A. Yu. Zubov, Authentication codes with secrecy (survey), *Mat. Vopr. Kriptogr.*, 2017, Volume 8, Issue 3, 5–40

DOI: 10.4213/mvk230

МАТЕМАТИЧЕСКИЕ ВОПРОСЫ КРИПТОГРАФИИ
2017 Т. 8 № 3 С. 5–40

УДК 519.719.2+519.712

Коды аутентификации с секретностью (обзор)

А. Ю. Зубов

ООО «Центр сертификационных исследований», Москва

Получено 25.I.2017

Аннотация. Приводится обзор кодов аутентификации с секретностью, предназначенных для защиты информации от пассивных и активных атак. Основное внимание уделяется конструкциям и оценкам стойкости кодов аутентификации комбинаторной или алгебраической природы. В качестве кодов аутентификации с секретностью рассматриваются также симметричные шифрсистемы, реализующие шифрование с аутентификацией.

Ключевые слова: код аутентификации с секретностью, вероятности успеха активных атак, ϵ-совершенное шифрование

Authentication codes with secrecy (survey)

A. Yu. Zubov

Certification Research Center, LLC, Moscow

Abstract. An overview of authentication codes with secrecy designed for information protection from passive and active attacks is proposed. Special attention is devoted to constructions and assessment of secrecy of authentication codes of combinatory or algebraic nature. The symmetrical cipher systems implementing ciphering with authentication are also considered as authentication codes with secrecy.

Key words: authentication code with secrecy, probabilities of active attacks success, ϵ-perfect enciphering

Citation: *Mathematical Aspects of Cryptography*, 2017, v. 8, № 3, pp. 5–40 (Russian)

Введение

Код аутентификации (далее А-код) — это математическая модель системы аутентификации, служащей для защиты от угроз модификации и фальсификации данных. А-код с секретностью позволяет гарантировать не только аутентичность данных, но и их конфиденциальность. Известны различные конструкции А-кодов. Один класс А-кодов основан на комбинаторных конфигурациях или алгебраических системах. Другой класс представляет собой, по сути дела, шифрсистемы, реализующие шифрование с аутентификацией[1]. На уровне математической модели нет никакой разницы между А-кодом с секретностью и имитостойким шифром. Как и симметричные шифры, А-коды используют секретные ключи. Многие А-коды первого класса допускают лишь однократное использование ключа. Это означает, что при повторном использовании ключа стойкость А-кода не гарантируется. Вместе с тем имеются и А-коды, стойкие при кратном использовании ключа. А-коды, представляемые AE-криптосистемами, допускают кратное использование ключа. Их анализ основан на методике доказуемой стойкости, развиваемой в последние два десятилетия применительно к режимам блочного шифрования на основе теоретико-сложностного подхода.

Настоящий обзор посвящен в основном А-кодам с секретностью, построенным на основе комбинаторных конфигураций и алгебраических систем. Их стойкость оценивается с позиции теоретико-информационного подхода. Стойкие с позиции этого подхода А-коды называют теоретически (или безусловно) стойкими. Оценка стойкости определяется параметрами, зависящими от распределений вероятностей на множествах ключей и открытых текстов и не зависящими от (вычислительных) затрат противника. Стойкость шифрования А-кода оценивается «близостью» к совершенному (по К. Шеннону) шифрованию. Близкий к совершенному шифр в данном обзоре назван ϵ-совершенным. Стойкость аутентификации оценивается вероятностью успеха активной атаки типа имитации или подмены. Приводятся конструкции А-кодов с секретностью, имеющих минимально возможное число ключей при данном уровне стойкости. Отдельно рассматриваются А-коды с неявно и явно заданной функцией шифрования. Как правило, А-коды с секретностью обеспечивают стойкость для равновероятного «входа». Вместе с тем известны и А-коды, обеспечивающие стойкость без ограничений на источник информации. Отмечается возможность эффективных реализаций ряда А-кодов.

[1] Будем их называть AE-криптосистемами (от Authenticated-Encryption Cryptosystems) или имитостойкими шифрами.

Обзор состоит из пяти разделов и заключения. В разделе 1 приведены определение, классификация и параметры А-кодов. В разделе 2 излагаются сведения об А-кодах, реализующих близкое к совершенному шифрование, для которых достигаются минимально возможные значения вероятностей успеха активных атак. Их конструкции основаны на комбинаторных конфигурациях и не определяют в явном виде функцию шифрования. Раздел 3 посвящен А-кодам с секретностью, в основном алгебраической природы, с одноразовым ключом и явно заданной функцией шифрования. В разделе 4 указываются конструкции стойких А-кодов с одноразовым ключом, допускающие эффективную реализацию. В разделе 5 приводятся краткие сведения об AE-криптосистемах.

1. Коды аутентификации и их параметры

1.1. Определение и классификация А-кодов

Пусть $\mathbf{S}, \mathbf{E}, \mathbf{M}$ — конечные множества, $|\mathbf{S}| \geqslant 2, |\mathbf{E}| \geqslant 3, |\mathbf{M}| \geqslant 3$, называемые соответственно множествами *состояний источника, правил кодирования и сообщений*. Каждое правило кодирования $e \in \mathbf{E}$ — инъективное отображение $e\colon \mathbf{S} |\to \mathbf{M}|$.

Тройка $(\mathbf{S}, \mathbf{E}, \mathbf{M})$ называется *кодом аутентификации* (А-*кодом*). Для удобства выбора правил кодирования может вводиться множество $\mathbf{K}$ *ключей* А-кода. При этом будем полагать, что $\mathbf{E} = \{e_\kappa, \kappa \in \mathbf{K}\}$ и $e_{\kappa_1} \neq e_{\kappa_2}$ при $\kappa_1 \neq \kappa_2$.

Удобно рассматривать элементы $e \in \mathbf{E}$ как отображения $e\colon \mathbf{S} \cup \{\mathbf{o}\} \to \mathbf{M}$, инъективные на $\mathbf{S}$, где $\mathbf{o}$ — произвольный символ, не содержащийся в $\mathbf{S}$. Тогда e^{-1} будет обозначать обратное к e отображение $e^{-1}\colon \mathbf{M} \to \mathbf{S} \cup \{\mathbf{o}\}$, т. е. что $e^{-1}(m) = s$, если $e(s) = m$, и $e^{-1}(m) = \mathbf{o}$, если $m \notin e(\mathbf{S}) = \{e(s),\, s \in \mathbf{S}\}$. Для использования А-кода с целью защиты от активных атак необходимо, чтобы отображения e, e^{-1} были эффективно реализуемы.

Как используется А-код? Для передачи состояния источника $s \in \mathbf{S}$ отправитель и получатель выбирают правило кодирования $e \in \mathbf{E}$. Отправитель вычисляет $m = e(s)$ и направляет сообщение m получателю. Критерий аутентичности полученного сообщения m' — условие $e^{-1}(m') \neq \mathbf{o}$. При его выполнении получатель восстанавливает состояние источника $s' = e^{-1}(m')$. А-код должен допускать возможность несовпадения s' и s лишь с очень малой вероятностью, которая и определяет уровень его стойкости.

Будем обозначать величины $|\mathbf{S}|, |\mathbf{E}|, |\mathbf{M}|$ символами k, b, v соответственно и полагать, что элементы множеств $\mathbf{S}, \mathbf{E}, \mathbf{M}$ упорядочены. Для указания параметров А-кода $\mathcal{AC}$ будем использовать обозначение $\mathcal{AC}(k, b, v)$.

Матрица аутентификации А-кода $\mathcal{AC}$ — это $b \times k$-матрица $\mathbf{A}(\mathcal{AC})$, строки которой пронумерованы элементами $e \in \mathbf{E}$, столбцы — элементами $s \in \mathbf{S}$, а на пересечении строки с номером e и столбца с номером s расположен элемент $m = e(s)$.

А-коды делятся на два класса. А-код *без секретности* характеризуется следующим свойством: при любом $s \in \mathbf{S}$ из условия $e(s) = m$ следует, что $e'^{-1}(m) = s$ для любого $e' \in \mathbf{E}(m)$, где $\mathbf{E}(m) = \{e \in \mathbf{E} \,|\, e^{-1}(m) \neq \mathbf{o}\}$. Ввиду этого состояние источника не является секретом для противника. Если это не так, то мы имеем А-код *с секретностью*. Любой А-код без секретности можно представить в виде А-*кода с аутентикатором*. Для такого А-кода $\mathbf{M} \subseteq \mathbf{S} \times \mathbf{T}$, где $\mathbf{T}$ — множество *аутентикаторов* (или *меток*)[2], $|\mathbf{T}| = n$, а $e(s) = (s, \overline{e}(s))$, где $\overline{e}$ — ассоциированное с e отображение $\mathbf{S} \to \mathbf{T}$ (не обязанное быть инъективным). Если $\mathbf{M} = \mathbf{S} \times \mathbf{T}$, то А-код называют *систематическим* (или *декартовым*) А-кодом. Для такого А-кода критерий аутентичности сообщения $m' = (s', \tau')$ равносилен условию $\overline{e}(s') = \tau'$, где e — используемое правило кодирования.

Правила кодирования А-кода могут быть однозначными отображениями. Тогда говорят об А-коде *без расщепления*. В противном случае — об А-коде *с расщеплением* [3].

1.2. Параметры стойкости А-кодов

При определении характеристик стойкости к активным атакам будем полагать, что состояния источника и правила кодирования А-кода выбираются случайно и независимо из множеств $\mathbf{S}$ и $\mathbf{E}$ в соответствии с априорно заданными распределениями вероятностей $\mathcal{P}_S = (p_S(s),\, s \in \mathbf{S})$, $\mathcal{P}_E = (p_E(e),\, e \in \mathbf{E})$. Они индуцируют распределение вероятностей $\mathcal{P}_M = (p_M(m),\, m \in \mathbf{M})$ на множестве $\mathbf{M}$ по формуле

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

Пусть S, E, M — случайные величины с указанными распределениями, а

$$\mathcal{P}_{SM},\ \mathcal{P}_{M|S},\ \mathcal{P}_{S|M},\ \mathcal{P}_{EM},\ \mathcal{P}_{M|E},\ \mathcal{P}_{E|M}$$

— совместное и условные распределения случайных величин S, E, M. Предполагается, что противник может модифицировать (или подменять) сообщения (атака *подмены*), а также вводить поддельные сообщения (атака *имитации*).

[2] От *authenticator* (или *tag*).

[3] Аналог омофона при шифровании.

Если каждое правило кодирования может использоваться многократно, то противник имеет возможность проведения атак на основе наблюдения сообщений, образованных с помощью одного правила кодирования. Атака достигает успеха, если поддельное сообщение принимается как аутентичное. При случайном выборе (стороной защиты) состояний источника и правил кодирования А-кода можно оценить вероятность успеха атаки. Говорят, что целью такой атаки является *навязывание наугад*. Если противник пытается добиться в атаке того, чтобы поддельное сообщение передавало конкретное состояние источника, то говорят о *целевом навязывании*. Мы будем рассматривать лишь случай навязывания наугад.

В случае когда каждое правило кодирования используется однократно, противник проводит атаки на основе наблюдения $t \in \{0,1\}$ сообщений: при $t = 0$ — *атаку имитации* (в этом случае говорят об *имитации в пустом канале*), при $t = 1$ — *атаку подмены*.

Стойкость А-кода к атаке имитации оценивают вероятностью $\mathbf{p}_0$ *успеха имитации*, определяемой следующим образом. Пусть $\mathbf{p_I}(m)$ — вероятность события «$m \in e(\mathbf{S})$» при случайном выборе $e \in \mathbf{E}$, т. е. $\mathbf{p_I}(m)$ — вероятность того, что «имитируемое сообщение» $m \in \mathbf{M}$ будет принято как аутентичное. Она вычисляется по формуле

$$\mathbf{p_I}(m) = \sum_{e \in \mathbf{E}(m)} p_E(e).$$

Тогда вероятность успеха имитации для А-кода определяется как максимум

$$\mathbf{p}_0 = \max_{m \in \mathbf{M}} \mathbf{p_I}(m).$$

Вероятность $\mathbf{p}_1$ *успеха подмены* определяется следующим образом. Пусть $m, n \in \mathbf{M}$ — различные сообщения и $\mathbf{p_S}(n|m)$ — вероятность успеха при подмене сообщения m сообщением n. Эта условная вероятность вычисляется по формуле

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

где $\mathbf{E}(m,n) = \mathbf{E}(m) \cap \mathbf{E}(n)$. Пусть

$$\mathbf{p_S}(m) = \max_{n \neq m} \mathbf{p_S}(n|m).$$

Тогда вероятность успеха подмены для А-кода определяется как максимум

$$\mathbf{p}_1 = \max_{m \in M} \mathbf{p_S}(m).$$

Пусть противник атакует на основе наблюдения r сообщений, полученных с использованием одного правила кодирования. При этом предполагается, что последовательность $s^r = (s_1, \ldots, s_r)$ состояний источника порождается случайным процессом, характеризуемым семейством распределений вероятностей

$$\mathcal{P}_{S^l} = \left\{ p_{S^l}(s^l), s^l \in \mathbf{S}^l \right\}, \; l \in \mathbb{N},$$

в котором $p_{S^l}(s^l) > 0$ в том и только том случае, когда s^l состоит из различных элементов[4]. Эти распределения удовлетворяют условию согласованности, в силу которого при $1 \leqslant t_1 < \ldots < t_l \leqslant r \leqslant k$ выполняется равенство

$$p_{S^l}\left(s_{t_1}, \ldots, s_{t_l}\right) = \sum_{s_i \in \mathbf{S},\, i \in \{1,\ldots,r\} \setminus \{t_1,\ldots,t_l\}} p_{S^r}\left(s_1, \ldots, s_r\right).$$

Пусть для А-кода без расщепления $m^r = (m_1, \ldots, m_r)$, $r \geqslant 1$, — последовательность сообщений, образованных с помощью одного правила кодирования $e \in \mathbf{E}$. Если противник использует атаку имитации, то он посылает вслед за m^r сообщение $m' \in M$. Оно принимается как аутентичное, если $m' \in \mathbf{M}(e) = \left\{ n \in M | e^{-1}(n) \neq \mathbf{o} \right\}$ и состояния источника не повторяются, т. е. если $e^{-1}(m') \neq e^{-1}(m_i)$, $i = 1, \ldots, r$. Если же противник использует атаку подмены, то он заменяет следующее за m^r сообщение m своим сообщением $m' \neq m$. Он добьется успеха, если дополнительно к указанным условиям $e^{-1}(m') \neq e^{-1}(m)$. Но для А-кода без расщепления последнее условие выполняется автоматически. Сказанное означает, что противник имеет равные шансы на успех как при имитации, так и при подмене. В связи с этим можно не различать атаки имитации и подмены и, следуя Мэсси, называть любую такую атаку на А-код без расщепления *активной атакой порядка* r.

Замечание. При разработке теории безусловно стойких А-кодов в 70–80-е годы XX в. использовалась концепция, согласно которой аутентифицируемая информация предварительно подвергается преобразованию, уменьшающему ее избыточность, а затем применяется кодирование. Предварительный этап позволял полагать, что источник информации вырабатывает последовательность, близкую к равновероятной. Этот подход послужил импульсом к исследованиям А-кодов с равновероятными состояниями источника. Таким А-кодам уделено значительное внимание в научной литературе. Вместе с тем не меньший интерес представляют и А-коды, обеспечивающие достаточный уровень стойкости для произвольного источника.

[4] Если дважды приходит одно и то же сообщение, то получатель не может определить, было повторное сообщение послано отправителем или повторено противником.

Пусть $\mathbf{p}_r$ — вероятность успеха активной атаки порядка r. Известны следующие оценки.

Теорема 1 ([45]). *Для любого A-кода*

$$\mathbf{p}_0 \geqslant \frac{k}{v}. \tag{1}$$

Равенство в (1) *имеет место тогда и только тогда, когда*

$$\sum_{e \in \mathbf{E}(m)} p_E(e) = \frac{k}{v} \quad \textit{для любого} \quad m \in \mathbf{M}.$$

Теорема 2 ([45]). *Для любого A-кода*

$$\mathbf{p}_1 \geqslant \frac{k-1}{v-1}\,. \tag{2}$$

Равенство в (2) *имеет место тогда и только тогда, когда для любых различных* $m, n \in \mathbf{M}$

$$\frac{1}{p_M(m)} \sum_{e \in \mathbf{E}(m,n)} p_E(e) \cdot p_S(e^{-1}(m)) = \frac{k-1}{v-1}\,.$$

Теорема 3 ([20]). *Для любого A-кода*

$$\max\{\mathbf{p}_0, \mathbf{p}_1\} \geqslant \frac{1}{\sqrt{b}}\,.$$

Теорема 4 ([34]). *При* $r \geqslant 0$ *для любого A-кода*

$$\mathbf{p}_r \geqslant \frac{k-r}{v-r}\,. \tag{3}$$

2. A-коды с секретностью с неявно заданным правилом кодирования

2.1. A-коды, обеспечивающие минимально возможные значения вероятности $\mathbf{p}_r$

Заметим, что в (2) равенство возможно лишь для A-кода с секретностью, поскольку известно, что для A-кода без секретности $\mathbf{p}_1 \geqslant k/v$ ([59], теорема 9.2.2). В связи с этим интересен вопрос о том, каково «качество шифрования» A-кода, для которого достигаются нижние оценки вероятностей $\mathbf{p}_0, \mathbf{p}_1$. Оказывается, что такой A-код создает равновероятный шифртекст.

Теорема 5 ([42]). *Для A-кода равенства в* (1) *и* (2) *выполняются в том и только том случае, когда для любых* $m, n \in \mathbf{M}$, $n \neq m$,

$$\sum_{e \in \mathbf{E}(m,n)} p_E(e) \cdot p_S(e^{-1}(m)) = \frac{k-1}{v(v-1)}\,.$$

При этом $\mathcal{P}_M$ *— равномерное распределение.*

Оценки (1) и (2) достижимы лишь при условии, что число правил кодирования велико. Это вытекает из следующего утверждения, в котором используется понятие t-схемы. Напомним определение.

Пусть v, k, λ, t — натуральные числа, $t \leqslant k$. Будем называть t-(v, k, λ)-*схемой* (или t-*схемой*) пару $(\mathbf{M}, \mathbf{E})$, где $\mathbf{M}$ — множество мощности v и $\mathbf{E}$ — семейство, состоящее из b таких k-подмножеств (*блоков*) множества $\mathbf{M}$, что любое подмножество из t элементов множества $\mathbf{M}$ содержится точно в λ блоках. *Симметричной* называется t-схема, в которой $b = v$.

Теорема 6 ([47]). *Пусть для A-кода без расщепления* $\mathbf{p}_1 = (k-1)/(v-1)$. *Тогда*

$$b \geqslant \frac{v^2 - v}{k^2 - k}\,. \tag{4}$$

Равенство в (4) имеет место тогда и только тогда, когда строки матрицы аутентификации A-кода, рассматриваемые как подмножества элементов из $\mathbf{M}$, образуют 2-$(v, k, 1)$-схему. Если при этом $\mathbf{p}_0 = k/v$, то $\mathcal{P}_S$ и $\mathcal{P}_E$ — равномерные распределения.

Справедливо обращение этого утверждения.

Теорема 7 ([47]). *Если существует* 2-$(v, k, 1)$-*схема, то существует и A-код без расщепления, имеющий* $b \geqslant (v^2 - v)/(k^2 - k)$ *правил кодирования и обеспечивающий для равномерных распределений* $\mathcal{P}_S$ *и* $\mathcal{P}_E$ *значения* $\mathbf{p}_0 = k/v$, $\mathbf{p}_1 = (k-1)/(v-1)$.

Следующее утверждение предлагает другую нижнюю оценку числа правил кодирования.

Теорема 8 ([41]). *Пусть для A-кода* $\mathbf{p}_1 = (k-1)/(v-1)$ *и* $v > k$. *Тогда* $b \geqslant v$.

A-код, имеющий параметры

$$\mathbf{p}_0 = k/v,\ \mathbf{p}_1 = (k-1)/(v-1),\ b = \min\left\{v, (v^2 - v)/(k^2 - k)\right\},$$

называют *экстремальным* A-кодом.

Теорема 9 ([41]). *Строки матрицы аутентификации экстремального A-кода, рассматриваемые как подмножества символов из* $\mathbf{M}$, *образуют симметричную* $2\text{-}(v,k,\lambda)$*-схему в том и только том случае, когда распределение* $\mathcal{P}_S$ *равномерное.*

A-код называется t*-стойким* к активным атакам[5], если в (3) выполняется равенство для любого целого r, $0 \leqslant r \leqslant t$.

Известны следующие результаты о числе правил кодирования t-стойкого к активным атакам A-кода ([50], [12]).

Теорема 10. *Если A-код является* $(t-1)$*-стойким к активным атакам, то число* b *его правил кодирования удовлетворяет неравенству* $b \geqslant \binom{v}{t}/\binom{k}{t}$.

Теорема 11. *Если существует* $t\text{-}(v,k,\lambda)$*-схема, то существует A-код, имеющий* k *состояний источника,* v *сообщений и* $\lambda\binom{v}{t}/\binom{k}{t}$ *правил кодирования,* $(t-1)$*-стойкий к активным атакам. Обратно, если существует A-код, имеющий* k *равновероятных состояний источника,* v *сообщений и* $\binom{v}{t}/\binom{k}{t}$ *правил кодирования,* $(t-1)$*-стойкий к активным атакам, то существует* $t\text{-}(v,k,1)$*-схема.*

2.2. A-коды, реализующие ϵ-совершенное шифрование

A-код с секретностью не позволяет по наблюдаемому сообщению однозначно восстановить состояние источника. В связи с этим можно говорить о его криптографической стойкости. Некоторые A-коды реализуют совершенное (по К. Шеннону) шифрование или близкое к нему ϵ-совершенное шифрование. Имеются в виду следующие определения.

A-код с данными распределениями $\mathcal{P}_S, \mathcal{P}_E$ реализует *совершенное шифрование*, если при любых $s \in \mathbf{S}, m \in \mathbf{M}$

$$p_{S|M}(s|m) = p_S(s).$$

A-код с данными распределениями $\mathcal{P}_S, \mathcal{P}_E$ реализует ϵ*-совершенное шифрование*, где $\epsilon \in [0,1)$, если

$$\max_{s\in\mathbf{S},m\in\mathbf{M}} \left|p_{S|M}(s|m) - p_S(s)\right| \leqslant \epsilon. \tag{5}$$

Отметим, что свойство A-кода реализовать совершенное шифрование не зависит от распределения вероятностей $\mathcal{P}_S$ в отличие от свойства реализовать ϵ-совершенное шифрование. При изменении $\mathcal{P}_S$ может изменяться и соответствующее значение ϵ.

[5] t-fold secure against spoofing.

Для А-кода $\mathcal{AC}$ обозначим через $\Delta_{\mathcal{AC}}$ левую часть в (5). Величина $\Delta_{\mathcal{AC}}$ — мера стойкости шифрования А-кода (к атаке на основе данного сообщения). Чем меньше $\Delta_{\mathcal{AC}}$, тем «ближе» шифрование, реализуемое А-кодом $\mathcal{AC}$, к совершенному шифрованию, для которого $\Delta_{\mathcal{AC}} = 0$.

Меру близости шифрования, реализуемого А-кодом, к совершенному шифрованию можно ввести и по-другому. Пусть $m \in \mathbf{M}$ и $\mathbf{S}(m) = \{s \in \mathbf{S} \colon \exists e \in \mathbf{E} \,|\, e(s) = m\}$. Распределение $\mathcal{P}_S$ индуцирует распределение вероятностей $\mathcal{P}_{S(m)}$ на подмножестве $\mathbf{S}(m) \subseteq \mathbf{S}$, где

$$p_{S(m)}(s) = (1/p)p_S(s), \quad p = \sum_{s' \in \mathbf{S}(m)} p_S(s').$$

Пусть $S(m)$ — случайная величина с множеством исходов $\mathbf{S}(m)$, $\mathsf{P}\left[S(m) = s\right] = p_{S(m)}(s)$. Энтропия $\mathbf{H}\left(S(m)\right)$ — мера неопределенности выбора состояния источника, соответствующего сообщению m. Величина

$$n_{\mathcal{AC}} = \min_{m \in \mathbf{M}} \mathbf{H}\left(S(m)\right)$$

характеризует для А-кода неопределенность выбора состояния источника, соответствующего произвольному сообщению. Чем больше $n_{\mathcal{AC}}$, тем «ближе» А-код к А-коду, который реализует совершенное шифрование и для которого $n_{\mathcal{AC}} = \mathbf{H}(S)$. При равномерном распределении $\mathcal{P}_S$ выполняется равенство $n_{\mathcal{AC}} = \log_2 |\mathbf{S}|$. Будем говорить, что А-код $\mathcal{AC}$ *создает* $n_{\mathcal{AC}}$ *битов секретности*.

Отметим, что термин «число битов секретности» встречается, например, в [43, 44]. Можно пояснить взаимную зависимость величин $\Delta_{\mathcal{AC}}$ и $n_{\mathcal{AC}}$ следующим образом. Пусть для А-кода $\mathcal{AC}$ распределения $\mathcal{P}_S$ и $\mathcal{P}_E$ равномерны. Тогда

$$p_{S|M}(s|m) = \frac{p_{M|S}(m|s)p_S(s)}{p_M(m)} = \frac{|\mathbf{E}(s,m)|\,|\mathbf{S}|\,|\mathbf{E}|}{|\mathbf{S}|\,|\mathbf{E}|\,|\mathbf{E}(m)|} = \frac{|\mathbf{E}(s,m)|}{|\mathbf{E}(m)|},$$

где $\mathbf{E}(s,m) = \{e \in \mathbf{E} | e(s) = m\}$. Отсюда следует, что

$$\Delta_{\mathcal{AC}} = \max_{s,m} \left| \frac{|\mathbf{E}(s,m)|}{|\mathbf{E}(m)|} - \frac{1}{|\mathbf{S}|} \right|. \tag{6}$$

Заметим, что имеет место разбиение

$$\mathbf{E}(m) = \bigcup_{s \in \mathbf{S}(m)} \mathbf{E}(s,m). \tag{7}$$

Предположим, что для А-кода $\mathcal{AC}$ величина $|\mathbf{S}(m)|$ не зависит от выбора m. Тогда из (7) следует равенство

$$|\mathbf{S}(m)| = \frac{|\mathbf{E}(m)|}{|\mathbf{E}(s,m)|},$$

откуда, с учетом (6), находим

$$\Delta_{\mathcal{AC}} = \frac{1}{|\mathbf{S}(m)|} - \frac{1}{|\mathbf{S}|}. \tag{8}$$

Если $\Delta_{\mathcal{AC}}$ выражается формулой (8), то

$$n_{\mathcal{AC}} = \log_2 |\mathbf{S}(m)| = \log_2 \frac{|\mathbf{S}(m)|}{\Delta_{\mathcal{AC}} |\mathbf{S}(m)| + 1}.$$

Итог подведем в следующем утверждении.

Теорема 12. *Пусть $\mathcal{AC}$ — это ϵ-совершенный А-код, для которого $\mathcal{P}_S, \mathcal{P}_E$ — равномерные распределения, а величина $|\mathbf{S}(m)|$ не зависит от выбора m. Тогда $\mathcal{AC}$ создает*

$$\log_2 |\mathbf{S}(m)| - \log_2 (\epsilon\, |\mathbf{S}(m)| + 1)$$

битов секретности.

Качественно последнее утверждение означает, что при уменьшении ϵ увеличивается число создаваемых А-кодом битов секретности, и наоборот.

Оптимальным называют А-код, который имеет минимально возможное число правил кодирования (ключей), обеспечивающее указанный набор свойств А-кода.

Д. Стинсон получил следующий критерий.

Теорема 13 ([48])**.** *Оптимальный А-код, реализующий совершенное шифрование и имеющий параметры*

$$\mathbf{p}_0 = \frac{k}{v}, \quad \mathbf{p}_1 = \frac{k-1}{v-1}, \quad b = \frac{v^2 - v}{k^2 - k},$$

существует тогда и только тогда, когда $v - 1 \equiv 0 \mod \left(k^2 - k\right)$ и существует 2-$(v, k, 1)$-схема. При этом $\mathcal{P}_S, \mathcal{P}_E$ — равномерные распределения.

В [41] показано, что для экстремального А-кода, реализующего совершенное шифрование, распределение $\mathcal{P}_S$ не обязано быть равномерным.

Теорема 14 ([41]). *Существует экстремальный А-код, реализующий совершенное шифрование, для которого вероятность $p_S(s)$ принимает не более двух различных значений для любого $s \in \mathbf{S}$.*

Теорема 15 ([41]). *Для любого $q \geqslant 3$, которое является степенью простого числа, существует экстремальный А-код, имеющий $k = 2q - 1$ состояний источника и $v = q^2 - 1$ сообщений, реализующий совершенное шифрование.*

Используя $2\text{-}\left(\left(q^{d+1} - 1\right)/(q-1), q+1, 1\right)$-схему частного вида, Д. Стинсон построил бесконечный класс оптимальных А-кодов, реализующих совершенное шифрование.

Теорема 16 ([48]). *Для любого q, являющегося степенью простого числа, и любого четного числа $d \geqslant 2$ существует оптимальный А-код, имеющий $q+1$ состояний источника и $\left(q^{d+1} - 1\right)/(q-1)$ сообщений, который при равномерном распределении $\mathcal{P}_S$ является 1-стойким к активным атакам и реализует совершенное шифрование.*

М. Хубер обобщил последнее утверждение.

Теорема 17 ([23]). *Предположим, что существует $t\text{-}(v, k, 1)$-схема, $t \geqslant 2$, где v делит число блоков b. Тогда существует оптимальный А-код, имеющий k состояний источника, v сообщений и $\binom{v}{t} / \binom{k}{t}$ правил кодирования, который является $(t-1)$-стойким к активным атакам и реализует совершенное шифрование для равномерного распределения $\mathcal{P}_S$.*

Используя конструкцию на основе сферической геометрии, М. Хубер построил следующий бесконечный класс оптимальных А-кодов.

Теорема 18 ([23]). *Пусть q — степень простого числа и $d \geqslant 2$ — четное число. Тогда существует оптимальный А-код, имеющий $q+1$ состояний источника и $q^d + 1$ сообщений, который при равномерном распределении $\mathcal{P}_S$ является 2-стойким к активным атакам и обеспечивает совершенное шифрование.*

В табл. 1 и 2 указаны параметры оптимальных А-кодов, построенных в [23, 24]. Все эти А-коды являются оптимальными, t-стойкими к активным атакам и обеспечивают совершенное шифрование.

Таблица 1

t	k	v	b	Параметры схемы t-$(v,k,1)$	Ссылка
1	$q+1,\ \ q=p^m,$ m — простое	$\frac{q^{d+1}-1}{q-1}$ $d\geqslant 2$ — четное	$\frac{v(v-1)}{k(k-1)}$	2-$(v,k,1)$	[48]
1	3	$v\equiv 1 \mod 6$	$\frac{v(v-1)}{6}$	2-$(v,3,1)$	[23]
1	4	$v\equiv 1 \mod 12$	$\frac{v(v-1)}{12}$	2-$(v,4,1)$	[23]
1	5	$v\equiv 1 \mod 20$	$\frac{v(v-1)}{20}$	2-$(v,5,1)$	[23]
2	$q+1,\ q=p^m,$ m — простое	q^d+1 $d\geqslant 2$ — четное	$\frac{v(v-1)(v-2)}{k(k-1)(k-2)}$	3-$(q^d{+}1,q{+}1,1)$	[23]
2	4	$v\equiv 2,10 \mod 24$	$\frac{v(v-1)(v-2)}{24}$	3-$(v,4,1)$	[23]

Таблица 2

t	k	v	b	Параметры схемы t-$(v,k,1)$	Ссылка
2	5	26	260	3-$(26,5,1)$	Denniston design
3	5	11	66	4-$(11,5,1)$	Witt design
	7	23	253	4-$(23,7,1)$	Witt design
	5	23	1771	4-$(23,5,1)$	Denniston design
	5	47	35673	4-$(47,5,1)$	Denniston design
	5	83	367524	4-$(83,5,1)$	Denniston design
	5	71	194327	4-$(71,5,1)$	Mills design
	5	107	1032122	4-$(107,5,1)$	[12]
	5	131	2343328	4-$(131,5,1)$	[12]
	5	167	6251311	4-$(167,5,1)$	[12]
	5	243	28344492	4-$(243,5,1)$	[12]
4	6	12	132	5-$(12,6,1)$	Witt design
	6	84	5145336	5-$(84,6,1)$	Denniston design
	6	244	1152676008	5-$(244,6,1)$	[12]

Известны конструкции А-кодов, обеспечивающих стойкость к активным атакам и совершенную стойкость шифрования при кратном использовании правила кодирования. Чтобы определить такие А-коды, введем на множестве $\mathbf{S}^L$, $L \in \mathbb{N}$, распределение вероятностей $\mathcal{P}_{S^L}$ формулой $p_{S^L}(\overline{s}) = \prod_{i=1}^{L} p_S(s_i)$, где $\overline{s} = (s_1, \ldots, s_L) \in S^L$. Пусть $\overline{\mathbf{S}}(L)$ и $\mathbf{S}(L)$ — множества всех размещений и сочетаний из L элементов множества $\mathbf{S}$. Распределение $\mathcal{P}_{S^L}$ индуцирует распределения вероятностей $\mathcal{P}_{\overline{S}(L)}$ и $\mathcal{P}_{S(L)}$ на множествах $\overline{\mathbf{S}}(L)$ и $\mathbf{S}(L)$ так, что для $\overline{s} \in \overline{\mathbf{S}}(L)$

$$p_{\overline{S}(L)}(\overline{s}) = \frac{p_{S^L}(\overline{s})}{\sum_{\overline{s'} \in \mathbf{S}(L)} p_{S^L}(\overline{s'})},$$

а для $\mathbf{S}' \in \mathbf{S}(L)$

$$p_{S(L)}(\mathbf{S}') = L! p_{\overline{S}(L)}(\overline{s}),$$

где $\overline{s}$ — любое размещение из элементов множества $\mathbf{S}'$.

Назовем $\mathbf{M}' \in \mathbf{M}(L)$ ($\overline{m} \in \overline{\mathbf{M}}(L)$) *допустимым*, если $\mathbf{M}' = e(\mathbf{S}')$ ($\overline{m} = e(\overline{s})$) для некоторых $\mathbf{S}' \in \mathbf{S}(L)$, $\overline{s} \in \overline{\mathbf{S}}(L)$ и $e \in \mathbf{E}$.

Априорные распределения $\mathcal{P}_{S(L)}$ ($\mathcal{P}_{\overline{S}(L)}$) и $\mathcal{P}_K$ индуцируют распределения вероятностей $\mathcal{P}_{M_{dop}(L)}$ ($\mathcal{P}_{\overline{M}_{dop}(L)}$) на множествах допустимых совокупностей из L элементов множества $\mathbf{M}$ по формулам

$$p_{M_{dop}(L)}(\mathbf{M}') = \sum_{\mathbf{S}' \in \mathbf{S}(L)} p_{S(L)}(\mathbf{S}') \sum_{e \in \mathbf{E}(\mathbf{S}', \mathbf{M}')} p_E(e)$$

и

$$p_{\overline{M}_{dop}(L)}(\overline{m}) = \sum_{\overline{s} \in \overline{\mathbf{S}}(L)} p_{\overline{S}(L)}(\overline{s}) \sum_{e \in \mathbf{E}(\overline{s}, \overline{m})} p_E(e).$$

Для $\mathbf{S}' \in \mathbf{S}(L)$ ($\overline{s} \in \overline{\mathbf{S}}(L)$) и $\mathbf{M}' \in \mathbf{M}_{dop}(L)$ ($\overline{m} \in \overline{\mathbf{M}}_{dop}(L)$) через $p_{S(L)|M_{dop}(L)}(\mathbf{S}'|\mathbf{M}')$ ($p_{\overline{S}(L)|\overline{M}(L)}(\overline{s}|\overline{m})$) обозначим вероятность того, что $\mathbf{M}' = e(\mathbf{S}')$ ($\overline{m} = e(\overline{s})$) для случайно выбранного $e \in \mathbf{E}$.

Будем говорить, что А-код реализует *t-кратное совершенное шифрование*, если для любого t', $1 \leqslant t' \leqslant t$, любой совокупности $\mathbf{M}'$ из t' допустимых сообщений и любого множества $\mathbf{S}'$ из t' состояний источника выполняется равенство

$$p_{S(L)|M_{dop}(L)}(\mathbf{S}'|\mathbf{M}') = p_{S(L)}(\mathbf{S}').$$

В [21] t-кратно совершенный шифр назван *$U(t)$-стойким*. Для упорядоченных совокупностей состояний источника и сообщений понятие *$O(t)$-стойкого* шифра введено равенством

$$p_{\overline{S}(L)|\overline{M}_{dop}(L)}(\overline{s}|\overline{m}) = p_{\overline{S}(L)}(\overline{s}).$$

Введены также более специфические понятия $S(t)$- и $M(t)$-стойкого шифрований. В настоящем обзоре мы приводим известные результаты лишь об А-кодах, обладающих свойством t-кратного совершенного шифрования (совпадающего со свойством $U(t)$-стойкости). С А-кодами, обладающими свойствами $S(t)$-, $O(t)$- или $M(t)$-стойкого шифрования, можно познакомиться, помимо [21], в [10, 64, 58].

Теорема 19 ([13]). *Любая t-$(v,k,1)$-схема определяет А-код, имеющий k состояний источника, v сообщений и $\frac{v!(t-k)!}{(v-t)!}$ правил кодирования, который является $(t-1)$-стойким к активным атакам и обеспечивает t-кратное совершенное шифрование.*

Теорема 20 ([50]). *Если А-код реализует t-кратное совершенное шифрование, то $b \geqslant \binom{k}{t}$.*

Теорема 21 ([47]). *Если А-код реализует t-кратное совершенное шифрование и является $(t-1)$-стойким к активным атакам, то $b \geqslant \binom{v}{t}$.*

Теорема 22 ([50]). *Если А-код реализует t-кратное совершенное шифрование и является t-стойким к активным атакам, то $b \geqslant \binom{v}{t} \frac{v-t}{k-t}$.*

Теорема 23 ([13]). *Если А-код без расщепления реализует t-кратное совершенное шифрование и является t-стойким к активным атакам, $t' \leqslant t+1$, то $b \geqslant \binom{v}{t+1} \binom{k}{t'} / \binom{k}{t+1}$.*

А-коды, реализующие t-кратное совершенное шифрование, для которых $b = \binom{k}{t}$, можно построить на основе комбинаторных схем, называемых перпендикулярными массивами. *Перпендикулярный массив* $PA_\lambda(t,k,v)$ — это $\lambda\binom{v}{t} \times k$-матрица, состоящая из элементов множества $V = \{1,\ldots,v\}$, каждая строка которой содержит k различных элементов из V, и любые t различных элементов из V содержатся точно в λ строках подматрицы, образованной любыми t столбцами.

Теорема 24 ([50]). *Если существует массив $PA_\lambda(t,k,v)$, где $k \geqslant 2t-1$, то существует А-код, имеющий k состояний источника, v сообщений и $\lambda\binom{v}{t}$ правил кодирования, реализующий t-кратное совершенное шифрование.*

Верно и частичное обращение этого утверждения.

Теорема 25 ([50]). *Если существует А-код, имеющий k состояний источника, $\binom{v}{t}$ правил кодирования и реализующий t-кратное совершенное шифрование при $k \geqslant 2t-1$, то существует массив $PA_1(t,k,k)$. При этом распределение $\mathcal{P}_E$ должно быть равномерным.*

В [50] приводятся значения параметров, при которых существуют перпендикулярные массивы $PA_\lambda(t,k,v)$. Например, существуют массивы $PA_1(1,k,k)$ для любого $k \in \mathbb{N}$ и массивы $PA_1(2,k,k)$ для любого k, являющегося степенью нечетного простого числа.

Массив $A = PA_\lambda(t,k,v)$ называется *аутентификационным перпендикулярным массивом* и обозначается $APA_\lambda(t,k,v)$, если для любого t', $t' \leqslant t$, и любого подмножества $V' \subseteq V$, состоящего из $t'+1$ элементов, в строках матрицы A, содержащих V', любое подмножество из t' элементов V' входит во все возможные подмножества из t' столбцов матрицы A одинаковое число раз.

Теорема 26 ([51]). *Если существует массив $APA_\lambda(t,k,v)$, то существует оптимальный А-код, имеющий k состояний источника, v сообщений, $\lambda\binom{v}{t}$ правил кодирования, который реализует t-кратное совершенное шифрование и является $(t-1)$-стойким к активным атакам.*

В [50] приводятся параметры, при которых существуют массивы $APA_\lambda(t,k,v)$. Например, существуют массивы $APA_1(1,k,v)$ для всех $k \in \{1,\ldots,v\}$ и массивы $APA_3(3,q+1,q+1)$ для любого $q \geqslant 7$, $q \equiv 3 \bmod 4$, являющегося степенью простого числа. Более полная информация об $APA_\lambda(t,k,v)$ содержится в [56], где указано 154 класса таких массивов.

Имеет место частичное обращение последнего утверждения.

Теорема 27 ([50]). *Если существует А-код, имеющий k состояний источника, v сообщений, $\binom{v}{t}$ правил кодирования, который реализует t-кратное, $t \leqslant \frac{k+1}{2}$, совершенное шифрование и является $(t-1)$-стойким к активным атакам для любого распределения $\mathcal{P}_S$, то существует массив $APA_1(t,k,v)$.*

Теорема 28 ([50]). *Если существуют массив $APA_\lambda(t,k,k)$ и $(t{+}1)$-(v,k,λ')-схема, где $k \geqslant 2t-1$, то существует А-код, имеющий k состояний источник, v сообщений и $\frac{\lambda\lambda'(v-t)}{k-t}\binom{v}{t}$ правил кодирования, который для любого распределения $\mathcal{P}_S$ реализует t-кратное совершенное шифрование и является t-стойким к активным атакам.*

Имеет место и частичное обращение последнего утверждения.

Теорема 29 ([50]). *Если существует А-код, имеющий k состояний источника, v сообщений и $\frac{v-t}{k-t}\binom{v}{t}$ правил кодирования, который для любого распределения $\mathcal{P}_S$ реализует t-кратное совершенное шифрование и является t-стойким к активным атакам, то существует $(t{+}1)$-(v,k,λ)-схема, где $\lambda = \binom{k}{t}$.*

Следующие результаты относятся к A-кодам с равномерным распределением $\mathcal{P}_S$.

Теорема 30 ([24]). *Предположим, что существует* t-$(v,k,1)$*-схема, где* $\binom{v}{t'}$ *делит число блоков* b *для любого* t', $1 \leqslant t' \leqslant t-1$. *Тогда существует оптимальный A-код, имеющий* k *состояний источника,* v *сообщений,* $\binom{v}{t} / \binom{k}{t}$ *правил кодирования, который при равномерном распределении* $\mathcal{P}_S$ *обеспечивает* $(t-1)$*-стойкость к активным атакам и* $(t-1)$*-кратное совершенное шифрование.*

Теорема 31 ([24]) . *Для любого* $v \in \mathbb{N}$, $v \equiv 2 \bmod 24$, *существует оптимальный A-код, имеющий* $k = 4$ *состояния источника,* v *сообщений,* $v(v-1)(v-2)/24$ *правил кодирования, который при равномерном распределении* $\mathcal{P}_S$ *обеспечивает* 2*-стойкость к активным атакам и* 2*-кратное совершенное шифрование.*

Пример A-кода из последнего утверждения строится на основе штейнеровой четверной системы $SQS(v)$, представляющей собой 3-$(v,4,1)$-схему. Наименьший пример такой системы, $SQS(26)$, имеет параметры $v = 26$, $b = 650$.

В [19] изучаются A-коды с секретностью с равномерными распределениями $\mathcal{P}_S, \mathcal{P}_E$, построенные на основе графов, схем отношений и конечных групп.

A-коду $\mathcal{AC}(b,k,v)$ сопоставляется двудольный граф $\Gamma(\mathcal{AC})$ с множеством вершин $V = \mathbf{E} \cup \mathbf{M}$ и ребер $W = \{(e,m) | \, m \in \mathbf{M}(e)\}$. Долями графа являются множества $\mathbf{E}$ и $\mathbf{M}$. Поскольку $|\mathbf{M}(e)| = k$, степень каждой вершины $e \in \mathbf{E}$ равна k. Будем говорить, что $\Gamma(\mathcal{AC})$ индуцирован A-кодом $\mathcal{AC}$. С другой стороны, двудольный граф Γ, имеющий множество вершин $V = \mathbf{E} \cup \mathbf{M}$, доли $\mathbf{E}, \mathbf{M}$ и степень каждой вершины $e \in \mathbf{E}$, равную k, индуцирует A-код $\mathcal{AC}(\Gamma)$ с множеством $\mathbf{S}$, образованным k состояниями источника, множеством правил кодирования $\mathbf{E}$ и множеством сообщений $\mathbf{M}$. Если $V(e)$ — множество вершин, смежных вершине $e \in \mathbf{E}$, и $f_e \colon \mathbf{S} \to V(e)$ — произвольная биекция, то правило кодирования определяется равенством $e(s) = f_e(s)$. Поскольку для каждой вершины $e \in \mathbf{E}$ имеется $k!$ биекций f_e, с графом Γ ассоциируется $(k!)^{|\mathbf{E}|}$ различных A-кодов. При равномерных распределениях $\mathcal{P}_S, \mathcal{P}_E$ такие A-коды имеют одинаковые значения $\mathbf{p}_0, \mathbf{p}_1$.

Для A-кода $\mathcal{AC}(b,k,v)$, реализующего совершенное шифрование, выполняется неравенство $b \geqslant v$. A-код, для которого $b = v$, называется *минимальным*. Если $\mathcal{AC}$ — минимальный A-код, обеспечивающий совершенное шифрование, то граф $\Gamma(\mathcal{AC})$ является k-регулярным.

Теорема 32 ([19]). *Если существует k-регулярный двудольный граф Γ с $2n$ вершинами, то существует минимальный А-код $\mathcal{AC}(b,k,v)$, обеспечивающий совершенное шифрование.*

Для такого А-кода $\mathbf{p}_0 = k/v$, $\mathbf{p}_1 = \max\{1/k, (k-1)/(n-1)\}$. Равенство $\mathbf{p}_1 = k/v$ имеет место тогда и только тогда, когда граф Γ не содержит циклов длины 4.

Минимальные А-коды, обеспечивающие совершенное шифрование, можно строить на основе схем отношений. Напомним соответствующее определение.

Пусть X — конечное множество и R_i, $i = 0, \ldots, d$, — подмножества в $X \times X$, удовлетворяющие следующим условиям:

1. $R_0 = \{(x,x) | \, x \in X\}$.
2. $X \times X = \bigcup_0^d R_i$, $R_i \cap R_j = \varnothing$ при $i \neq j$.
3. Для любого i, $0 \leqslant i \leqslant d$, найдется такое i', $0 \leqslant i' \leqslant d$, что
$$\overline{R}_i = \{(y,x) | (x,y) \in R_i\} = R_{i'}.$$
4. Для любых i,j,k, $0 \leqslant i,j,k \leqslant d$, число таких $z \in X$, что $(x,z) \in R_i$ и $(z,y) \in R_j$, не зависит от выбора x,y, если $(x,y) \in R_k$. Это число обозначается p_{ij}^k.
5. Для любых i,j,k, $0 \leqslant i,j,k \leqslant d$, выполняется равенство $p_{ij}^k = p_{ji}^k$.

Тогда совокупность $\mathcal{X} = \left(X, \{R_i\}_{0 \leqslant i \leqslant d}\right)$ называется *коммутативной схемой отношений* (или *ассоциативной схемой*) на X с d классами. Неотрицательные целые числа p_{ij}^k называются *числами пересечений схемы $\mathcal{X}$*.

Пусть $k_i = p_{ii'}^0$, т. е. k_i — число таких $z \in X$, что $(x,z) \in R_i$ для фиксированного $x \in X$. Это число не зависит от выбора x и называется *валентностью R_i*. Числа $n = |X|$, k_i и p_{ij}^k называются *параметрами схемы отношений $\mathcal{X}$*.

А-код на основе схемы отношений с двумя классами построен в [46]. Следующая, более общая конструкция А-кода предложена в [19].

Теорема 33. *Пусть $\mathcal{X} = \left(X, \{R_i\}_{0 \leqslant i \leqslant d}\right)$ — схема отношений с параметрами n, k_i, p_{ij}^k, $0 \leqslant i,j,k \leqslant d$. Для любого такого l, $1 \leqslant l \leqslant d$, что $k_l > 1$, существует минимальный А-код $\mathcal{AC}(k_l, n, n)$, обеспечивающий совершенное шифрование, для которого*

$$\mathbf{p}_0 = \frac{k_l}{n}, \quad \mathbf{p}_1 = \frac{1}{k_l} \max_{1 \leqslant j \leqslant d} p_{l'l}^j.$$

Пример 1 ([19]). Пусть $\mathcal{A}=\{0,1,\ldots,q-1\}$ и $X=\mathcal{A}^m, m\geqslant 1$. Для $x,y\in X$ и $i\in\{0,1,\ldots,m\}$ определим $(x,y)\in R_i$ условием $\mu_H(x,y)=i$, где μ_H — метрика Хэмминга. Тогда $\mathcal{X}=\left(X,\{R_i\}_{0\leqslant i\leqslant d}\right)$ — схема отношений с m классами. Она называется *схемой Хэмминга*. При $l=1$ схема имеет следующие параметры:

$$n=q^m,\quad k_1=m(q-1),\quad p_{11}^1=q-2,\quad p_{11}^2=2,\quad p_{11}^3=\ldots=p_{11}^m=0.$$

На основе этой схемы для любых m и $q\geqslant 4$ можно построить минимальный А-код $\mathcal{AC}\left(m(q-1),q^m,q^m\right)$, обеспечивающий совершенное шифрование, для которого

$$\mathbf{p}_0=\frac{m(q-1)}{q^m},\quad \mathbf{p}_1=\frac{q-2}{m(q-1)}.$$

Например, при $m=2$, $q=4$ получается минимальный А-код $\mathcal{AC}(6,16,16)$, обеспечивающий совершенную стойкость.

В [19] показано также, как можно строить минимальные А-коды, обеспечивающие совершенное шифрование, на основе графов Кэли конечных групп.

Пусть Γ — k-регулярный граф с множеством вершин $V(\Gamma)=\{v_1,\ldots,v_n\}$. Построим граф $\widetilde{\Gamma}$ с множеством вершин $V(\widetilde{\Gamma})=\{v_1,\ldots,v_n\}\cup\{v_1',\ldots,v_n'\}$, в котором вершины v_i,v_j' смежны в том и только том случае, когда v_i,v_j смежны в Γ. Тогда $\widetilde{\Gamma}$ — k-регулярный двудольный граф. Он называется *каноническим двойным покрытием графа* Γ. Ясно, что $\widetilde{\Gamma}$ содержит 4-цикл в том и только том случае, когда Γ содержит 4-цикл. Это позволяет воспользоваться теоремой 32, которая дает минимальный А-код $\mathcal{AC}(k,n,n)$ с $\mathbf{p}_0=k/n$, $\mathbf{p}_1=1/k$, реализующий совершенное шифрование в случае, если граф Γ не содержит циклов длины 4. В свою очередь, k-регулярный граф можно следующим образом построить с помощью любой конечной группы.

Пусть G — конечная группа и H — такое подмножество в G, что $e\notin H$ и для любого $h\in H$ имеет место включение $h^{-1}\in H$. *Граф Кэли*, $\Gamma=Cay(G,H)$, *группы* G *с множеством соединителей* H имеет множество вершин $V(\Gamma)=G$, и вершины g,l смежны, если $g^{-1}l\in H$. Граф $\Gamma=Cay(G,H)$ — $|H|$-регулярный граф с $|G|$ вершинами. Как показано выше, его можно использовать для построения минимального А-кода, обеспечивающего совершенное шифрование.

Пример 2 ([28]). Пусть q — нечетное простое число и $G = F_q \times F_q$. Зададим на G операцию $*$ формулой $(a,b)*(a',b') = (a+a', b+b'+aa')$, в которой сложение и умножение выполняются в поле F_q. Тогда $(G,*)$ — группа порядка q^2 с единичным элементом $(0,0)$. Пусть H — линия аффинной плоскости $AG(2,q)$, не содержащая точку $(0,0)$. Тогда $H = \{(x,y) \,|\, ax+by=c\}$ для любых таких $a,b \in F_q$, что $(a,b) \neq (0,0)$, и $c \in F_q^*$. Граф Кэли $Cay(G,H)$ является q-регулярным графом с q^2 вершинами. На его основе можно построить А-код $\mathcal{AC}(q,q^2,q^2)$, обеспечивающий совершенное шифрование, для которого $\mathbf{p}_0 = \mathbf{p}_1 = 1/q$.

3. А-коды с явно заданным правилом кодирования

3.1. А-коды с секретностью на основе абелевых групп

Следующие конструкции А-кодов с секретностью обеспечивают ϵ-совершенное шифрование для равномерных распределений $\mathcal{P}_S, \mathcal{P}_E$.

Конструкция I ([14, 15]). Пусть $m,n \in \mathbb{N}$, m делит n. Пусть $\mathrm{Tr}\,(x)$ — функция след из F_{q^n} в F_{q^m}, определенная для $\alpha \in F_{q^n}$ формулой $\mathrm{Tr}\,(\alpha) = \alpha + \alpha^q + \ldots + \alpha^{q^{n/m-1}}$. Пусть $\mathcal{AC}_1$ — А-код, для которого $\mathbf{S} = F_{q^n}$, $\mathbf{K} = \mathbf{M} = F_{q^n} \times F_{q^m}$, и $e_\kappa(s) = (s+k_1, \mathrm{Tr}\,(sk_1)+k_2)$, где $s \in \mathbf{S}$, $\kappa = (k_1,k_2) \in \mathbf{K}$, а операции выполняются в соответствующем поле.

Теорема 34. *А-код $\mathcal{AC}_1$ реализует совершенное шифрование и имеет параметры $\mathbf{p}_0 = \mathbf{p}_1 = q^{-m}$.*

Конструкция II ([14, 15]). Пусть $\mathcal{AC}_2$ — А-код, для которого $\mathbf{S} = F_{q^n}^*$, $\mathbf{K} = \mathbf{M} = F_{q^n}^* \times F_{q^m}$, а правило кодирования задано формулой $e_\kappa(s) = (sk_1, \mathrm{Tr}\,(s+k_1)+k_2))$, где $s \in \mathbf{S}$, $\kappa = (k_1,k_2) \in \mathbf{K}$.

Теорема 35. *А-код $\mathcal{AC}_2$ реализует совершенное шифрование и имеет параметры*

$$\mathbf{p}_0 = \frac{1}{q^m}, \quad \mathbf{p}_1 = \frac{1}{q^m} + \frac{1}{q^m(q^n-1)}.$$

Конструкция III ([43]). Пусть q — степень простого числа и $m > 1$ — целое число. Пусть $L(x) = u_0x + u_1x^q + \ldots + u_hx^{q^h}$ — ненулевой многочлен и $\mathrm{Tr}\,(x)$ — функция след из F_{q^m} в F_q. Пусть $\mathcal{AC}_3$ — А-код, для которого $\mathbf{S} = F_{q^m}$, $\mathbf{K} = \mathbf{M} = F_{q^m} \times F_q$, и $e_\kappa(s) = (s+k_1, \mathrm{Tr}\,(L(s)k_1)+k_2)$, где $s \in \mathbf{S}$, $\kappa = (k_1,k_2) \in \mathbf{K}$.

Теорема 36. *А-код $\mathcal{AC}_3$ реализует совершенное шифрование и имеет параметры $\mathbf{p}_0 = \mathbf{p}_1 = 1/q$.*

Конструкция IV ([43]). Пусть $L(x)$ — многочлен из конструкции III и $B_L\colon F_{q^m}\times F_{q^m}\to F_q$ — симметрическая билинейная форма, заданная правилом $(x,y)\mapsto \operatorname{Tr}\left(xL(y)+yL(x)\right)$. Пусть W_L — радикал формы B_L, определенный формулой $W_L=\{a\in F_{q^m}\,|\,B_L(a,b)=0,\text{ для каждого } b\in F_{q^m}\}$, и d — размерность W_L над F_q. Пусть $\mathcal{AC}_4$ — А-код, для которого $\mathbf{S}=\mathbf{K}=F_{q^m}$, $\mathbf{M}=F_{q^m}\times F_q$, и правило кодирования определено формулой $e_\kappa(s)=(s+\kappa,\operatorname{Tr}\left(L(s)\kappa\right))$, где $s\in\mathbf{S}$, $\kappa\in\mathbf{K}$.

Теорема 37. *Для А-кода* $\mathcal{AC}_4$

$$\mathbf{p}_0\leqslant\begin{cases}\frac{1}{q}+\frac{q-1}{q}\cdot\frac{q^{d/2}}{q^{m/2}}, & \text{если } q \text{ четно или } q \text{ нечетно и } d\equiv m\,(\mathrm{mod}2),\\ \frac{1}{q}+\frac{q^{(d-1)/2}}{q^{m/2}}, & \text{если } q \text{ нечетно и } d\equiv m+1\,(\mathrm{mod}2),\end{cases}$$

$$\mathbf{p}_1\leqslant\begin{cases}\frac{1}{q}+\frac{\left(q^2+q-2\right)q^{d/2}}{q\left(q^{m/2}-(q-1)q^{d/2}\right)}, & \text{если } q \text{ четно или } q \text{ нечетно и } d\equiv m\,(\mathrm{mod}2),\\ \frac{1}{q}+\frac{(q+2)q^{(d-1)/2}}{q^{m/2}-q^{(d+1)/2}}, & \text{если } q \text{ нечетно и } d\equiv m+1\,(\mathrm{mod}2).\end{cases}$$

А-код $\mathcal{AC}_4$ *реализует* ϵ*-совершенное шифрование, создавая не менее чем*

$$\begin{array}{c}\log_2\left(q^{m-1}-(q-1)q^{(m+d-2)/2}\right), \text{ если } q \text{ четно или } q \text{ нечетно и } d\equiv m\,(\mathrm{mod}2),\\ \log_2\left(q^{m-1}-q^{(m+d-1)/2}\right), \quad \text{если } q \text{ нечетно и } d\equiv m+1\,(\mathrm{mod}2),\end{array}$$

битов секретности.

Конструкция V ([15]). Пусть $q=p^h$, p — нечетное простое число, $h\in\mathbb{N}$. Пусть $\mathcal{AC}_5$ — А-код, для которого $\mathbf{S}=\mathbf{K}=F_{q^n}$, $\mathbf{M}=F_{q^n}\times F_q$, и $e_\kappa(s)=(s+\kappa,\operatorname{Tr}\left(s\kappa\right))$, где $s\in\mathbf{S}$, $\kappa\in\mathbf{K}$.

Теорема 38. *А-код* $\mathcal{AC}_5$ *имеет параметры*

$$\mathbf{p}_0\leqslant\begin{cases}\frac{1}{q}+\frac{1}{q^{(n+1)/2}}, \text{ если } n \text{ четно и } p\equiv 1\,(\mathrm{mod}4) \text{ или}\\ \qquad\qquad p\equiv 3\,(\mathrm{mod}4) \text{ и } nh\equiv 0\,(\mathrm{mod}4),\\ \frac{1}{q}+\frac{q-1}{q^{(n+1)/2}}, \text{ если } n \text{ четно } p\equiv 3\,(\mathrm{mod}4) \text{ и } nh\equiv 2\,(\mathrm{mod}4),\\ \frac{1}{q}+\frac{1}{q^{(n+1)/2}}, \text{ если } n \text{ нечетно},\end{cases}$$

$$\frac{q^{n-1}-(q-1)q^{n/2}}{q^n+(q-1)q^{n/2}}\leqslant\mathbf{p}_1\leqslant\frac{q^{n-1}+(q-1)q^{n/2}}{q^{n-1}-(q-1)q^{n/2}}.$$

А-код $\mathcal{AC}_5$ *реализует* ϵ*-совершенное шифрование, создавая не менее чем*

$$\begin{array}{c}\log_2\frac{q^n-(q-1)q^{n/2}}{q}, \text{ если } n \text{ четно},\\ \log_2\frac{q^n-q^{(n+1)/2}}{q}, \text{ если } n \text{ нечетно},\end{array}$$

битов секретности.

Конструкция VI ([15]). Пусть $\mathcal{AC}_6$ — А-код, для которого $\mathbf{S} = \mathbf{K} = F_{q^n}^*$, $\mathbf{M} = F_{q^n}^* \times F_q$, и правило кодирования задается формулой $e_\kappa(s) = (s\kappa, \operatorname{Tr}(s+\kappa))$, где $s \in \mathbf{S}$, $\kappa \in \mathbf{K}$.

Теорема 39. *А-код $\mathcal{AC}_6$ имеет параметры*

$$\frac{1}{q} - \frac{2(q-1)q^{n/2}}{q(q^n-1)} \leqslant \mathbf{p}_0 \leqslant \frac{1}{q} + \frac{2(q-1)q^{n/2}}{q(q^n-1)},$$

$$\frac{-2(q^2-1)q^{n/2}+q^n-1}{q\left(2(q-1)q^{n/2}+q^n-1\right)} \leqslant \mathbf{p}_1 \leqslant \frac{2(q^2-1)q^{n/2}+q^n-1}{q\left(-2(q-1)q^{n/2}+q^n-1\right)}.$$

А-код $\mathcal{AC}_6$ реализует ϵ-совершенное шифрование, создавая не менее чем

$$\log_2 \frac{q^n-1-2(q-1)q^{n/2}}{q}$$

битов секретности.

Конструкция VII ([14]). Пусть $(A,+)$, $(B,+)$ — конечные абелевы группы и $\mathcal{F}\colon A \to B$ — произвольное отображение. А-код $\mathcal{AC}_7$ задается множествами $\mathbf{S} = A$, $\mathbf{K} = \mathbf{M} = A \times B$ и правилом кодирования $e_\kappa(s) = (s + k_1, \mathcal{F}(s) + k_2)$, где $s \in \mathbf{S}$, $\kappa \in \mathbf{K}$.

Теорема 40. *А-код $\mathcal{AC}_7$ реализует совершенное шифрование и имеет параметры*

$$\mathbf{p}_0 = 1/|B|, \ \mathbf{p}_1 = \max_{\delta_1 \neq 0, \delta_2} \mathsf{P}\left[\mathcal{F}(s+\delta_1) - \mathcal{F}(s) = \delta_2\right].$$

В последней формуле вероятность вычисляется при случайном и равновероятном выборе $s \in \mathbf{S}$.

Рассматриваются частные случаи конструкции VII, когда отображение $\mathcal{F}$ имеет специальный вид. Пусть $\mathcal{F}\colon A \to B$ — произвольное отображение. Мерой нелинейности отображения $\mathcal{F}$ служит величина

$$\mathbf{p}_{\mathcal{F}} = \max_{0 \neq a \in A} \max_{b \in B} \mathsf{P}\left[\mathcal{F}(x+a) - \mathcal{F}(x) = b\right] = \\ = \max_{0 \neq a \in A} \max_{b \in B} \frac{|\{x \in A | \mathcal{F}(x+a) - \mathcal{F}(x) = b\}|}{|A|}.$$

Отображение $\mathcal{F}\colon A \to B$ называется *максимально нелинейным*, если $\mathbf{p}_{\mathcal{F}} = 1/|B|$.

Теорема 41. *А-код $\mathcal{AC}_7$, использующий в качестве $\mathcal{F}$ максимально нелинейное отображение, реализует совершенное шифрование и имеет параметры* $\mathbf{p}_0 = \mathbf{p}_1 = 1/|B|$.

Конструкция VIII ([43]). А-код $\mathcal{AC}_8$ задан множествами $\mathbf{S} = \mathbf{K} = A$, $\mathbf{M} = A \times B$, где $(A,+)$, $(B,+)$ — абелевы группы, и правилом кодирования $e_\kappa(s) = (s+\kappa, \mathcal{F}(s)+\mathcal{F}(\kappa))$, где $s \in \mathbf{S}$, $\kappa \in \mathbf{K}$, $\mathcal{F}\colon A \to B$ — произвольное отображение.

Теорема 42. *А-код $\mathcal{AC}_8$ имеет параметры*

$$\mathbf{p}_0 = \max_{m_1,m_2} \mathsf{P}\left[\mathcal{F}(m_1-\kappa)+\mathcal{F}(\kappa) = m_2\right],$$
$$\mathbf{p}_1 = \max_{\delta_1\neq 0,\delta_2,m_1,m_2} \mathsf{P}\left[\mathcal{F}(s+\delta_1)-\mathcal{F}(s) = \delta_2 | m_2 = \mathcal{F}(s)+\mathcal{F}(m_1-s)\right].$$

Рассматриваются частные случаи отображения $\mathcal{F}$.

Теорема 43. *Пусть в конструкции* VIII $(A,+)=((F_q)^{2t},+)$, $(B,+)=(F_q,+)$,

$$\mathcal{F}(x_1,\ldots,x_{2t}) = x_1x_2 + x_3x_4 + \ldots + x_{2t-1}x_{2t}.$$

Тогда А-код $\mathcal{AC}_8$ имеет параметры

$$\mathbf{p}_0 = \frac{1}{q} + \frac{q-1}{q^{t+1}}, \quad \mathbf{p}_1 \leqslant \frac{q^{t-1}+q-1}{q^t-q+1}$$

и реализует ϵ-совершенное шифрование, создавая не менее чем $\log_2\left(q^{2t-1}-q^{t-1}\right)$ битов секретности.

Теорема 44. *Пусть в конструкции* VIII $(A,+)=(F_{q^n},+)$, $(B,+)=(F_q,+)$, $\mathcal{F}(x)=\mathrm{Tr}\,(x^2)$. *Тогда А-код $\mathcal{AC}_8$ имеет параметры*

$$\mathbf{p}_0 = \begin{cases} \frac{1}{q}+\frac{q-1}{q^{n/2}+1} \text{ или } \frac{1}{q}+\frac{1}{q^{n/2}+1}, & \text{если } n \text{ четно,} \\ \frac{1}{q}+\frac{1}{q^{(n+1)/2}}, & \text{если } n \text{ нечетно,} \end{cases}$$
$$\mathbf{p}_1 \leqslant \frac{q^{n/2-1}+(q-1)}{q^{n/2}-(q-1)}$$

и реализует ϵ-совершенное шифрование, создавая не менее чем

$$\begin{array}{ll} \log_2\left(q^{n-1}-(q-1)q^{n/2}-1\right), & \text{если } n \text{ четно,} \\ \log_2\left(q^{n-1}-q^{(n-1)/2}\right), & \text{если } n \text{ нечетно,} \end{array}$$

битов секретности.

А-коды, указанные в конструкциях I–VIII, представляют собой, по сути дела, системы гаммирования (в абелевой группе) с имитовставкой. Первая координата сообщения представляет шифртекст, а вторая — имитовставку. В конструкциях I, II, III и VII ключи шифрования и аутентификации совпадают, в конструкциях IV, V, VI и VIII — различаются. Основной недостаток таких А-кодов состоит в большом размере ключа, который, по сути дела, представляет собой случайную равновероятную гамму. Далее речь пойдет о конструкциях А-кодов другой природы, в частности А-кодов, которые используют ключ небольшой длины.

3.2. А-коды с секретностью на основе конечных геометрий

Конструкция IX. А-код на основе аффинной плоскости.

Аффинная плоскость $AG(2,q)$ состоит из множества точек и множества прямых. *Прямую* можно определить как множество *точек* $(x,y) \in F_q \times F_q$, удовлетворяющих уравнению $ax+by=c$, где a,b,c — произвольные фиксированные элементы поля F_q и $(a,b) \neq (0,0)$. В качестве c достаточно взять 0 или 1. Множество точек аффинной плоскости и множество ее прямых (взятых в качестве блоков) образуют 2-$(q^2,q,1)$-схему. Поэтому, согласно теореме 9, существует экстремальный А-код с равномерным распределением $\mathcal{P}_S$. Покажем, как построить такой А-код с явно заданным правилом кодирования, реализующий ϵ-совершенное шифрование для достаточно малого ϵ.

Рассмотрим А-код $\mathcal{AC}_9$, для которого $\mathbf{S}=F_q$, $\mathbf{M}=F_q \times F_q$ и

$$\begin{aligned}\mathbf{K} = &\{(a,b,1) \,|\, a,b \in F_q,\, a \neq 0\} \cup \\ &\cup \{(1,b,0) | b \in F_q\} \cup \{(0,b,1) | b \in F_q,\, b \neq 0\} \cup \{(0,1,0)\}\,.\end{aligned}$$

Пусть множества элементов строк матрицы аутентификации $A(\mathcal{AC}_9)$ образованы прямыми плоскости $AG(2,q)$. Это означает, что правило кодирования e_κ, отвечающее ключу $\kappa=(a,b,c)$, имеет образ $e_\kappa(s)=B_\kappa$, где B_κ — прямая, определяемая уравнением $ax+by=c$. Правило кодирования $e_\kappa(s)$ определим формулой

$$e_\kappa(s) = \begin{cases} (s,0), & \text{если } \kappa=(0,1,0), \\ (0,s), & \text{если } \kappa=(1,0,0), \\ (s,b^{-1}), & \text{если } \kappa=(0,b,1), b\neq 0, \\ (a^{-1},s), & \text{если } \kappa=(a,0,1), a\neq 0, \\ \left(-(1+bs), s+b^{-1}\right), & \text{если } \kappa=(1,b,0), b\neq 0, \\ \left(a^{-1}(1-bs)-1, s+ab^{-1}\right), & \text{если } \kappa=(a,b,1), a,b\neq 0. \end{cases} \tag{9}$$

Формула (9) определяет инъективное отображение $e_\kappa\colon \mathbf{S} \to \mathbf{M}$, причем если $e_{(a,b,c)}(s) = (\alpha, \beta)$, то $\alpha a + \beta b = c$. Это означает, что формула (9) корректно задает правило кодирования.

Непосредственно проверяется следующее утверждение.

Теорема 45. *А-код $\mathcal{AC}_9$ реализует ϵ-совершенное шифрование для $\epsilon = \frac{(q-1)}{q(q+1)}$ и имеет параметры $\mathbf{p}_0 = 1/q$, $\mathbf{p}_1 = 1/(q+1)$.*

Отметим, что вид формулы (9) свидетельствует о том, что правило кодирования А-кода $\mathcal{AC}_9$ допускает эффективную реализацию. Сложность реализации определяется сложностью выполнения операций сложения и умножения, а также обращения элемента в поле F_q. При $q = 2^n$, например, для таких операций известен ряд эффективных алгоритмов.

Конструкция X. А-код на основе проективной геометрии.

Во многих публикациях утверждается, что первый безусловно стойкий А-код без секретности с равновероятными состояниями источника был представлен в [20]. Конструкция этого А-кода основана на проективной плоскости. В [61] построен оптимальный А-код с секретностью на основе проективной геометрии, который реализует совершенное шифрование.

Напомним, что *проективная геометрия* $PG(n,q)$ размерности n над F_q — это пространство всех векторов $(a_0, \ldots, a_n)$, $a_i \in F_q$. Вектор $\overline{0} = (0, \ldots, 0)$ образует пустое подпространство размерности (-1). Точка геометрии — подпространство размерности 0, а именно множество векторов bx, где $\overline{x} = (x_0, \ldots, x_n) \neq \overline{0}$, а b пробегает все элементы из F_q. Если векторы $\overline{y}_0, \ldots, \overline{y}_h$ линейно независимы, то

$$\{b_0\overline{y}_0 + \cdots + b_h\overline{y}_h,\ b_i \in F_q\}$$

— подпространство S_h размерности h. Подпространство S_{n-1} называется *гиперплоскостью*. Если $(c_0, \ldots, c_n) \neq \overline{0}$, то множество всех точек $(x_0, \ldots, x_n)$, удовлетворяющих уравнению $c_0x_0 + \cdots + c_nx_n = 0$, образует гиперплоскость; обратно, каждая гиперплоскость может быть определена таким образом, причем $(c_0, \ldots, c_n)$ и $(sc_0, \ldots, sc_n)$, $s \neq 0$, определяют одну и ту же гиперплоскость. Отсюда следует, что $PG(n,q)$ содержит $\left(q^{n+1} - 1\right)/(q-1)$ точек и столько же гиперплоскостей.

С $PG(n,q)$ ассоциируется блок-схема ([65]). Симметричная блок-схема называется *циклической*, если она имеет автоморфизм α, который переставляет элементы и блоки по полному циклу.

Теорема 46 (Зингера)**.** *Гиперплоскости проективной геометрии $PG(n,q)$, взятые в качестве блоков, и точки, взятые в качестве элементов, образуют циклическую симметричную блок-схему.*

Рассмотрим А-код $\mathcal{AC}_{10}$, множеством сообщений и ключей которого служит множество точек геометрии $PG(n,q)$, а множества $e_\kappa(s)$, $\kappa \in \mathbf{K}$, совпадают с множествами точек гиперплоскостей. Таким образом, правило кодирования e_κ, отвечающее ключу κ, определяется формулой $e_\kappa(\mathbf{S}) = B_\kappa$, где $\mathbf{S}$ — множество состояний источника, а B_κ — гиперплоскость, определяемая точкой κ.

Теорема 47 ([61]). *А-код $\mathcal{AC}_{10}$ имеет параметры*

$$|\mathbf{S}| = \frac{q^n-1}{q-1} = r, \quad |\mathbf{E}| = |\mathbf{M}| = \frac{q^{n+1}-1}{q-1} = v, \quad \mathbf{p}_0 = \frac{q^n-1}{q^{n+1}-1}, \quad \mathbf{p}_1 = \frac{q^{n-1}-1}{q^n-1}.$$

При подходящем выборе правила кодирования $\mathcal{AC}_{10}$ реализует совершенное шифрование.

Указанное в этой теореме правило кодирования можно задать в явном виде. Одно из них, основанное на свойстве цикличности блок-схемы, приведено в [61]. Для получения его явного выражения нужно заметить, что имеется взаимно однозначное соответствие между множеством степеней примитивного элемента θ поля $F_{q^{n+1}}$ и множеством ненулевых векторов $(a_0, \ldots, a_n)$, рассматриваемых как точки геометрии $PG(n,q)$. Отображение $\alpha\colon F_{q^{n+1}} \to F_{q^{n+1}}$ вида $\alpha\colon 0 \longmapsto 0$, $\alpha\colon \theta^i \longmapsto \theta^{i+1}$ можно рассматривать и как отображение

$$\alpha\colon (a_0, a_1, \ldots, a_n) \longmapsto (-a_0c_0, a_0 - a_nc_1, \ldots, a_{n-1} - a_nc_n)$$

множества точек в себя, где c_i — коэффициенты неприводимого над F_q многочлена $\mathcal{F}(x) = x^{n+1} + c_nx^n + \cdots + c_0$, корнем которого является θ. Это отображение биективно и переставляет точки по полному циклу. Поэтому можно полагать, что множества ключей и сообщений А-кода представлены в виде $\mathbf{K} = \mathbf{M} = \{\theta^0, \theta^1, \ldots, \theta^{v-1}\}$. Пусть $\mathbf{S} = \{s_0, s_1, \ldots, s_{r-1}\}$ и $B_0 = \{\theta^{\gamma_0}, \theta^{\gamma_1}, \ldots, \theta^{\gamma_{r-1}}\}$ — одна из гиперплоскостей. Тогда $B_j = (B_0)(\alpha^j) = \{\theta^{\gamma_0+j}, \theta^{\gamma_1+j}, \ldots, \theta^{\gamma_{r-1}+j}, \}$, $j = 1, \ldots, v-1$, — все блоки, связанные в один цикл автоморфизмом α. В итоге искомое правило кодирования можно записать в виде $e_{\theta^j}(s_i) = \theta^{(\gamma_i+j) \bmod v}$, $\quad i = 0, 1, \ldots, r-1$, $j = 0, 1, \ldots, v-1$.

4. А-коды с секретностью на основе А-кодов без секретности

Одним из методов построения А-кодов с секретностью является модификация правила кодирования А-кода без секретности. Идея метода для минимальных А-кодов приведена в [19], а ее развитие использовано в [60, 63] для построения А-кодов с секретностью на основе блоковых кодов. Суть метода состоит в следующем.

Будем модифицировать правило кодирования $e(s) = (s, \overline{e}(s))$ А-кода без секретности $\mathcal{AC}$ по формуле $e'(s) = (\varphi_e(s), \overline{e}(\varphi_e(s)))$, получая А-код с секретностью $\mathcal{BC}$ с теми же, что и у $\mathcal{AC}$, множествами состояний источника и сообщений. Здесь $\varphi_e \colon \mathbf{S} \to \mathbf{S}$ — биекция для каждого $e \in \mathbf{E}$. Нетрудно проверить, что при равномерных распределениях $\mathcal{P}_S, \mathcal{P}_E$ вероятности $\mathbf{p}_0, \mathbf{p}_1$ для А-кодов $\mathcal{AC}$ и $\mathcal{BC}$ одинаковы. Если $\mathcal{AC}$ гарантирует стойкую аутентификацию, то таковым же будет и $\mathcal{BC}$. Кроме того, удачный выбор подстановок φ_e позволяет добиться ϵ-совершенного шифрования. Таким образом, метод позволяет строить стойкие А-коды с секретностью с равновероятными состояниями источника. В [60] метод применяется к А-кодам без секретности на основе кодов Рида-Соломона, предложенных в [29].

Конструкция XI. Множествами состояний источника и правил кодирования А-кода $\mathcal{AC}$ служат соответственно $\mathbf{S} = \{s = (s_1, \ldots, s_r) \,|\, s_i \in F_q\}$, $r \in \mathbb{N}$, и $\mathbf{E} = \{e = (e_1, e_2) | e_i \in F_q\}$. Состояние источника $s \in \mathbf{S}$ определяет полином $s(x) = s_1 x + s_2 x^2 + \ldots + s_r x^r \in F_q[x]$. Для передачи состояния источника s отправитель создает сообщение m вида $m = (s, e_1 + s(e_2)) = (s_1, \ldots, s_r, e_1 + s(e_2))$.

Теорема 48 ([29]). *Для равномерных распределений $\mathcal{P}_S, \mathcal{P}_E$ А-код $\mathcal{AC}$ имеет параметры*

$$\mathbf{p}_0 = \frac{1}{q}, \quad \mathbf{p}_1 \leqslant \frac{r}{q}.$$

Пусть F_q — поле характеристики 2. Модифицируем $\mathcal{AC}$. Для этого пронумеруем элементы $e \in \mathbf{E}$ парами $(a, b) \in (F_q)^2$. Пусть $\mathcal{AC}_{11}$ — А-код с теми же, что и у $\mathcal{AC}$, множествами $\mathbf{S}, \mathbf{E}, \mathbf{M}$ и правилом кодирования, определенным формулой

$$e'_{(a,b)}(s_1, \ldots, s_r) = (u_1, \ldots, u_r, a + u_1 b + \ldots + u_r b^r),$$

где $u_i = s_i + c_i a + d_i b$, $c_i, d_i \in F_q$, $i = 1, \ldots, r$, — произвольные ненулевые константы, причем $c_i d_j \neq c_j d_i$ при любых $i, j \in \{1, \ldots, r\}$.

Теорема 49 ([60]). *А-код $\mathcal{AC}_{11}$ реализует ϵ-совершенное шифрование для равномерных распределений $\mathcal{P}_S, \mathcal{P}_E$, где $\epsilon < q^{-1}$, и имеет параметры*

$$\mathbf{p}_0 = \frac{1}{q}, \quad \mathbf{p}_1 \leqslant \frac{r}{q}.$$

Конструкция А-кода $\mathcal{AC}_{11}$ использует константы c_i, d_j, удовлетворяющие соотношениям $c_i d_j \neq c_j d_i$ при $i \neq j$. В случае когда $q = 2^n$, $r < n$, можно предложить следующий выбор c_i, d_j. Элемент поля F_{2^n} представляется многочленом $a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ с коэффициентами из F_2.

Пусть константа c_i представлена многочленом $f_i(x)=c_{n-1}^{(i)}x^{n-1}+\cdots+c_1^{(i)}x$, а d_i — многочленом $h_i(x)=c_{n-1}^{(i)}x^{n-1}+\cdots+c_1^{(i)}x+1$. Пусть $c_i\neq c_j$, тогда $f_i(x)\neq f_j(x)$. Произведение c_id_j представляется многочленом

$$f_i(x)g_j(x)=f_i(x)\left(f_j(x)+1\right),$$

а произведение c_jd_i — многочленом

$$f_j(x)g_i(x)=f_j(x)\left(f_i(x)+1\right).$$

Тогда, очевидно, $c_id_j\neq c_jd_i$. Выбирая произвольно различные двоичные векторы $\left(c_{n-1}^i,\ldots,c_1^i\right)$, получаем искомый набор констант.

Конструкция XII. Пусть $Q=2^{r+t}$, $q=2^r$, $2t\geqslant r$. А-код $\mathcal{AC}$ задан множествами

$$\mathbf{S}=(F_Q)^{2^t+1},\quad \mathbf{E}=F_Q\times F_Q\times F_q,\quad \mathbf{M}=(F_Q)^{2^t+1}\times F_q.$$

Каждое состояние источника $s=(s_{2^t},\ldots,s_1,s_0)$ определяет многочлен $s(x)\in F_Q[x]$ степени, не превосходящей 2^t, где $s(x)=s_{2^t}x^{2^t}+\ldots+s_1x+s_0$. Для правила кодирования $e=(e_1,e_2,e_3)$ и состояния источника $s=(s_{2^t},\ldots,s_1,s_0)$ $\mathcal{AC}$ составляет сообщение $m=(s,e_3+[s(e_1)\cdot e_2]_q)$, где $[c]_q$ означает приведение элемента $c\in F_Q$ по модулю q.

Теорема 50 ([29]). *Для равномерных распределений $\mathcal{P}_S,\mathcal{P}_E$ А-код $\mathcal{AC}$ имеет параметры*

$$\mathbf{p}_0=\frac{1}{2^r},\quad \mathbf{p}_1<\frac{1}{2^{r-1}}.$$

Модифицируем $\mathcal{AC}$. Для этого пронумеруем правила кодирования тройками $(a,b,c)\in F_Q\times F_Q\times F_q$ и построим А-код $\mathcal{AC}_{12}$ с теми же, что и у $\mathcal{AC}$, множествами $\mathbf{S},\mathbf{E},\mathbf{M}$ и правилом кодирования, определенным для $s\in\mathbf{S}$ и $e\in\mathbf{E}$ формулой

$$e'_{(a,b,c)}\left(s_{2^t},\ldots,s_0\right)=\left(u_{2^t},\ldots,u_0,c+\left[u_{2^t}a^{2^t}+\ldots+u_0\right]_q\right),$$

где $u_i=s_i+h_ia+g_ib$, $i=0,1,\ldots,2^t$, а ненулевые константы $h_i,g_i\in F_Q$, $i=0,1,\ldots,2^t$, удовлетворяют соотношениям $h_ig_j\neq h_jg_i$ при любых $i,j\in\left\{0,1,\ldots,2^t\right\}$.

Теорема 51 ([60]). *А-код $\mathcal{AC}_{12}$ обеспечивает ϵ-совершенное шифрование для равномерных распределений $\mathcal{P}_S,\mathcal{P}_E$, где $\epsilon=|2^{-(r+2t)}-2^{-(r+t)(2^t+1)}|$ и имеет параметры*

$$\mathbf{p}_0=\frac{1}{2^r},\quad \mathbf{p}_1<\frac{1}{2^{r-1}}.$$

Проиллюстрируем возможности A-кода $\mathcal{AC}_{12}$. Пусть $t = 32$, $r = 64$. Тогда при использовании 256-битового ключа $\mathcal{AC}_{12}$ обеспечивает $\left(2^{-128}\right)$-совершенное шифрование строк длины, не превосходящей $(64 + 32)\left(2^{31} + 1\right)$ битов, и их аутентификацию с уровнем стойкости, определяемым параметрами $\mathbf{p}_0 = 1/2^{64}$ и $\mathbf{p}_1 < 1/2^{63}$.

В [63] показано, что A-коды $\mathcal{AC}_{11}$ и $\mathcal{AC}_{12}$ остаются достаточно стойкими и в случае когда распределение $\mathcal{P}_S$ не является равномерным.

Теорема 52. *Пусть для A-кодов $\mathcal{AC}_{11}$ и $\mathcal{AC}_{12}$ распределение $\mathcal{P}_E$ — равномерное, а $\mathcal{P}_S$ — любое такое распределение, что для некоторых действительных чисел α, β, δ, удовлетворяющих неравенствам $0 < \alpha, \beta < 1 \leqslant \delta$, выполняются условия $\alpha \leqslant p_S(s) \leqslant \beta$, $\beta/\alpha \leqslant \delta$, для каждого $s \in \mathbf{S}$. Тогда A-код $\mathcal{AC}_{11}$ обеспечивает ϵ-совершенное шифрование для $\epsilon < \delta q^{-1}$, а A-код $\mathcal{AC}_{12}$ — ϵ'-совершенное шифрование, где $\epsilon' < \delta\, 2^{-(r+2t)}$. A-код $\mathcal{AC}_{11}$ имеет параметры $\mathbf{p}_0 = 1/q$, $\mathbf{p}_1 \leqslant k\delta/q$, A-код $\mathcal{AC}_{12}$ имеет параметры $\mathbf{p}_0 = 1/2^r$, $\mathbf{p}_1 < \delta/2^{r-1}$.*

Метод модификации можно применять и к A-кодам без секретности на основе универсальных семейств хеш-функций (см. [9, 49 – 53]).

Речь идет о функциях $h\colon \mathbf{S} \to \mathbf{A}$, где $\mathbf{S}$ и $\mathbf{A}$ — конечные множества, $|\mathbf{S}| = r$, $|\mathbf{A}| = n$, $n < r$, и их свойстве иметь коллизии, под которым понимается совпадение $h(s_1)$ и $h(s_2)$ для различных элементов s_1, s_2 из $\mathbf{S}$. Такие функции получили название *хеш-функций*. Если $H = \{h\colon \mathbf{S} \to \mathbf{A}\}$ — семейство хеш-функций, $|H| = b$, то H называют $(b; r, n)$-*семейством*.

$(b; r, n)$-семейство H хеш-функций называют *строго универсальным* (SU-*семейством*), если для любых $s_1, s_2 \in \mathbf{S}$, $s_1 \neq s_2$, и $a_1, a_2 \in \mathbf{A}$ справедливо равенство

$$|\{h \in H \,|\, h(s_i) = a_i,\ i = 1, 2\}| = b/n^2,$$

и ϵ-*строго-универсальным* (ϵSU-*семейством*), если для любых $s \in \mathbf{S}$, $a \in \mathbf{A}$

$$|\{h \in H \,|\, h(s) = a\}| = b/n$$

и для любых $s_1, s_2 \in \mathbf{S}$, $s_1 \neq s_2$, и $a_1, a_2 \in \mathbf{A}$

$$|\{h \in H \,|\, h(s_i) = a_i,\, i = 1, 2\}| \leqslant \epsilon \cdot b/n.$$

Условия последнего определения равносильны тому, что при случайном и равновероятном выборе $h \in H$ значение $h(s)$ распределено равномерно в $\mathbf{A}$ и что невозможно угадать значение $h(s')$ с вероятностью, большей ϵ, даже если известно значение $h(s)$. Заметим, что ϵ-строго-универсальное $(b; r, n)$-семейство H при $\epsilon = 1/n$ становится строго-универсальным.

Роль универсальных семейств хеш-функций в теории кодов аутентификации проясняет следующее утверждение.

Теорема 53 ([57]). *Если существует ϵSU-$(b; r, n)$-семейство H хеш-функций, то существует и А-код с r состояниями источника, n метками* [6], *b правилами кодирования, реализующий для равномерных распределений $\mathcal{P}_S$, $\mathcal{P}_E$ значения $\mathbf{p}_0 = 1/n$, $\mathbf{p}_1 \leqslant \epsilon$.*

Матрицей аутентификации А-кода в теореме 53 является табличное задание хеш-семейства H. Это утверждение позволяет строить стойкие А-коды без секретности, которые после модификации могут стать стойкими А-кодами с секретностью. Приведем пример.

Конструкция XIII. Пусть α, β, γ — натуральные числа, $\alpha \geqslant \beta$ и $\varphi\colon (F_q)^\alpha \to (F_q)^\beta$ — сюръективное линейное отображение. Положим $\mathbf{A} = (F_q)^\beta$,

$$\mathbf{S} = \{p(x) \in (F_q)^\alpha [x] \mid \deg p(x) \leqslant \gamma,\ p(0) = 0\}$$

и рассмотрим семейство

$$H = \left\{ h_{u,v}\colon \mathbf{S} \to \mathbf{A} \mid u \in (F_q)^\alpha,\ v \in (F_q)^\beta \right\},$$

где $h_{u,v}(p(x)) = \varphi(p(u)) + v$. Известно [6], что H образует ϵSU-$(b; r, n)$-семейство хеш-функций с $\epsilon = \gamma/q^\beta$ и $(b; r, n) = (q^{\alpha+\beta}; q^{\alpha\gamma}, q^\beta)$. Согласно теореме 52 семейство H определяет А-код $\mathcal{AC}$ с параметрами $\mathbf{p}_0 = q^{-\beta}$, $\mathbf{p}_1 \leqslant \gamma q^{-\beta}$, для которого множеством сообщений является $\mathbf{M} = \mathbf{S} \times \mathbf{A}$, множеством ключей — $\mathbf{K} = (F_q)^\alpha \times (F_q)^\beta$.

Будем записывать состояние источника в виде многочлена $s = s_\gamma x^\gamma + \cdots + s_1 x$ или в виде строки коэффициентов $(s_\gamma, \ldots, s_1)$. Для $\kappa = (u, v)$, $u \in (F_q)^\alpha$, $v \in (F_q)^\beta$, правило кодирования e_κ А-кода $\mathcal{AC}$ задается формулой

$$e_{(u,v)}(s_\gamma, \ldots, s_1) = ((s_\gamma, \ldots, s_1), \varphi(s_\gamma u^\gamma + \cdots + s_1 u) + v).$$

Модифицируем правило кодирования следующим образом. Положим

$$e'_{(u,v)}(s_\gamma, \ldots, s_1) = \\ = \big((s_\gamma + c_\gamma u, \ldots, s_1 + c_1 u), \varphi((s_\gamma + c_\gamma u)u^\gamma + \cdots + (s_1 + c_1 u)u) + v\big),$$

где $c_1, \ldots, c_\gamma$ — ненулевые константы. Пусть $\mathcal{AC}_{13}$ — А-код, определенный этой формулой. Несложно проверить, что этот А-код обладает следующими свойствами.

[6] Метка — синоним имитовставки.

Теорема 54. *А-код* $\mathcal{AC}_{13}$ *имеет параметры* $\mathbf{p}_0 = 1/q^\beta$, $\mathbf{p}_1 \leqslant \gamma/q^\beta$ *и обеспечивает* $(1/q^\alpha)$*-совершенное шифрование.*

Конструкция XIV. Пусть q — степень простого числа p, D, m — натуральные числа и Tr — функция след из F_{q^m} в F_q. Пусть

$$\mathbf{S} = \left\{ s(x) \in F_{q^m}[x] \,|\, s(x) = s_D x^D + \cdots + s_1 x + s_0;\ s_i = 0, \text{ если } p \text{ делит } i \right\}$$

и $\mathbf{A} = F_q$. Тогда $H = \{h_{u,v} \colon \mathbf{S} \to \mathbf{A} \,|\, u \in F_{q^m},\ v \in F_q\}$, где $h_{u,v}(s(x)) = \mathrm{Tr}\,(s(u)) + v$.

Известно [22], что H образует ϵSU-$(b; r, n)$- семейство хеш-функций с $\epsilon = 1/q + (D-1)/\sqrt{q^m}$ и $(b; r, n) = \left(q^{m+1}; q^{m(D-\lfloor D/p \rfloor)}, q\right)$. Оно определяет А-код $\mathcal{AC}$ с параметрами $\mathbf{p}_0 = q^{-1}$, $\mathbf{p}_1 \leqslant 1/q + (D-1)/\sqrt{q^m}$, для которого множеством сообщений служит $\mathbf{M} = \mathbf{S} \times \mathbf{A}$, множеством ключей — $\mathbf{K} = F_{q^m} \times F_q$, и правилом кодирования $e_{u,v}(s(x)) = (s(x),\ \mathrm{Tr}\,(s(u)) + v)$.

Модифицируем правило кодирования. Положим

$$e_{u,v}\left((s_D, \ldots, s_0)\right) = \left(s_D + c_D u, \ldots, s_0 + c_0 u,\ \mathrm{Tr}\,(s'(u) + v)\right),$$

где $s'(u) = s'_D u^D + \cdots + s'_0$, $s'_i = s_i + c_i u$, $i = 0, \ldots, D$, а c_i — ненулевые константы. Пусть $\mathcal{AC}_{14}$ — А-код, определенный этой формулой. Несложно проверить, что $\mathcal{AC}_{14}$ обладает следующими свойствами.

Теорема 55. *А-код* $\mathcal{AC}_{14}$ *имеет параметры*

$$\mathbf{p}_0 = \frac{1}{q}, \quad \mathbf{p}_1 < \frac{1}{q} + \frac{D-1}{\sqrt{q^m}}$$

и реализует ϵ*-совершенное шифрование для* $\epsilon = q^{-r} - q^{-r(D-\lfloor D/p \rfloor)}$.

Подобные результаты можно получить, беря за основу другие ϵSU-семейства хеш-функций. Некоторые из таких семейств (см. [5, 3, 31, 39, 7, 27, 6, 36, 18, 32]) допускают эффективную реализацию. Более полная библиография по тематике А-кодов приведена в [54, 59].

5. АЕ-криптосистемы как коды аутентификации с секретностью

В отличие от рассмотренных выше А-кодов алгебраической или комбинаторной природы, АЕ-криптосистему как код аутентификации с секретностью выделяет то, что функцию шифрования выполняет шифрсистема, как правило, блочная. Функция аутентификации реализуется путем шифрования метки аутентификации.

Фактически AE-криптосистема реализует режим шифрования с аутентификацией и обеспечивает функции шифрования и аутентификации на общем секретном ключе. При этом допускается использование одного ключа для шифрования многих соообщений. Для оценки стойкости AE-криптосистем подход, который применялся в предыдущих разделах, не применим, поскольку эта задача так или иначе сводится к задаче оценки стойкости базовой шифрсистемы, в качестве которой используется, как правило, стандарт шифрования. Типичный подход к оценке стойкости одной из AE-криптосистем приведен, например, в [62]. Этот подход основан на атаках различения и позволяет получить оценку стойкости, зависящую лишь от затрат атакующего. AE-криптосистемам посвящен ряд обзоров ([40, 55, 8, 35, 37, 30, 1]), аналитических статей и рекомендаций ([2, 16, 17, 38, 25, 11, 26, 33, 4]). Вопросы синтеза и анализа AE-криптосистем требуют отдельного рассмотрения.

6. Заключение

A-коды с секретностью — это класс криптосистем, обеспечивающих конфиденциальность и аутентичность информации. A-коды, основанные на комбинаторных или алгебраических структурах, являются, как правило, криптосистемами с одноразовым ключом. Это означает, что для защиты каждого сообщения требуется свой секретный ключ. С одной стороны, это обстоятельство является недостатком криптосистемы. Но, с другой стороны, такие A-коды могут иметь достаточно простую конструкцию и высокую скорость вычислений. Еще одно их достоинство состоит в том, что они являются криптосистемами с доказуемой стойкостью. Некоторые из них обеспечивают ϵ-совершенное шифрование и δ-стойкость к активным атакам, что гарантирует требуемый уровень стойкости к атакам противника с неограниченными вычислительными возможностями. A-коды комбинаторной или алгебраической природы могут задаваться как таблично, так и явным указанием правила кодирования. Естественно, второй способ задания более практичен, поскольку позволяет оценить возможность и эффективность реализации A-кода. С этой точки зрения представляют интерес A-коды, приведенные в разделе 4 данного обзора. Они позволяют надежно защищать данные большого объема, используя короткий ключ, и допускают эффективную реализацию. Многие теоретические оценки стойкости A-кодов получены при условии, что их состояния источника (входная информация) равновероятны. Это условие можно считать допустимым, если предварительно подвергать информацию преобразованию, уменьшаемому избыточность. Вместе с тем для некоторых A-кодов, например представленных конструкциями XI и XII, можно получить оценку стойкости практически для любого входа (теорема 52). Интересен вопрос о возможности и целесообразности использования таких A-кодов в конкретных приложениях.

Ко второму классу A-кодов с секретностью можно отнести AE-криптосистемы, совмещающие шифрсистему и систему аутентификации. Для оценки их стойкости используется методика доказуемой стойкости, основанная на теоретико-сложностном подходе. Конструкции таких A-кодов сложнее, но допускают многократное использование ключа. В настоящее время имеются международные и государственные стандарты AE-криптосистем. С 2012 года проводится конкурс под названием CAESAR[7], цель которого — разработка AE-криптосистемы, превышающей по эффективности и стойкости существующие системы. Итоги конкурса должны быть объявлены в конце 2017 года.

Список литературы

[1] Abed F., Forler C., Lucks S., *General overview of the first-round CAESAR candidates for authenticated encryption*, Cryptology ePrint Archive, 2014/792, 20 pp.

[2] Bellare M., Namprempre C., "Authenitcated encryption: relations among notions and analysis of the composition paradigm". In: "*ASIACRYPT 2000*", Lect. Notes Comput. Sci., **1976**, 2000, 26 pp.

[3] Bernstein D. J., "The Poy1305-AES message authentication code". In: "*FSE 2005*", Lect. Notes Comput. Sci, **3494**, 2005, 164–180.

[4] Bernstein D. J., *CAESAR call for submissions, final*, 2014, http: //competitions.cr.yp.to/ caesar-call.html.

[5] Bierbrauer J., Johansson T., Kabatianskii G., Smeets B., "On families of hash functions via geometric codes and concatenation". In: "*CRYPTO 93*", Lect. Notes Comput. Sci., **773**, 1994, 331–342.

[6] Bierbrauer J., "Universal hashing and geometric codes", *Des., Codes and Cryptogr.*, **11**:3 (1997), 207–221.

[7] Bierbrauer J., "Authentication via algebraic-geometric codes", *Rend. Circ. Mat. Palermo (2) Suppl.*, № 51 (1998), 139–152.

[8] Black J., *Authenticated Encryption*, August 19. 2004, 12 pp., https ://www.cs.colorado.edu/ ~jrblack/papers/ae.pdf.

[9] Carter L., Wegman M., "Universal hash functions", *J. Comput. Syst. Sci.*, № 18 (1979), 143–154.

[10] Casse L. R. A., Martin K. M., Wild P. R., "Bound and characterizations of authentication/secrecy schemes", *Des., Codes and Cryptogr.*, **13**:2 (1998), 107–129.

[11] Chen H., "Authenticated encryption modes of block ciphers, their security and implementation properties. Seminararbeit" (2009), 20 pp., https://www.emsec.rub.de/media/ crypto/attachments/files/2011/03/chen.pdf.

[12] Colbourn C. J., Dinitz J. H. (eds.), *Handbook of Combinatorial Designs. 2nd ed.*, Boca Raton: CRC Press, 2006, 1010 pp.

[13] De Soete M., "Some constructions for authentication — secrecy codes". In: "*EUROCRYPT 88*", Lect. Notes Comput. Sci., **330**, 1988, 57–75.

[14] Ding C., Salomaa A., Sole P., Tian X., "Three constructions of authentication secrecy codes", *J. Pure and Applied Algebra*, **196** (2005), 149–168.

[15] Ding C., Tian X., "Three constructions of authentication codes with perfect secrecy", *Des., Codes and Cryptogr.*, **33**:3 (2004), 227–239.

[16] Dworkin M., “NIST Recommendation for block cipher modes of operation: the CCM mode for authentication and confidentiality”, NIST Special Pub. 800-38C, 2004.

[17] Dworkin M., “NIST Recommendation for block cipher modes of operation: Galois/Counter Mode (GCM) and GMAC”, NIST Special Pub. 800-38D, 2007.

[18] Etzel M., Patel S., Ramzan Z., “Square hash: fast message authentication via optimized hash functions”. In: “*CRYPTO 99*”, Lect. Notes Comput. Sci., **1666**, 1999, 234–251.

[19] Fenga R., Hub L., Kwakc J. H., “Authentication codes and bipartite graphs”, *European J. Combinatorics*, № 29 (2008), 1473–1482.

[20] Gilbert E. N., MacWilliams F. J., Sloane J. A., “Codes which detect deception”, *The Bell System Technical J.*, **53** (1974), 405–424.

[21] Godlewsky P., Mitchell C., “Key-minimal cryptosystems for unconditional secrecy”, *J. Cryptology*, **3**:1 (1990), 1–25.

[22] Helleseth T., Johansson T., “Universal hash functions from exponential sums over finite feekds and Galois rings”. In: “*CRYPTO 96*”, Lect. Notes Comput. Sci., **1109**, 1996, 31–44.

[23] Huber M., “Authentication and secrecy codes for equiprobable source probability distributions”. In: “*Proc. IEEE Int. Symp. Inf. Theor. (ISIT)*”, 2009, 1105–1109.

[24] Huber M., “Constructing optimal authentication codes with perfect multifold secrecy”. In: “*Int. Zurich Seminar on Communic. (IZS), ETH Zurich*”, 2010, 86–89.

[25] Hwang M. S., Liu C. Y., “Authenticated encryption schemes: current status and key issues”, *Int. J. Network Secur.*, **1**:2 (2005), 54–66.

[26] “International Standard ISO/IEC 19772. First edition 2009-02-15”, Information technology Security techniques Authenticated encryption (2009), 7 pp.

[27] Johansson T., “Bucket hashing with a small key size”. In: “*EUROCRYPT 97*”, Lect. Notes Comput. Sci., **1233**, 1997, 149–162.

[28] Jungnickel D., “On automorphism groups of divisible designs”, *Canad. J. Math.*, **XXXIV**:2 (1982), 257–297.

[29] Kabatianskii G. A., Johansson T., Smeets B., “On the cardinality of systematic A-codes via error correcting codes”, *IEEE Trans. Inf. Theory*, **IT-42**:2 (1996), 566–578.

[30] Kim H., Kim K., “Who can survive in CAESAR competition at round-zero?”. In: “*The 31th Symp. Cryptogr. Inf. Secur.*”, 2014, 7 pp.

[31] Krawczyk H., “New hash functions for message authentication”. In: “*EUROCRYPT 95*”, Lect. Notes Comput. Sci., **921**, 1995, 301–310.

[32] Krovetz T., Rogaway P., “Fast universal hashing with small keys and no preprocessing: the PolyR construction”. In: “*ICICS 2000*”, Lect. Notes Comput. Sci., **2015**, 73–89.

[33] Krovetz T., Rogaway P., “The software performance of authenticated-encryption modes”, Lect. Notes Comput. Sci., **6733**, 2011, 306–327, https:/web.cs.ucdavis.edu/ rogaway/papers/ae.pdf.

[34] Massey J. L., “Cryptography — a selective survey”. In: “*Digital Communications*”, North-Holland, 1986, 3–21.

[35] Minematsu K., “A Study of Block Cipher Modes for Encryption and Authentication” (2008), 85, https:/dspace.wul.waseda.ac.jp/dspace/ bitstream/2065/28755/3/Honbun-4809.pdf.

[36] Nevlsteen W., Preneel B., “Software performance of universal hash functions”. In: “*EUROCRYPT 99*”, Lect. Notes Comput. Sci., **1592**, 1999, 24–41.

[37] Oszywa W., Gliwa R., *Designing authenticated encryption modes of operation*, Zegrze, Poland: Military Communication Institute, 05-130, 2010, 12 pp.

[38] Parelkar M. M., *Authenticated Encryption in Hardware*, Master of Science thesisto the Graduate Faculty of George Mason University in Partial Filfullment of the the Requirements for he Degree of Master of Science Electrical and Computer Engineering: George Mason University, 2005, 143 pp.

[39] Rogaway P., "Bucket hashing and its application to fast message authentication". In: "*CRYPTO 95*", Lect. Notes Comput. Sci., **963**, 1995, 29–42.

[40] Rogaway P., "Authenticated-encryption with associated-data". In: "*ACM Conf. Comput. Commun. Secur.*": ACM Press, 2002, 98–107.

[41] Rees R. S., Stinson D. R., "Combinatorial characterizations of authentication codes", *Des., Codes and Cryptogr.*, **7**:3 (1996), 239–259.

[42] Safavi-Naini R., Tombak L., "Optimal authentication systems". In: "*EUROCRYPT 93*", Lect. Notes Comput. Sci., **765**, 1994, 12–27.

[43] Saygi Z., *Constructions of Authentication Codes*, Graduate school thesis: Middle Technical University, 2007, 74 pp.

[44] Sgarro A., "An introduction to the theory of unconditional secrecy and authentication". In: "*Geometries, Codes and Cryptography. CISM Courses and Lectures*": Springer-Verlag, 1990, 131–160.

[45] Simmons G. J., "Authentication theory/coding theory". In: "*CRYPTO 84*", Lect. Notes Comput. Sci., **196**, 1985, 411–432.

[46] Song Y., Kurosawa K., Tsujii S., "Authentication codes based on association schemes", *IEICE Trans. Fundamentals*, **E79-A** (1996), 126–130.

[47] Stinson D. R., "A construction for authentication secrecy codes from certain combinatorial designs". In: "*CRYPTO 87*", Lect. Notes Comput. Sci., **293**, 1988, 355–366.

[48] Stinson D. R., "The combinatorics of authentication and secrecy codes", *J. Cryptology*, **2**:1 (1990), 23–49.

[49] Stinson D. R., "Universal hashing and authentication codes". In: "*CRYPTO 91*", Lect. Notes Comput. Sci., **576**, 1992, 74–85.

[50] Stinson D. R., "Combinatorial characterization of authentication codes", *Des., Codes and Cryptogr.*, **2**:2 (1992), 175–187.

[51] Stinson D. R., "Combinatorial techniques for universal hashing", *J. Comput. Syst. Sci.*, **48**:2 (1994), 337–346.

[52] Stinson D. R., "On the connections between universal hashing, combinatorial designs and error-correcting codes", *Congressus Numerantium*, **114** (1996), 7–27.

[53] Stinson D. R., "Universal hash families and the leftover hash lemma? And applications to cryptography and computing", *J. Comb. Math. Comb. Comput.*, № 1 (2001), 3–32.

[54] Stinson D. R., Wei R., "Bibliography on authentication codes" (1998), 11 pp., http://cacr.uwaterloo.ca/ dstinson/acbib.html.

[55] Svenda P., "Basic comparison of modes for authenticated-encryption (IAPM, XCBC, OCB, CCM, EAX, CWC, GCM, PCFB, CS)" (2004), 16 pp., https://www.fi.muni.cz/-xsvenda/.../ AE–comparison-ipics04.pdf.

[56] Trung Van T., "On the construction of authentication and secrecy codes", *Des., Codes and Cryptogr.*, **5**:3 (1995), 269–280.

[57] Wegman M., Carter L., “New hash functions and their use in authentication and set equality”, *J. Comput. Syst. Sci.*, **22**:3 (1981), 265–279.

[58] Зубов А. Ю., *Совершенные шифры*, М.: Гелиос АРВ, 2003, 160 с.

[59] Зубов А. Ю., *Математика кодов аутентификации*, М.: Гелиос АРВ, 2007, 480 с.

[60] Зубов А. Ю., “Почти совершенные шифры и коды аутентификации”, *Прикладная дискретная математика*, № 4 (14) (2011), 28–33.

[61] Зубов А. Ю., “Код аутентификации с секретностью на основе проективной геометрии”, *Прикладная дискретная математика*, № 2 (20) (2013), 39–49.

[62] Зубов А. Ю., “Об оценке стойкости AEAD-криптосистемы типа GCM”, *Прикладная дискретная математика*, № 2 (32) (2016), 49–62.

[63] Зубов А. Ю., “О понятии ϵ-совершенного шифра”, *Прикладная дискретная математика*, № 3 (33) (2016), 45–52.

[64] Коновалова С. С., “Исследование линейных совершенных шифров и их современных аналогов”, В сб.: РусКрипто 2009, с. 20.

[65] Холл М., *Комбинаторика*, М.: Мир, 1970, 424 с.