УДК 004.056.53 DOI 10.18522/2311-3103-2022-4-40-50

Д.В. Загуменнов, В.В. Мкртичян

ЭКСПЕРИМЕНТАЛЬНОЕ ИССЛЕДОВАНИЕ НАДЕЖНОСТИ СХЕМ ШИРОКОВЕЩАТЕЛЬНОГО ШИФРОВАНИЯ С АЛГЕБРОГЕОМЕТРИЧЕСКИМИ КОДАМИ МАЛОЙ МОЩНОСТИ*

Рассматриваются схемы специального широковещательного шифрования – криптографический протокол, решающий задачу распространения цифровой продукции среди авторизованных пользователей. Широковещательное шифрование находит применение в различных областях, например, защита данных в компьютерных сетях, кабельное и спутниковое цифровое телевидение, распределенное хранение информации. В схемах широковещательного шифрования данные распространяются свободно, но в зашифрованном виде, и каждому легальному пользователю выдается уникальный набор ключей для их расшифрования. В схемах специального широковещательного шифрования возможны атаки со стороны коалиций злоумышленников из числа авторизованных пользователей, пытающихся создать "пиратские" ключи и получить несанкционированный доступ к распространяемым данным. Эффективный способ борьбы с такими атаками найден в использовании линейных кодов, обладающих специальными идентифицирующими свойствами, в частности, так называемыми "frameproof" (FP) и "traceability" (TA) свойствами. Ранее получены теоретические границы мощности коалиции злоумышленников, в пределах которой применимы схемы, основанные на использовании идентифицирующих алгеброгеометрических кодов. В работе представлена информационная система для проведения экспериментальных исследований надежности схем, основанных на использовании идентифицирующих алгеброгеометрических кодов малой мощности, в частности, для вычисления вероятностей нарушения идентифицирующих свойств таких кодов, в том числе при превышении известных теоретических границ. В качестве примера использования представленной системы приведены и проанализированы результаты вычислительного эксперимента для двух алгеброгеометрических кодов. В заключение рассмотрены открытые вопросы, представляющие интерес для дальнейших исследований, в частности, возможность расширения экспериментальных исследований до кодов произвольной мощности.

Математические методы защиты информации; широковещательное шифрование; алгеброгеометрические коды; идентифицирующие коды.

D.V. Zagumennov, V.V. Mkrtichyan

EXPERIMENTAL STUDY OF THE RELIABILITY OF BROADCAST ENCRYPTION SCHEMES WITH LOW-POWER ALGEBRAIC GEOMETRIC CODES

Broadcast encryption is a data distribution protocol that solve the problem of distributing digital products to authorized users and prevent unauthorized parties from accessing the data. It is widely used in computer networks data protection, digital television and distributed storage. In broadcast encryption schemes, data is distributed freely, but in encrypted form, and each legal user is given a unique set of keys to decrypt it. However, broadcast encryption schemes are vulnerable to attacks from coalitions of malicious users from among authorized users who are trying to create "pirated" keys and gain unauthorized access to distributed data. Attacks of this kind can be handled in broadcast encryption schemes by using error-correction codes that have special identifying properties, in particular, frameproof (FP) and traceability (TA) properties. Previously, theoretical limits were obtained for the power of a coalition of attackers, within which schemes based on identifying algebraic geometric codes are applicable. The paper presents an information system for conducting experimental studies of schemes reliability based on low-power identifying algebraic geometric codes, in

* Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 20-31-90098.

particular, for calculating identifying properties violation probabilities, including when exceeding known theoretical limits. As an example of using the presented system, the results of a computational experiment for two algebraic geometric codes are presented and analyzed. In conclusion, some open questions are considered that are of interest for further research, in particular, the possibility of expanding experimental studies to codes of arbitrary power.

Copy protection; broadcast encryption; algebraic geometric codes; identifying codes.

Введение. В работе рассматриваются схемы защиты легально тиражируемой цифровой продукции от несанкционированного копирования [1–5], называемые схемами специального широковещательного шифрования (ССШШ). В ССШШ распространитель тиражирует данные свободно, но в зашифрованном виде, и каждому легальному пользователю для расшифрования выдаёт уникальный набор ключей и векторов из некоторого линейного кода. Далее пользователи применяют эту информацию при выполнении легального доступа к данным. В случае обнаружения нелегального использования вектора и ключа их владелец может быть идентифицирован контролёром. В ССШШ допускаются атаки следующего вида: некоторые недобросовестные легальные пользователи могут объединяться в коалиции злоумышленников мощности $c \geq 2$ с целью создания пиратских вектора и ключа, которые можно использовать для выполнения нелегального доступа к данным. Исследования в этой области продолжены в других работах, например в [6–10], и в настоящее время представляются актуальными в связи с ростом популярности широковещательных служб и увеличения многообразия атак.

Для борьбы с коалиционными атаками в [3] предложен метод обнаружения членов коалиций, основанный на использовании линейных кодов, обладающих так называемыми идентифицирующими свойствами, например, свойствами c-FP и c-TA.

Интересной представляется задача исследования применимости алгеброгеометрических кодов [11–13] в ССШШ. Ранее проведены теоретические исследования наличия идентифицирующих свойств у алгеброгеометрических кодов [14–15], получены теоретические границы мощности коалиций злоумышленников, в пределах которых некоторые классы алгеброгеометрических кодов обладают c-FP и c-TA свойствами.

Актуальной представляется задача экспериментального исследования надежности ССШШ в случае, когда мощность атакующей коалиции превышает теоретические границы: интересно, как часто нарушаются идентифицирующие свойства у алгеброгеометрических кодов в данных условиях. Для проведения такого исследования нужно, во-первых, формализовать алгеброгеометрический код, представить его в удобном для необходимых вычислений виде: в работе коды представляются в виде порождающей и проверочной матриц кода, конструируемых с помощью пакета компьютерной алгебры Magma. Во-вторых, необходимо спланировать вычислительный эксперимент и написать программу, которая его реализует: в ходе работы такая программа разработана, но алгоритм, используемый в ней, имеет экспоненциальную сложность, что накладывает вычислительные ограничения на мощность рассматриваемых кодов. С целью иллюстрации работы алгоритма выбраны два алгеброгеометрических кода, для которых проведены соответствующие эксперименты. Результаты этих экспериментов и их анализ представлены в заключительном разделе.

Идентифицирующие коды. Пусть $F = F_q$ – конечное поле, и C – линейное подпространство размерности k в F^n. Подпространство C называют линейным кодом, k называют размерностью кода, а n – длиной кода. Также рассмотрим в F^n метрику $\rho(x, y) = |\{\, 1 \leq i \leq n : x_i \neq y_i \,\}|$, то есть число координат, в которых вектора не совпадают. Эта метрика называется расстоянием

Хемминга. Минимальное из значений $\rho(x,y)$ для всех различных векторов x и y из кода C называется минимальным кодовым расстоянием кода и обозначается как d. Рассмотрим также множество $I(x,y)$ координат, совпадающих в векторах x и y, ясно, что $|I(x,y)| = n - \rho(x,y)$.

Коалицией кода C мощностью $c \in \mathbb{N} \setminus \{1\}$ называется набор из c различных кодовых векторов, множество всех коалиций кода C мощностью не более c обозначим как $coal_c(C)$. Множеством потомков коалиции C_0 называется следующее множество:

$$desc(C_0) = \{ (y_1,\dots,y_n) \in F^n : \exists\, 1 \le i \le c, \exists\, 1 \le j \le n, y_i = u_{i,j} \}.$$

Код C называется c-FP кодом ([3], определение 1.1.1), если:

$$\forall C_0 \in coal_c(C)\ \forall z \in C \setminus C_0\ z \notin desc(C_0).$$

Множеством FP-компрометации кода C называется множество таких значений c, для которых код C не является c-FP кодом. Очевидно, что это множество является целочисленным лучом, началом которого является некоторое натуральное число $R_{FP}(C)$. Это число называется рубежом FP-компрометации для кода C.

Код C называется c-TA кодом ([3], определение 1.1.4), если:

$$\forall C_0 \in coal_c(C)\ \forall v \in C \setminus C_0\ \forall y \in desc(C_0)\ \exists \omega \in C_0 \colon \rho(\omega,y) < \rho(v,y).$$

Множеством TA-компрометации кода C называется множество таких значений c, для которых код C не является c-TA кодом. Аналогично, как и для свойства FP, что множество TA-компрометации является целочисленным лучом, началом которого является некоторое натуральное число $R_{TA}(C)$, называемое рубежом TA-компрометации для кода C.

Алгеброгеометрические коды. Пусть $F^{hom}[X,Y,Z]$ – множество однородных многочленов от трех переменных X,Y,Z над полем F. Пусть $G \in F^{hom}[X,Y,Z]$ – неприводим над полем и всеми его расширениями. Пусть $\chi = \chi(G,F)$ – проективная кривая в двумерном проективном пространстве $P^2(F)$, заданная нулями G, т.е. точки двумерного пространства $(a\colon b\colon c)$, такие, что $G(a,b,c) = 0$.

Рассмотрим теперь поле рациональных функций над кривой χ и обозначим его $F(\chi)$. Это поле состоит из рациональных функций, числители и знаменатели которых являются многочленами из $F^{hom}[X,Y,Z]$ одной и той же степени, при этом две функции считаются равными, если они отличаются на аддитивную константу, делящуюся на многочлен G ([12], 2.5.4). Согласно [12], 2.5.2, для каждой функции $H \in F(\chi)$ в каждой точке M кривой специальным образом задают целочисленный параметр, называемый порядком функции в точке и обозначаемый как $ord_M(H)$. В самом простом случае это значение равно разности кратности точки M как корня числителе и кратности точки M как корня знаменателя.

Дивизором D на кривой называют формальную сумму вида: $D = \sum_{M \in \chi} a_M M, a_M \in Z$. Сумма всех таких a_M называются степенью дивизора и обозначается $deg(D)$, а множество точек M, для которых $a_M \neq 0$, называется носителем дивизора и обозначается как $supp(D)$. Дивизор называют эффективным и пишут $D \ge 0$, если все a_M неотрицательны. Таким образом, на множестве дивизоров вводится частичный порядок. Для каждой рациональной функции $H \in F(\chi)$ можно задать собственный дивизор: $(H) = \sum_{M \in \chi} ord_M(H)M$. Также дивизоры можно поточечно складывать и вычитать:

$$D_1 + D_2 = \sum_{M \in \chi} a_M M + \sum_{M \in \chi} b_M M = \sum_{M \in \chi} (a_M + b_M)M.$$

Пусть D – дивизор на гладкой проективной кривой χ, тогда множество

$$L(D) = \{H \in F(\chi) : (H) + D \geq 0\}$$

является конечномерным линейным пространством над полем F и называется пространством Римана-Роха.

Пусть $P = \{P_1, \ldots, P_n\} \subset \chi, supp(D) \cap P = \emptyset, deg(D) = \alpha < n$. Определим алгеброгеометрический код как образ линейного отображения:

$$Ev: L(D) \rightarrow F^n, Ev(H) = (H(P_1), \ldots, H(P_n))$$

и обозначим его как $C = C(\chi, P, D)$.

При работе с алгеброгеометрическими кодами удобно иметь порождающую и проверочную матрицы этого кода: это позволяет абстрагироваться от объектов алгебраической геометрии и проводить стандартные вычисления в терминах линейной алгебры. Напомним, что порождающей матрицей A алгеброгеометрического кода C является матрица отображения Ev, т.е. матрица размера $dim(L(D)) \times n$, строками которой являются элементы базиса пространства Римана-Роха, отображенные в F^n с помощью Ev. Проверочной матрицей B является матрица кода, ортогонального к коду C как к векторному пространству. Таким образом, $A \times B^T = 0$.

Для получения порождающей и проверочной матриц кода использован пакет компьютерной алгебры Magma [16]. В листинге 1 приведем текст программы на языке программирования Magma, выводящую на экран порождающую и проверочную матрицы кода $C = C(\chi(X^5 + Y^4Z + YZ^4, F), 9 \cdot (0:1:0), P)$ над полем $F = F_{16}$, где $P = \chi \setminus \{(0:1:0)\}$, т.е. множество всех точек кривой, кроме точки $(0:1:0)$. На 1 строке мы строим конечное поле F_{16}, на второй – проективное пространство $P^2(F)$ над этим полем. Затем на строках 3-5 мы задаем многочлен G, строим кривую и вычисляем ее точки. Убедившись, что в массиве точек $places$ необходимая нам точка имеет индекс 1, далее на строке 6 мы строим дивизор $D = 9 \cdot (0:1:0)$. Затем на строке 7 удаляем первую точку из массива $places$. На 8 строке мы получаем код. Далее остается вывести на экран порождающую и проверочную матрицы кода.

Схема эксперимента по исследованию надежности ССШШ с алгеброгеометрическими кодами. Пусть $c \in \mathbb{N} \setminus \{1\}, C$ – алгеброгеометрический код. Пусть C_0 – случайно выбранная коалиция из $coal_c(C)$, а $\omega \in desc(C_0)$ – случайно выбранный потомок этой коалиции.

Листинг 1.

```
1  F<w> := GF(16);
2  P2<x,y,z> := ProjectiveSpace(F, 2);
3  G := x^5 + y^4*z + y*z^4;
4  X := Curve(P2, G);
5  places := Places(X, 1);
6  D := 9 * places[1];
7  Exclude(~places, places[1]);
8  C := AlgebraicGeometricCode(places, D);
9  GeneratorMatrix(C);
10 ParityCheckMatrix(C).
```

Рассмотрим следующие события: 1) A_1: потомок ω является кодовым вектором. Это означает, что при наступлении события A_1 можно сделать вывод, что код C не является c-FP-кодом. 2) A_2: потомок ω относительно метрики ρ лежит ближе к $C \setminus C_0$, чем к коалиции. Т.е., после вычисления d – минимального из расстояний

между ω и векторами коалиции – найден кодовый вектор из $C \setminus C_0$, расстояние от которого до ω не больше d. Это означает, что при наступлении события A_2 можно сделать вывод, что код C не является c-TA кодом.

Рассмотрим схему проведения вычислительных экспериментов:

♦ Выбрать алгеброгеометрический код C над полем $F = F_q$, построить его порождающую и проверочную матрицы. Пусть k – размерность кода, а n – его длина.

♦ Положить $c = 2$, выбрать c случайных элементов пространства F^k, отобразить их с помощью отображения Ev в F^k, умножив на порождающую матрицу A. Таким образом, мы получим случайную коалицию C_0.

♦ Выбрать случайным образом потомка ω коалиции C_0, не совпадающего ни с одним вектором из коалиции, т.е. $\omega \in desc(C_0) \setminus C_0$.

♦ Проверить условие $\omega \in C \setminus C_0$, вычислив синдром: $s = \omega B^T$, где B – проверочная матрица кода. Если $s = 0$, то выполняется, что $\omega \in C \setminus C_0$, тогда необходимо зафиксировать события A_1 и A_2, а в противном случае продолжить.

♦ Проверить, лежит ли ω ближе к C_0, чем к $C \setminus C_0$. Для этого вычислить расстояние d – минимальное из расстояний между ω и векторами C_0, а затем, перебрав все кодовые векторы из $C \setminus C_0$ и вычислив расстояния от ω до них, проверить, существует ли кодовый вектор из $\$C \setminus C_0$, расстояние от которого до ω не больше d. Если есть, то зафиксировать событие A_2.

Эксперименты для данной величины c повторяются заданное количество раз. Далее значение c увеличивается, и эксперименты повторяются, пока $c < n$.

Вычислим, сколько раз нужно провести эксперимент при заданном c. Будем считать, что случайная величина, определенная на пространстве исходов событий A_1 и A_2, имеет распределение Стьюдента. Выберем для события доверительную вероятность $p_\alpha = 0.99$ и точность оценки $\delta = 0.005$. Согласно [17], глава 16, параграф 15, $\delta = t^{-1}(p_\alpha)\sqrt{\frac{p(1-p)}{N}}$, где $t(x)$ – распределение Стьюдента, p – частота появления события, N-- число экспериментов. Так как p неизвестно, мы можем полагать, что $p = 0.5$. Тогда в нашем случае $N = 66564$. В работе мы провели 70000 экспериментов для каждого из c.

Алгеброгеометрические коды, выбранные для проведения экспериментов. В качестве примера были проведены эксперименты для двух алгеброгеометрических кодов:

$$\mathrm{C}_1 = (\chi_1 = \chi_1(Y^2Z + XYZ + YZ^2 - X^3 - Z^3, F), 3 \cdot (0:1:0), P_1),$$

$$\mathrm{C}_1 = (\chi_1(X^3Y + Y^3Z + Z^3X, F), 5 \cdot (0:1:0), P_2),$$

где $P_1 = \chi_1 \setminus \{(0:1:0)\}, P_2 = \chi_2 \setminus \{(0:1:0), (1:0:0)\}, F = \mathrm{F}_8$. Для первого кода длина $n = 13$, а для второго $n = 22$.

Приведем теорему о рубежах компрометации FP-свойства и TA-свойства и затем вычислим теоретические оценки этих рубежей для кодов C_1 и C_2.

Теорема 1 ([14], теоремы 3, 4). Пусть $\mathrm{C} = \mathrm{C}(\chi(G, F), D, \{P_1, \ldots, P_n\})$ – алгеброгеометрический код над полем F. Тогда

$$R_{FP}(C) \geq \lceil \frac{n}{deg(D)} \rceil, R_{TA}(C) \geq \lceil \sqrt{\frac{n}{deg(D)}} \rceil$$

Если Q – единственная точка на кривой, и $D = \alpha Q$, а $|P| > 1$, то

$$R_{FP}(C) \leq \lceil \frac{n}{\lfloor deg(D)/deg(G) \rfloor} \rceil, R_{TA}(C) \leq \lceil \frac{n+\alpha}{2\lfloor deg(D)/deg(G) \rfloor} \rceil.$$

Согласно теореме 1,

$$\lceil\frac{13}{3}\rceil = 5 \le R_{FP}(C_1) \le \lceil\frac{13}{\lfloor 3/3\rfloor}\rceil = 13,$$

$$\lceil\sqrt{\frac{13}{3}}\rceil = 3 \le R_{TA}(C_1) \le \lceil\frac{13+3}{2\lfloor 3/3\rfloor}\rceil = 8,$$

$$R_{FP}(C_2) \ge \lceil\frac{22}{5}\rceil = 5, R_{TA}(C_2) \ge \lceil\sqrt{\frac{22}{5}}\rceil = 3.$$

Покажем, что для кода C_1 значение R_{TA} равно ровно 3, а значение R_{FP} равно ровно 5. Для этого предъявим коалицию ${C_0}^1$ мощности 3 и такого ее потомка, который лежит ближе к множеству $C \setminus {C_0}^1$, чем к коалиции ${C_0}^1$, относительно метрики ρ. Это будет означать, что

$R_{TA}(C_1) \le 3$, и тогда, учитывая оценки выше, это также означает, что $R_{TA}(C_1) = 3$. Далее предъявим коалицию ${C_0}^2$ мощности 5 и ее потомка, являющегося кодовым вектором. Аналогично, это будет означать, что $R_{FP}(C_1) = 5$. Коалиции будем строить согласно принципу, описанному в [5], лемме 1. Пусть $F = \mathrm{F}_8{=}\mathrm{F}_2[\xi]/(\xi^3 + \xi + 1)$, а множество P_1 упорядочено следующим образом:

$$P_1 = \{(1:0:1), (\xi^4:1:1), (\xi^2:1:1), (\xi:1:1), (\xi:\xi:1), (\xi^5:\xi:1), (\xi^6:\xi:1), (\xi^2:\xi^2:1),$$
$$(\xi^5:\xi^2:1), (\xi^3:\xi^2:1), (\xi^3:\xi^4:1), (\xi^4:\xi^4:1), (\xi^6:\xi^4:1)\}.$$

Тогда коалиция ${C_0}^1$ состоит из векторов:

$$u_1 = (\xi, \xi^3, \xi^3, \xi^3, 0,0,0, \xi^4, \xi^4, \xi^4, \xi^2, \xi^2, \xi^2),$$
$$u_2 = (\xi^2, \xi^6, \xi^6, \xi^6, \xi^4, \xi^4, \xi^4, 0,0,0, \xi, \xi, \xi),$$
$$u_3 = (\xi^4, \xi^5, \xi^5, \xi^5, \xi^2, \xi^2, \xi^2, \xi, \xi, \xi, 0,0,0).$$

Очевидно, что можно построить потомка ω этой коалиции:

$$\omega = (\xi, \xi^3, \xi^3, \xi^3, 0,0,0,0,0,0,0,0,0),$$

расстояние ρ от которого до нулевого вектора равно 4.

При этом $\rho(u_1, \omega) = 6, \rho(u_1, \omega) = 9, \rho(u_1, \omega) = 9$, т.е. ω лежит ближе к множеству $C \setminus {C_0}^1$, чем к коалиции ${C_0}^1$, относительно метрики ρ, значит, $R_{TA}(C_1) = 3$. В коалицию ${C_0}^2$ поместим u_1, u_2, u_3, а также следующие кодовые векторы:

$$u_4 = (1,0,0,0, \xi^3, \xi^3, \xi^3, \xi^6, \xi^6, \xi^6, \xi^5, \xi^5, \xi^5),$$
$$u_5 = (0, 1,1,1, \xi, \xi, \xi, \xi^2, \xi^2, \xi^2, \xi^4, \xi^4, \xi^4).$$

Одним из потомков коалиции ${C_0}^2$ является нулевой вектор, это означает, что $R_{FP}(C_1) = 5$. Таким образом, теоретические исследования показывают, что $R_{FP}(C_1) = 5, R_{TA}(C_1) = 3, R_{FP}(C_2) \ge 5, R_{TA}(C_2) \ge 3$.

Результаты эксперимента. Вычисления проведены с помощью программы, реализованной на языке программирования Python с использованием библиотек *numpy* и *galois*. Использован компьютер с 12 ядрами мощностью 3.2 ГГц и ОЗУ объемом 32 Гб. Кроме того, для каждого из значений c эксперименты запущены параллельно на разных ядрах процессора с помощью библиотеки *concurrent.futures*.

В табл. 1 приведены полученные значения вероятности $p(A_1, c), p(A_2, c)$ появления событий A_1 и A_2 для кода C_1, а в табл. 2 – значения $p(A_1, c), p(A_2, c)$ для кода C_2. На рис. 1 показан график зависимости оценок вероятности p события A_2 для кодов C_1 и C_2 от величины c.

Таблица 1

Значения вероятностей наступления событий A_1 и A_2 для кода C_1

c	2	3	4	5	6	7
$p(A_1, c)$	0	0	0	0	0	
$p(A_2, c)$	0	0,052	0,188	0,315	0,406	0,478
c	8	9	10	11	12	13
$p(A_1, c)$	0	0	0	0	0	
$p(A_2, c)$	0,529	0,570	0,595	0,618	0,634	0,649

Проведенный вычислительный эксперимент подтверждает справедливость теоретических исследований, согласно которым значения R_{FP} и R_{TA} для кода C_1равны 5 и 3 соответственно, так как оценки вероятности события A_1 для $c < R_{FP}(C_1) = 5$ и события A_2 для $c < R_{TA}(C_1) = 3$ на практике равны нулю.
Аналогично, подтверждается, что $R_{TA}(C_2) \geq 3, R_{FP}(C_2) \geq 5$. Более того, на основании эксперимента можно утверждать, что для C_2 получено точное значение рубежа $R_{TA}(C_2)$, так как для C_2 выполняется, что $p(A_2, 3) > 0$, т.е., $R_{TA}(C_2) \leq 3$, и тогда, учитывая теоретическую границу $R_{TA}(C_2) \geq 3$, получаем, что $R_{TA}(C_2) = 3$.

Таблица 2

Значения вероятностей наступления событий A_1 и A_2 для кода C_2

c	2	3	4	5	6	7	8
$p(A_1, c)$	0	0	0	0	0		
$p(A_2, c)$	0	0,002	0,033	0,110	0,202	0,289	0,360
c	9	10	11	12	13	14	15
$p(A_1, c)$	0	0	0	0	0	0	0
$p(A_2, c)$	0,419	0,470	0,503	0,534	0,560	0,584	0,597
c	16	17	18	19	20	21	22
$p(A_1, c)$	0	0	0	0	0	0	0
$p(A_2, c)$	0,613	0,622	0,632	0,642	0,647	0,653	0,660

Обратим теперь внимание на оценки частоты нарушения идентифицирующих свойств при превышении теоретически допустимой мощности коалиции злоумышленников. Мы видим, что C_2 имеет лучшие показатели надежности при превышении границ. Однако отметим, что это достигается за счет большей длины кодового вектора, а обработка векторов большей длины требует больших вычислительных затрат и затрат памяти.

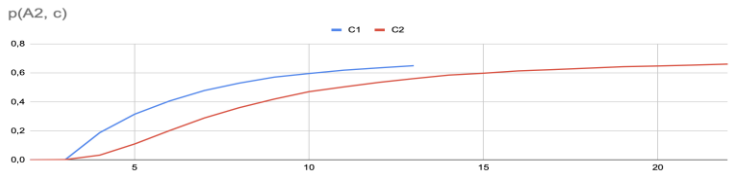

Рис. 1. График зависимости вероятности p события A_2 для кодов C_1 и C_2 от величины c

Для кода C_1 вероятность нарушения TA-свойства менее 10% при $c = 3$, менее 50% при значениях c вплоть до 7; для кода C_2 вероятность нарушения TA-свойства менее 10% при $c = 3,4$, и менее 50% при значениях c вплоть до 10. Эти данные могут быть использованы при проектировании схем широковещательного шифрования: полученные значения означают, что при незначительном превышении рубежа R_{TA} для рассматриваемых кодов вероятность успешного нахождения нелегального пользователя из коалиции злоумышленников все еще достаточно велика.

Рассмотрим открытые вопросы, представляющие интерес для дальнейших исследований. Первым вопросом является переход от экспоненциальной сложности проверки события A_2 к полиномиальной. Возможным вариантом реализации такого перехода является использование полиномиального списочного декодера. Списочным декодером называют алгоритм, который по заданному коду, произвольному вектору из пространства (необязательно кодовому) и расстоянию d получает список всех кодовых векторов, лежащих не более, чем на расстоянии d от заданного вектора. Таким образом, при проверке события A_2 можно использовать списочный декодер, на вход которого необходимо подать код, случайного потомка случайной коалиции ω и минимальное из расстояний от ω до векторов из коалиции. Если списочный декодер будет иметь полиномиальную сложность, то и вся проверка будет иметь полиномиальную сложность. Полиномиальные списочные декодеры для алгеброгеометрических кодов существуют, например, [18–20]. Вторым вопросом является построение более точного события – индикатора нарушения FP-свойства. Предложенное в работе событие A_1 ни разу не наступило ни для кода C_1, ни для кода C_2. Это говорит как и об устойчивости FP-свойства для рассмотренных алгеброгеометрических кодов, так и о несовершенстве эксперимента.

Заключение. В работе представлен вычислительный эксперимент и программные инструменты для его проведения, которые могут быть использованы с целью оценки надежности схем специального широковещательного шифрования, основанных на использовании алгеброгеометрических кодов малой мощности, в том числе в условиях превышения допустимых теоретических рубежей мощности злоумышленников. Представленная схема может быть использована, во-первых, для уточнения теоретических рубежей R_{TA} и R_{FP}, и во-вторых, для анализа поведения схем специального широковещательного шифрования при различных условиях.

В качестве примера вычислительный эксперимент проведен для конкретных алгеброгеометрических кодов C_1 и C_2. Для них получены оценки надежности схем специального широковещательного шифрования, в частности, частота нарушения идентифицирующих FP-свойства и TA-свойства при превышении теоретически допустимой мощности коалиции злоумышленников. Эти данные проанализированы, в том числе в сравнении с полученными ранее теоретическими границами. С помощью эксперимента удалось вычислить неизвестную ранее точную оценки R_{TA} для кода C_2. Очевидно, что представленный вычислительный эксперимент может быть использован для анализа других алгеброгеометрических кодов малой мощности.

Рассмотрены открытые вопросы, представляющие интерес для дальнейших исследований.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Fiat A., Naor M.* Broadcast Encryption // Advances in cryptology. Lecture Notes in Computer Science 773. – SpringerVerlag, 1994. – P. 480-491.
2. *Chor B., Fiat A., Naor M.* Tracing traitors // Advances in cryptology – CRYPTO'94. – Springer Berlin Heidelberg, 1994. – P. 257-270.
3. *Staddon J.N., Stinson D.R., Wei R.* Combinatorial properties of frameproof and traceability codes // Information Theory, IEEE Transactions on. – 2001. – Vol. 47, No. 3. – P. 1042-1049.
4. *Stinson D.R., Wei R.* Combinatorial properties and constructions of traceability schemes and frameproof codes // Information Theory, IEEE Transactions on. – 2001. – Vol. 47, No. 3. – P. 1042-1049.
5. *Silverberg A., Staddon J., Walker J.L.* Applications of list decoding to tracing traitors // Information Theory, IEEE Transactions on. – 2003. – Vol. 49, No. 5. – P. 1312-1318.
6. *Fernandez M., Cotrina J., Soriano M., Domingo N.* A Note about the Traceability Properties of Linear Codes // Proc. 10th Int. Conf. on Information Security and Cryptology (ICISC'2007). Seoul, Korea. November 29–30, 2007. Lecture Notes in Comp. Science. – Vol. 4817. – Berlin: Springer, 2007. – P. 251-258.
7. *Moreira J., Fernandez M. and Soriano M.* A note on the equivalence of the traceability properties of Reed-Solomon codes for certain coalition sizes // 2009 First IEEE International Workshop on Information Forensics and Security (WIFS), London, 2009. – P. 36-40.
8. *Кабатянский Г.А.* Идентифицирующие коды и их обобщения // Проблемы передачи информации. – 2019. – Т. 55, № 3. – С. 90-111.
9. *Егорова Е.Е., Фернандес М., Кабатянский Г.А., Мяо И.* Существование и конструкции мультимедийных кодов, способных находить полную коалицию при атаке усреднения и шуме // Проблемы передачи информации. – 2020. – Т. 56, № 4. – С. 97-108.
10. *Егорова Е.Е., Кабатянский Г.А.* Разделимые коды для защиты мультимедиа от нелегального копирования коалициями // Проблемы передачи информации. – 2021. – Т. 57, № 2. – С. 178-198.
11. *Гоппа В.Д.* Алгебраико-геометрические коды // Известия Российской академии наук. Серия математическая. – 1982. – Т. 46, № 4. – С. 762-781.
12. *Влэдуц С.Г., Ногин Д.Ю., Цфасман М.А.* Алгеброгеометрические коды. Основные понятия. – М.: МЦНМО, 2003.
13. *Hoholdt T., van Lint J. H., Pellikaan R.* Algebraic geometry codes // Handbook of coding theory. – 1998. – Vol. 1, No. Part 1. – P. 871-961.
14. *Deundyak V.M. and Zagumennov D.V.* On the Properties of Algebraic Geometric Codes as Copy Protection Codes // Automatic Control and Computer Sciences. – 2021. – Vol. 55, No. 7. – P. 795-808.
15. *Деундяк В.М., Загуменнов Д.В.* О границах мощности злоумышленников для идентифицирующих алгеброгеометрических кодов на специальных кривых // Прикладная дискретная математика. – 2021. – № 53. – С. 55-74.
16. Magma Computational Algebra System. Адрес доступа: http://magma.maths.usyd.edu.au/magma/ (дата обращения: 06.08.2022).
17. *Гмурман В.Е.* Теория вероятностей и математическая статистика. – 8-е изд. – М.: Высшая школа, 2002. – 479 с.
18. *Guruswami V, Sudan M.* Improved decoding of Reed-Solomon and algebraic-geometric codes // Foundations of Computer Science. – Palo Alto: IEEE, 1998. – P. 28-37.
19. *Shokrollahi A., Wasserman H.* List Decoding of Algebraic-Geometric Codes // IEEE Transactions on Information Theory. – 1999. – Vol. 45, No. 2. – P. 432-437.
20. *Fernandez M., Soriano M.* Identification of Traitors in Algebraic-Geometric Traceability Codes // IEEE Transactions on Signal Processing. – 2004. – Vol. 52, No. 10. – P. 3073-3077.

REFERENCES

1. *Fiat A., Naor M.* Broadcast Encryption, Advances in cryptology. Lecture Notes in Computer Science. – SpringerVerlag, 1994. Vol. 773. – P. 480-491.
2. *Chor B., Fiat A., Naor M.* Tracing traitors, *Advances in cryptology – CRYPTO'94*. Springer Berlin Heidelberg, 1994, pp. 257-270.
3. *Staddon J.N., Stinson D.R., Wei R.* Combinatorial properties of frameproof and traceability codes, *Information Theory, IEEE Transactions on*, 2001, Vol. 47, No. 3, pp. 1042-1049.

4. *Stinson D.R., Wei R.* Combinatorial properties and constructions of traceability schemes and frameproof codes, *Information Theory, IEEE Transactions on,* 2001, Vol. 47, No. 3, pp. 1042--1049.
5. *Silverberg A., Staddon J., Walker J.L*. Applications of list decoding to tracing traitors // Information Theory, *IEEE Transactions on,* 2003, Vol. 49, No. 5, pp. 1312-1318.
6. *Fernandez M., Cotrina J., Soriano M., Domingo N.* A Note about the Traceability Properties of Linear Codes, *Proc. 10th Int. Conf. on Information Security and Cryptology (ICISC'2007). Seoul, Korea. November 29–30, 2007. Lecture Notes in Comp. Science,* Vol. 4817. Berlin: Springer, 2007, pp. 251–258.
7. *Moreira J., Fernandez M. and Soriano M.* A note on the equivalence of the traceability properties of Reed-Solomon codes for certain coalition sizes, *2009 First IEEE International Workshop on Information Forensics and Security (WIFS), London, 2009,* pp. 36-40.
8. *Kabatyanskiy G.A.* Identifitsiruyushchie kody i ikh obobshcheniya [Identifying codes and their generalizations], *Problemy peredachi informatsii* [Problems of information transmission], 2019, Vol. 55, No. 3, pp. 90-111.
9. *Egorova E.E., Fernandes M., Kabatyanskiy G.A., Myao I.* Sushchestvovanie i konstruktsii mul'timediynykh kodov, sposobnykh nakhodit' polnuyu koalitsiyu pri atake usredneniya i shume [The existence and construction of multimedia codes capable of finding a complete coalition in the averaging attack and noise], *Problemy peredachi informatsii* [Problems of information transmission], 2020, Vol. 56, No. 4, pp. 97-108.
10. *Egorova E.E., Kabatyanskiy G.A.* Razdelimye kody dlya zashchity mul'timedia ot nelegal'nogo kopirovaniya koalitsiyami [Separable codes to protect multimedia from illegal copying by coalitions], *Problemy peredachi informatsii* [Problems of information transmission], 2021, Vol. 57, No. 2, pp. 178-198.
11. *Goppa V.D.* Algebraiko-geometricheskie kody [Algebraic-geometric codes], *Izvestiya Rossiyskoy akademii nauk. Seriya matematicheskaya* [Proceedings of the Russian Academy of Sciences. The series is mathematical], 1982, Vol. 46, No. 4, pp. 762-781.
12. *Vleduts S.G., Nogin D.Yu., TSfasman M.A.* Algebrogeometricheskie kody. Osnovnye ponyatiya [Algebraogeometric codes. Basic concepts]. Moscow: MTSNMO, 2003.
13. *Hoholdt T., van Lint J. H., Pellikaan R.* Algebraic geometry codes, *Handbook of coding theory,* 1998, Vol. 1, No. Part 1, pp. 871-961.
14. *Deundyak V.M. and Zagumennov D.V*. On the Properties of Algebraic Geometric Codes as Copy Protection Codes, *Automatic Control and Computer Sciences,* 2021, Vol. 55, No. 7, pp. 795-808.
15. *Deundyak V.M., Zagumennov D.V.* O granitsakh moshchnosti zloumyshlennikov dlya identifitsiruyushchikh algebrogeometricheskikh kodov na spetsial'nykh krivykh [On the limits of the power of intruders for identifying algebra-geometric codes on special curves], *Prikladnaya diskretnaya matematika* [Applied Discrete Mathematics], 2021, No. 53, pp. 55-74.
16. Magma Computational Algebra System. Available at: http://magma.maths.usyd.edu.au/magma/ (accessed 06 August 2022).
17. *Gmurman V.E.* Teoriya veroyatnostey i matematicheskaya statistika [Probability theory and mathematical statistics]. 8th ed. Moscow: Vysshaya shkola, 2002, 479 p.
18. *Guruswami V, Sudan M.* Improved decoding of Reed-Solomon and algebraic-geometric codes, *Foundations of Computer Science*. Palo Alto: IEEE, 1998, pp. 28-37.
19. *Shokrollahi A., Wasserman H.* List Decoding of Algebraic-Geometric Codes, *IEEE Transactions on Information Theory,* 1999, Vol. 45, No. 2, pp. 432-437.
20. *Fernandez M., Soriano M.* Identification of Traitors in Algebraic-Geometric Traceability Codes, *IEEE Transactions on Signal Processing,* 2004, Vol. 52, No. 10, pp. 3073-3077.

Статью рекомендовал к опубликованию к.ф.-м.н. А.В. Криворучко.

Загуменнов Денис Владимирович – Южный федеральный университет; e-mail: zagumen.denis@gmail.com; г. Ростов-на-Дону, Россия; тел.: +79185820982; кафедра алгебры и дискретной математики; м.н.с.; аспирант.

Мкртичян Вячеслав Витальевич – e-mail: mkrtichan@list.ru; тел.: +79034310555; кафедра алгебры и дискретной математики; к.т.н.; доцент.

Zagumennov Denis Vladimirovich – Southern Federal University; e-mail: zagumen.denis@gmail.com; Rostov-on-Don, Russia; phone: +79185820982; the department of algebra and discrete mathematics; junior researcher; graduate student.

Mkrtichyan Vyacheslav Vital'evich – e-mail: mkrtichan@list.ru; phone: +79034310555; the department of algebra and discrete mathematics; cand. of eng. sc.; associate professor.

УДК 519.224.22 DOI 10.18522/2311-3103-2022-4-50-62

А.К. Мельников, И.И. Левин, А.И. Дордопуло, Л.М. Сластен

ОЦЕНКА ВОЗМОЖНОСТЕЙ ПЕРСПЕКТИВНЫХ ВЫЧИСЛИТЕЛЬНЫХ ТЕХНОЛОГИЙ ДЛЯ РАСЧЕТА ТОЧНЫХ ПРИБЛИЖЕНИЙ РАСПРЕДЕЛЕНИЙ ВЕРОЯТНОСТЕЙ ЗНАЧЕНИЙ СТАТИСТИК

Статья посвящена оценке аппаратного ресурса вычислительных систем для решения вычислительно-трудоемкой задачи – расчета распределений вероятностей значений статистик методом второй кратности на основе Δ-точных приближений для выборок объемом от 320 до 1280 знаков при мощности алфавита от 128 до 256 символов с точностью $\Delta=10^{-5}$. Общее время решения не должно превышать 30 дней или $2{,}592\cdot10^{6}$ секунд при круглосуточном режиме вычислений. Использование свойств метода второй кратности позволяет привести вычислительную сложность расчета к диапазону $9{,}68\cdot10^{22}$–$1{,}60\cdot10^{52}$ операций с числом проверяемых векторов – от $6{,}50\cdot10^{23}$ до $1{,}39\cdot10^{50}$. Решение этой задачи для указанных параметров выборок в заданное время с помощью современных вычислительных средств (процессоров, графических ускорителей, программируемых логических интегральных схем) требует недостижимого на практике аппаратного ресурса. Поэтому в статье анализируются возможности перспективных квантовых и фотонных технологий для решения задачи с заданными параметрами. Основным преимуществом квантовых вычислительных систем является высокая скорость вычислений для всех возможных значений параметров. Однако, для расчета распределений вероятностей значений статистик квантовое ускорение не будет достигнуто из-за необходимости проверки всех полученных решений, число которых соответствует размерности задачи. Кроме того, текущий уровень развития элементной базы не позволяет создавать и использовать квантовые вычислители с разрядностью 120 кубитов, необходимой для решения рассматриваемой задачи. Фотонные вычислители могут обеспечить высокую скорость вычислений при низком энергопотреблении и для решения рассматриваемой задачи требуют наименьшее число узлов. Однако, нерешенные проблемы с физической реализацией элементов оперативного хранения данных и отсутствием доступной элементной базы не позволяют в обозримой перспективе (5–7 лет) использовать фотонные вычислительные технологии для расчета распределений вероятностей значений статистик, поэтому наиболее целесообразно применение гибридных вычислительных систем, содержащих узлы различных архитектур. Для реализации задачи на различных аппаратных платформах (универсальные процессоры, графические ускорители, программируемые логические интегральные схемы) и конфигурациях гибридных вычислительных систем предложено использование архитектурно-независимого языка программирования высокого уровня SET@L, объединяющего представление вычислений в виде множеств и совокупностей с помощью альтернативной теории множеств П. Вопенка с абсолютным параллелизмом информационного графа и парадигмами аспектно-ориентированного программирования.

Вероятность; статистика; точное распределение; точное приближение; алгоритмическая сложность; квантовые вычисления; фотонные технологии; архитектурно-независимое программирование; язык Set@l.