i = (x_i)\alpha, \\ \alpha : B_j \rightarrow (B'_j)\alpha, \end{cases}$$

то $x_i \in B_j$ тогда и только тогда, когда $x'_i \in B'_j$.

Множество D , состоящее из k вычетов $a_1, \dots, a_k$ по модулю v , называется (v, k, λ) -разностным множеством, если для каждого $d \neq 0 \pmod{v}$ существует ровно λ упорядоченных пар (a_i, a_j) , $a_i, a_j \in D$, таких, что $a_i - a_j \equiv d \pmod{v}$.

3. А-код на основе проективной геометрии

Рассмотрим А-код, множеством сообщений и ключей которого служит множество точек геометрии $PG(n, q)$, а множества $e_{\kappa}(S)$, $\kappa \in K$, совпадают с множествами точек гиперплоскостей (произвольным образом упорядоченными). Таким образом, правило кодирования e_{κ} , отвечающее ключу κ , удовлетворяет равенству $e_{\kappa}(S) = B_{\kappa}$, где S — множество состояний источника, а B_{κ} — гиперплоскость, определяемая точкой κ .

По теореме Зингера для построенного А-кода множества $e_{\kappa}(S)$ составляют блоки симметричной (v, k, λ) -схемы с параметрами, указанными в (5). Для такой схемы выполняется равенство $r = k$ и любые два блока имеют ровно λ общих точек. Отсюда

следует, что для любого сообщения m и любой пары различных сообщений m_1 и m_2

$$|E(m)| = r = k = \frac{q^n - 1}{q - 1} \text{ и } |E(m, n)| = \lambda = \frac{q^{n-1} - 1}{q - 1}.$$

Поскольку для параметров блок-схемы выполняются соотношения (4), из формул (1), (3) получаем значения вероятностей успеха имитации и подмены для построенного A -кода:

$$p_{\text{и}} = \frac{q^n - 1}{q^{n+1} - 1}, \quad p_{\text{п}} = \frac{q^{n-1} - 1}{q^n - 1}.$$

Таким образом, $\max\{p_{\text{и}}, p_{\text{п}}\} \approx 1/q$. Например, при $q = 2^{128}$ шансы на успех атаки имитации или подмены оцениваются величиной порядка 2^{-128} .

Уточним теперь выбор гиперплоскости $e_{\kappa}(S)$ для каждого $\kappa \in K$ и значение $e_{\kappa}(s)$ для каждого $s \in S$, при котором A -код, рассматриваемый как шифр, реализует совершенное (по К. Шеннону [20]) шифрование. В связи с этим отметим, что любой A -код с секретностью может быть формально рассмотрен как шифр. При этом S и M — множества открытых и зашифрованных текстов, $e_{\kappa} : S \rightarrow M$ и $e_{\kappa}^{-1} : M \rightarrow S \cup \{\emptyset\}$ — правила зашифрования и расшифрования на ключе $\kappa \in K$. Такой взгляд на код аутентификации позволяет формально ставить вопрос о его стойкости как шифра.

Теорема 2. Правило кодирования A -кода на основе проективной геометрии можно выбрать так, чтобы A -код являлся совершенным шифром.

Доказательство. Пусть A — код аутентификации на основе проективной геометрии и $I(A)$ — его матрица инцидентности. Как было отмечено, для параметров кода A справедливы равенства $|M| = v = b = |E|$ и $r = k = |S|$, означающие, что $I(A)$ — квадратная $(0, 1)$ -матрица, в каждой строке и каждом столбце которой содержится ровно k единиц. Согласно [21, теорема 4, с. 364], такая матрица представляется в виде суммы k подстановочных матриц. Поместив на места единиц в каждой из подстановочных матриц одно из k состояний источника, получим матрицу, в каждой строке и каждом столбце которой содержатся все состояния источника. Обозначим полученную матрицу через $C(A)$. Она является матрицей кодирования кода аутентификации A с данными множествами S, E, M . Покажем, что A реализует совершенное шифрование.

Для этого воспользуемся критерием совершенности, согласно которому для любых $m \in M$ и $s \in S$ выполняется равенство $p_M(m) = p_{M|S}(m|s)$. Это равенство можно записать в виде

$$\sum_{e \in E(s, m)} p_E(e) = \sum_{e \in E(m)} p_E(e) \cdot p_S(e^{-1}(m)), \quad (6)$$

где $E(s, m) = \{e \in E : e(s) = m\}$. С учётом условия равновероятности выбора состояний источника и правил кодирования (6) равносильно равенству

$$\frac{1}{b} |E(s, m)| = \frac{1}{bk} |E(m)|. \quad (7)$$

Из свойств матрицы $C(A)$ следует, что $|E(s, m)| = 1$ для любых $s \in S$ и $m \in M$. А поскольку $|E(m)| = k$, приходим к выводу о том, что равенство (7), а вместе с ним и (6) справедливо. ■

Остаётся найти подходящее разложение матрицы $I(A)$ в сумму подстановочных матриц. Для того чтобы сделать это, обратимся к доказательству (из [19]) цикличности блок-схемы в теореме Зингера.

Пусть θ — примитивный элемент поля $\text{GF}(q^{n+1})$. Тогда θ — корень многочлена $F(x)$ степени $n+1$, неприводимого над $\text{GF}(q)$. Пусть

$$F(x) = x^{n+1} + c_n x^n + \dots + c_0, \quad c_i \in \text{GF}(q).$$

Поскольку $F(\theta) = 0$, выполняется соотношение

$$\theta^{n+1} = -c_0 - c_1 \theta - \dots - c_n \theta^n.$$

Отсюда следует, что для любой степени i элемента θ для подходящих элементов $a_0, \dots, a_n \in \text{GF}(q)$ выполняется равенство

$$\theta^i = a_0 + a_1 \theta + \dots + a_n \theta^n. \quad (8)$$

Тем самым устанавливается взаимно однозначное соответствие между множеством степеней элемента θ и множеством ненулевых векторов $(a_0, \dots, a_n)$ над $\text{GF}(q)$, рассматриваемых как точки геометрии $PG(n, q)$.

В условиях теоремы $v = \frac{q^{n+1} - 1}{q - 1}$, поэтому элементы $0, 1, \theta^v, \dots, \theta^{(q-2)v}$ дают q решений уравнения $z^q = z$ и образуют подполе $\text{GF}(q)$ поля $\text{GF}(q^{n+1})$. Если $\theta^{sv} = t$, то $t \in \text{GF}(q)$, и поэтому если (8) выполняется, то

$$\theta^{i+sv} = ta_0 + ta_1 \theta + \dots + ta_n \theta^n.$$

Следовательно, θ^i и θ^j соответствуют одной и той же точке из $PG(n, q)$ тогда и только тогда, когда $i \equiv j \pmod{v}$. Таким образом, если задано отображение α поля $\text{GF}(q^{n+1})$ в себя

$$\begin{cases} \alpha : 0 \rightarrow 0, \\ \alpha : \theta^i \rightarrow \theta^{i+1}, \end{cases} \quad (9)$$

то, ввиду (8), α можно рассматривать и как отображение

$$\alpha : (a_0, a_1, \dots, a_n) \rightarrow (-a_n c_0, a_0 - a_n c_1, \dots, a_{n-1} - a_n c_n) \quad (10)$$

множества точек в себя. Поскольку $\theta^{v(q-1)} = 1$, отображение (9) является взаимно однозначным, и поэтому взаимно однозначно и отображение (10). Так как θ^i и θ^{i+v} соответствуют одной и той же точке, а $1, \theta, \dots, \theta^{v-1}$ — различным точкам, отображение α в (10) переставляет все v точек по полному циклу.

Заметим теперь, что $v - qk = 1$. Из этого равенства следует, что k и v взаимно просты. Если для некоторого $j \neq 0$ отображение α^j переводит точки некоторой гиперплоскости в себя, то α^j переставляет их по циклам длины t , где t делит k . Но тогда, поскольку $\alpha^v = 1$, t должно делить v и, раз $v - qk = 1$, приходим к выводу, что $t = 1$ и $\alpha^j = 1$. Так как никакая степень отображения α , за исключением степени v , не фиксирует гиперплоскость, α должно переставлять гиперплоскости по циклу длины v . Это доказывает цикличность блок-схемы.

Пусть $q = p^d$. Рассмотрим башню полей $\text{GF}(p) \subset \text{GF}(q) \subset \text{GF}(q^{n+1})$. Пусть θ — примитивный элемент поля $\text{GF}(q^{n+1})$ над $\text{GF}(q)$ и ω — примитивный элемент поля $\text{GF}(q)$ над $\text{GF}(p)$. Тогда для подходящих $b_i \in \text{GF}(p)$ и $c_j \in \text{GF}(q)$ выполняются равенства

$$\begin{aligned} \omega^d + b_{d-1} \omega^{d-1} + \dots + b_0 &= 0, \\ \theta^{n+1} + c_n \theta^n + \dots + c_0 &= 0. \end{aligned} \quad (11)$$

Пусть $\theta^i \leftrightarrow (a_0, \dots, a_{n-1})$ — взаимно однозначное соответствие из (8) и α — автоморфизм (9). Можно полагать, что множества ключей и сообщений нашего A -кода представлены в виде $K = M = \{\theta^0, \theta^1, \dots, \theta^{v-1}\}$. Пусть $S = \{s_0, s_1, \dots, s_{k-1}\}$ — произвольное множество состояний источника. Блоками блок-схемы, ассоциированной с геометрией $PG(n, q)$, служат гиперплоскости. Пусть

$$B_0 = \{\theta^i \mid i : \theta^i = a_0 + a_1\theta + \dots + a_{n-1}\theta^{n-1}, a_0, a_1, \dots, a_{n-1} \in \text{GF}(q)\}$$

— одна из гиперплоскостей. Запишем для удобства её элементы в виде

$$B_0 = \{\theta^{\gamma_0}, \theta^{\gamma_1}, \dots, \theta^{\gamma_{k-1}}\}. \quad (12)$$

Положим

$$B_j = (B_0)\alpha^j = \{\theta^{\gamma_0+j}, \theta^{\gamma_1+j}, \dots, \theta^{\gamma_{k-1}+j}\}, \quad j = 1, 2, \dots, v-1.$$

Тогда $B_0, B_1, \dots, B_{v-1}$ — все блоки блок-схемы, связанные в один цикл преобразованием α :

$$B_0 \xrightarrow{\alpha} B_1 \xrightarrow{\alpha} \dots \xrightarrow{\alpha} B_{v-1} \xrightarrow{\alpha} B_0.$$

Если теперь строки и столбцы матрицы кодирования упорядочить в соответствии с последовательностью степеней $\theta : \theta^0, \theta^1, \dots, \theta^{v-1}$, и для $\varkappa \in K$ положить $e_\varkappa(S) = B_\varkappa$, то, согласно сказанному выше, получим циклическую матрицу. При этом элементы множества S упорядочены естественным образом: $s_0, s_1, \dots, s_{k-1}$. Мы получили искомую «раскраску» клеток матрицы инцидентности и соответствующую формулу для правила кодирования. Её можно записать в виде

$$e_{\theta^j}(s_i) = \theta^{(\gamma_i+j) \bmod v}, \quad (13)$$

где γ_i определены формулой (12).

Итоги проведённых рассуждений сформулируем в следующем утверждении.

Теорема 3. Код аутентификации с правилом кодирования (13) гарантирует успех активной атаки с вероятностью, не превосходящей $1/q$, и совершенное шифрование.

Для лучшего понимания устройства такого A -кода приведём пример.

4. Пример

Пусть $q = 2^2$ и $n = 2$. В этом случае $\text{GF}(q^{n+1}) = \text{GF}(2^6)$. Выберем в качестве ω корень примитивного многочлена $f(y) = y^2 + y + 1$ над полем $\text{GF}(2)$, а в качестве θ — корень примитивного многочлена $F(x) = x^3 + \omega x^2 + \omega x + \omega$ над полем $\text{GF}(2^2)$. Используя равенства (11) $\omega^2 = \omega + 1$ и $\theta^3 = \omega\theta^2 + \omega\theta + \omega$, вычисляем степени θ^i для $i = 0, 1, \dots, v-1$, где $v = q^2 + q + 1 = 21$ (табл. 1).

Для большей наглядности закодируем элементы поля $\text{GF}(2^2)$ числами 0, 1, 2, 3, а операции сложения и умножения этих элементов будем производить в соответствии с операциями фактор-кольца $\text{GF}(2)[y]/f(y)$ (табл. 2).

При этом элемент ω заменится на 2, а $\omega + 1$ — на 3. Учитывая, что векторы $(c_n, \dots, c_0)$ и $(sc_n, \dots, sc_0)$, $s \neq 0$, определяют одну и ту же гиперплоскость, получаем следующее представление элементов множеств $K = M$ (табл. 3).

Заменяем θ^i вычетом $i \bmod 21$ или соответствующей тройкой $a_0a_1a_2$ согласно табл. 3. Тогда гиперплоскость B_0 из (11) имеет вид

$$B_0 = \{0, 1, 6, 8, 18\} \quad \text{или} \quad B_0 = \{100, 010, 130, 110, 120\}.$$

Т а б л и ц а 1

Степени θ^i

θ^0	=	1				(1, 0, 0)
θ^1	=		θ			(0, 1, 0)
θ^2	=			θ^2		(0, 0, 1)
θ^3	=	ω	+	$\omega\theta$	+	$\omega\theta^2$
θ^4	=	$(\omega + 1)$	+	θ	+	θ^2
θ^5	=	ω	+	θ	+	$(\omega + 1)\theta^2$
θ^6	=	1	+	$(\omega + 1)\theta$		
θ^7	=			θ	+	$(\omega + 1)\theta^2$
θ^8	=	1	+	θ		
θ^9	=			θ	+	θ^2
θ^{10}	=	ω	+	$\omega\theta$	+	$(\omega + 1)\theta^2$
θ^{11}	=	1	+	$(\omega + 1)\theta$	+	$(\omega + 1)\theta^2$
θ^{12}	=	1	+			$\omega\theta^2$
θ^{13}	=	$(\omega + 1)$	+	$\omega\theta$	+	$(\omega + 1)\theta^2$
θ^{14}	=	1	+	$\omega\theta$	+	$(\omega + 1)\theta^2$
θ^{15}	=	1	+			$(\omega + 1)\theta^2$
θ^{16}	=	1	+			$\omega\theta^2$
θ^{17}	=	ω	+	$(\omega + 1)\theta$	+	$\omega\theta^2$
θ^{18}	=	$(\omega + 1)$	+	θ		
θ^{19}	=			$(\omega + 1)\theta$	+	θ^2
θ^{20}	=	ω	+	$\omega\theta$	+	θ^2
θ^{21}	=	ω				

Т а б л и ц а 2

Операции в кольце $\text{GF}(2)[y]/f(y)$

+	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

Т а б л и ц а 3

Представление степеней θ

θ^0	100
θ^1	010
θ^2	001
θ^3	111
θ^4	122
θ^5	132
θ^6	130

θ^7	013
θ^8	110
θ^9	011
θ^{10}	112
θ^{11}	133
θ^{12}	102
θ^{13}	131

θ^{14}	123
θ^{15}	103
θ^{16}	101
θ^{17}	121
θ^{18}	120
θ^{19}	012
θ^{20}	113

Отметим, что элементы множества $\{0, 1, 6, 8, 18\}$ образуют $(21, 5, 1)$ -разностное множество и дают $(21, 5, 1)$ -блок-схему с блоками

$$B_i = \{i, i + 1, i + 6, i + 8, i + 18\}, \quad i = 0, 1, \dots, 20,$$

являющимися гиперплоскостями геометрии $PG(2, 4)$.

Приведём теперь матрицу кодирования A -кода с правилом кодирования (13) (табл. 4). В матрице первый столбец соответствует номеру $\varkappa$ правила кодирования, а первая строка — сообщению m . Например, $e_{122}(s_3) = 102$.

Таблица 4

Матрица кодирования 1

	100	010	001	111	122	132	130	013	110	011	112	133	102	131	123	103	101	121	120	012	113
100	s_0	s_1					s_2		s_3										s_4		
010		s_0	s_1					s_2		s_3										s_4	
001			s_0	s_1					s_2		s_3										s_4
111	s_4			s_0	s_1					s_2		s_3									
122		s_4			s_0	s_1					s_2		s_3								
132			s_4			s_0	s_1					s_2		s_3							
130				s_4			s_0	s_1					s_2		s_3						
013					s_4			s_0	s_1					s_2		s_3					
110						s_4			s_0	s_1					s_2		s_3				
011							s_4			s_0	s_1					s_2		s_3			
112								s_4			s_0	s_1					s_2		s_3		
133									s_4			s_0	s_1					s_2		s_3	
102										s_4			s_0	s_1					s_2		s_3
131	s_3										s_4			s_0	s_1					s_2	
123		s_3										s_4			s_0	s_1					s_2
103	s_2		s_3										s_4			s_0	s_1				
101		s_2		s_3										s_4			s_0	s_1			
121			s_2		s_3										s_4			s_0	s_1		
120				s_2		s_3										s_4			s_0	s_1	
012					s_2		s_3										s_4			s_0	s_1
113	s_1					s_2		s_3										s_4			s_0

5. Обсуждение

Подчеркнём, что при построении полученной матрицы важен порядок следования состояний источника в строках (он соответствует разложению матрицы инцидентности в сумму подстановочных матриц). Перестановки элементов множества S в строках матрицы кодирования могут привести к тому, что получится код аутентификации без секретности. Такой A -код на основе проективной плоскости изучается в работе [22]. Этот A -код без секретности и построенный здесь A -код с секретностью «диаметрально удалены» друг от друга с точки зрения криптографической стойкости. «Между ними» расположены многие другие A -коды с секретностью. Приведём один пример (табл. 5).

Пусть $S = \{(1, a) : a \in \text{GF}(q)\} \cup \{(0, 1)\}$ и правило кодирования задаётся формулой

$$e_{(\kappa_2, \kappa_1, \kappa_0)}(s_1, s_0) = \begin{cases} (0, s_1, s_0), & \text{если } \kappa = (1, 0, 0), \\ (s_1, -\kappa_2 \kappa_1^{-1} s_1, s_0), & \text{если } \kappa = (\kappa_2, \kappa_1, 0), \kappa_1 \neq 0, \\ (s_1, s_0, -\kappa_0^{-1} (\kappa_2 s_1 + \kappa_1 s_0)), & \text{если } \kappa_0 \neq 0. \end{cases} \quad (14)$$

Операции в (14) производятся в поле $\text{GF}(q)$. Непосредственно из (14) получаем следующее утверждение.

Теорема 4. Сообщение $m = (m_2, m_1, m_0)$ однозначно определяет состояние источника $s = (s_1, s_0)$ тогда и только тогда, когда $m \in \{(0, 0, 1), (1, a, a), a \in \text{GF}(q)\}$. Если при этом $m = (0, 0, 1)$, то $s = (0, 1)$, а если $m = (1, a, a)$, то $s = (1, a)$. Сообщение

Таблица 5

Матрица кодирования 2

	001	010	011	012	013	100	101	102	103	110	111	112	113	120	121	122	123	130	131	132	133
011		01				10				11				12				13			
010	01					10	11	12	13												
011			01			10					11					12					13
012					01	10							11		12					13	
013				01		10						11					12		13		
100	01	10	11	12	13																
101		01					10				11				12				13		
102		01							10				11				12				13
103		01						10				11				12				13	
110	01									10	11	12	13								
111			01				10			11							12			13	
112					01				10	11						12			13		
113				01				10		11					12						13
120	01																	10	11	12	13
121				01			10						11			12		13			
122			01						10			11			12			13			
123					01			10			11						12	13			
130	01													10	11	12	13				
131					01		10					11		12							13
132				01					10		11			12						13	
133			01					10					11	12					13		

$m = (0, 1, a)$ в одном случае определяет $s = (1, a)$ и в q случаях — $s = (0, 1)$; сообщение $m = (1, a, b)$ в одном случае определяет $s = (1, b)$ и в q случаях — $s = (1, a)$.

Мы построили A -код, позволяющий злоумышленнику однозначно определить состояние источника для $q + 1$ сообщений, а для q^2 сообщений — по два состояния источника, причём одно из них с вероятностью $\frac{q}{q+1}$, а другое — с вероятностью $\frac{1}{q+1}$. Матрица кодирования такого A -кода при $q = 4$ приведена в табл. 5.

Следует отметить, что конструкция кода аутентификации с секретностью на основе проективной плоскости изучается (в числе других конструкций) в [17], где указывается возможность построения совершенного шифра (частный случай теоремы 2), но не получена явная формула для соответствующего правила кодирования (аналог формулы (13)).

В заключение отметим, что основной сложностью в практическом использовании предлагаемого A -кода является нахождение явного выражения степеней θ^i , что связано с выбором примитивных многочленов $f(y)$ и $F(x)$. Вместе с тем эффективно вычисляемое правило кодирования (14) оставляет надежду на то, что неким подобным образом может быть построен A -код, допускающий совершенное или почти совершенное [4] шифрование.

ЛИТЕРАТУРА

1. *Зубов А. Ю.* К теоретико-игровому подходу исследования кодов аутентификации // Дискретная математика. 2009. Т. 21. Вып. 3. С. 45–72.
2. *Зубов А. Ю.* О выборе оптимальной стратегии для кода аутентификации с двумя состояниями источника // Дискретная математика. 2009. Т. 21. Вып. 4. С. 135–147.
3. *Зубов А. Ю.* Математика кодов аутентификации. М.: Гелиос АРВ, 2007.
4. *Зубов А. Ю.* Почти совершенные шифры и коды аутентификации // Прикладная дискретная математика. 2011. № 4(14). С. 28–33.
5. *Casse L. R. A., Martin K. M., and Wild P. R.* Bound and characterizations of authentication / secrecy schemes // Designs, Codes and Cryptography. 1998. V. 13. P. 107–129.
6. *Ding C. and Tian X.* Three constructions of authentication codes with perfect secrecy // Designs, Codes and Cryptography. 2004. V. 33. P. 227–239.
7. *Huber M.* Authentication and secrecy codes for equiprobable source probability distributions // arxiv.org/abs/0904.0109, 2009.
8. *Huber M.* Constructing optimal authentication codes with perfect multi-fold secrecy // Proc. IEEE Int. Zurich Seminar on Communications (IZS), March 3–5, 2010. Zurich, 2010. P. 86–89.
9. *Mitchell C. J., Piper C., Walker M., and Wild P.* Authentication schemes, perfect local randomizers, perfect secrecy and secret sharing schemes // Designs, Codes and Cryptography. 1996. V. 7. P. 101–110.
10. *Rees R. and Stinson D. R.* Combinatorial characterizations of authentication codes II // Designs, Codes and Cryptography. 1996. V. 7. P. 239–259.
11. *Sgarro A.* An introduction to the theory of unconditional secrecy and authentication // Geometries, Codes and Cryptography. CISM Courses and Lectures. No. 313. Springer Verlag, 1990. P. 131–160.
12. *Saygi Z.* Constructions of authentication codes. A thesis submitted to the Graduate School of Applied Mathematics of the METU. Ankara, 2007. 74 p.
13. *Smeets B., Vanrose P., and Wan C.-X.* On the construction of authentication codes with secrecy and codes withstanding spoofing attack of order L // Eurocrypt'90. LNCS. 1990. V. 473. P. 307–312.
14. *De Soete M.* Some constructions for authentication — secrecy codes // Eurocrypt'88. LNCS. 1988. V. 330. P. 57–75.
15. *De Soete M.* Authentication/secrecy codes. Geometries, Codes and Cryptography // CISM Courses and Lectures. No. 313. Springer Verlag, 1990. P. 187–199.
16. *Stinson D. R.* A construction for authentication secrecy codes from certain combinatorial designs // Crypto'87. LNCS. 1988. V. 293. P. 355–366.
17. *Stinson D. R.* The combinatorics of authentication and secrecy codes // J. Cryptology. 1990. No. 2. P. 23–49.
18. *Van Tran T.* On the construction of authentication and secrecy codes // Designs, Codes and Cryptography. 1995. V. 5. P. 269–280.
19. *Холл М.* Комбинаторика. М.: ИЛ, 1970.
20. *Зубов А. Ю.* Криптографические методы защиты информации. Совершенные шифры. М.: Гелиос АРВ, 2005.
21. *Сачков В. Н.* Введение в комбинаторные методы дискретной математики. М.: МЦНМО, 2004.
22. *Gilbert E., MacWilliams F. J., and Sloane J. A.* Codes which detect deception // Bell System Tech. J. 1974. V. 53. P. 405–424.