АЛГОРИТМЫ ЭЦП НА КОНЕЧНЫХ НЕКОММУТАТИВНЫХ АЛГЕБРАХ НАД ПОЛЯМИ ХАРАКТЕРИСТИКИ ДВА

Молдовян А.А.[1], Молдовян Н.А.[2]

Ключевые слова: *конечная некоммутативная алгебра; ассоциативная алгебра; вычислительно трудная задача; скрытая коммутативная группа; цифровая подпись; многомерная криптография; постквантовая криптография.*

Цель *работы: повышение производительности и снижение схемотехнической сложности аппаратной реализации постквантовых алгебраических алгоритмов ЭЦП, основанных на вычислительной трудности решения систем многих квадратных уравнений с многими неизвестными.*

Метод *исследования: разработка постквантовых алгоритмов ЭЦП на конечных некоммутативных ассоциативных алгебрах, заданных над конечными полями характеристики два, обладающих высокой производительностью и малыми размерами подписи и открытого и секретного ключей. Использование концепции построения алгебраических схем ЭЦП со скрытой коммутативной группой, характеризующихся применением векторного проверочного уравнения степенного типа с многократным вхождением подписи в качестве множителя. Выбор степени расширения поля GF(2^z), при которой порядок скрытой группы делится только на простые делители размером не менее 24 бит.*

Результаты *исследования: сформулированы основные положения реализации постквантовых алгоритмов ЭЦП со скрытой группой, стойкость которых основана на вычислительной трудности решения систем многих квадратных уравнений с многими неизвестными, на конечных некоммутативных алгебрах, заданных над полями вида GF(2^z). Установлены значения степени расширения z, при которых порядок скрытой коммутативной группы делится только на простые делители достаточно большого размера. Разработан новый постквантовый алгоритм ЭЦП со сравнительно высокой производительностью и малыми размерами подписи и открытого и секретного ключей. Используя неформальный показатель стойкости в виде произведения двоичного логарифма от порядка поля на число неизвестных, выполнено сравнение разработанных и известных постквантовых алгоритмов при заданном уровне стойкости.*

Научная и практическая значимость *результатов статьи состоит в основных положениях построения постквантовых алгоритмов ЭЦП со скрытой группой при использовании в качестве алгебраического носителя конечных некоммутативных алгебр, заданных над полями GF(2z) с вычислительно эффективными операциями сложения и умножения, обеспечивающих предпосылки повышения производительности и снижения стоимости аппаратной реализации.*

DOI: 10.21681/2311-3456-2022-3-58-68

Введение

Последние 40 лет для обеспечения информационной безопасности в информационно-телекоммуникационных системах и технологиях широко применяются криптографические алгоритмы с открытым ключом, стойкость которых базируется на вычислительной трудности задачи дискретного логарифмирования (ЗДЛ) и задачи факторизации (ЗФ), хотя достаточно давно предложены эффективные полиномиальные по времени алгоритмы решения ЗДЛ и ЗФ на квантовом компьютере [1,2] и в теоретическом плане рассматривалась задача разработки постквантовых двухключевых криптосхем, которые являются стойкими к квантовым атакам (атакам с использованием квантовых вычислителей). Исследования в этом направле-

1 Молдовян Александр Андреевич, доктор технических наук, главный научный сотрудник лаборатории кибербезопасности и постквантовых криптосистем Санкт-Петербургского федерального исследовательского центра Российской академии наук, Санкт-Петербург, Россия. ORCID. org/0000-0001-5480-6016. E mail: maa1305@yandex.ru

2 Молдовян Николай Андреевич, доктор технических наук, главный научный сотрудник лаборатории кибербезопасности и постквантовых криптосистем Санкт-Петербургского федерального исследовательского центра Российской академии наук, Санкт-Петербург, Россия. ORCID. org/0000-0002-4483-5048. E mail: nmold@mail.ru

нии привели к формированию области постквантовой криптографии[3,4,5].

Для разработки постквантовых двухключевых криптосхем используются вычислительно трудные задачи, формулируемые над конечными некоммутативными алгебрами [3,4], помехоустойчивыми кодами [5,6], алгебраическими решетками [7] и булевыми функциями [8].

До конца 2016 г. считалось, что предпосылки практического появления в обозримом будущем многокубитового квантового компьютера отсутствуют, поэтому не было опасений за безопасность действующих официальных стандартов на криптоалгоритмы с открытым ключом. Однако существенный прогресс в технологии квантовых вычислений побудил специалистов Национального института стандартов и технологий США (НИСТ) прийти к мнению, что после 2025 г. реально действующий многокубитовый квантовый компьютер может в неожиданный момент появиться, означая необходимость отказа от действующих стандартов на криптографические алгоритмы с открытым ключом. С целью упреждения такой критической ситуации в декабре 2016 г. НИСТ анонсировал программу по разработке постквантовых криптографических стандартов на период 20172024 гг., в рамках которой объявил всемирный конкурс на разработку постквантовых криптосхем по следующим двум номинациям: 1) алгоритмам открытого распределения ключей и открытого шифрования и 2) алгоритмам электронной цифровой подписи (ЭЦП)[6].

Из 69 постквантовых схем, заявленных и принятых к рассмотрению в рамках конкурса НИСТ, после первого этапа было отобрано 26 алгоритмов для участия во втором раунде [9], который завершился выбором четырех финалистов и пяти альтернативных алгоритмов по первой номинации, а также трех финалистов и трех альтернативных алгоритмов по второй номинации[10]. Третий этап конкурса завершился, однако официальный отчет по нему пока не опубликован. По предварительной оценке итогов по номинации алгоритмов ЭЦП НИСТ имеет намерение объявить дополнительный прием заявок для включения в конкурс по указанной номинации [11]. Неожиданно конкурс НИСТ выявил ряд проблем по разработке постквантовых схем ЭЦП, включающих большие размеры подписи и/или открытого и секретного ключей для отобранных финалистов и альтернативных алгоритмов.

Для устранения этого недостатка в работах [12,13] предложен подход к разработке постквантовых алгоритмов ЭЦП на основе вычислительной трудности скрытой ЗДЛ. Использование различных способов маскирования скрытой группы, в которой задается ЗДЛ, позволило предложить несколько алгоритмов ЭЦП, представляющих интерес в качестве практичных постквантовых криптосхем, в том числе алгоритмов с удвоенным проверочным уравнением [14,15], в которых в качестве одного из элементов ЭЦП используется вектор. Дальнейшие поиски новых вариантов построения алгоритмов ЭЦП со скрытой группой неожиданно привели к новой концепции построения схем ЭЦП на некоммутативных алгебрах [16], в основе стойкости которых лежит вычислительная трудность решения систем многих квадратных уравнений с многими неизвестными.

Квантовый компьютер не является эффективным для решения этой задачи, которая лежит в основе ряда постквантовых двухключевых криптоалоритмов многомерной криптографии [17]. Поэтому алгоритмы ЭЦП, разрабатываемые в рамках концепции [16] не требуют специального обоснования постквантовой стойкости. При этом они, также как и схемы ЭЦП на основе скрытой ЗДЛ, используют операции экспоненцирования в скрытой группе, но их принципиальным отличием от последних является то, что подпись в обязательном порядке включает некоторый вектор **S**, который многократно входит в уравнение проверки подлинности ЭЦП в качестве множителя. Известные алгоритмы ЭЦП со скрытой группой, основанные на вычислительной трудности решения систем квадратных уравнений [16,18], разработаны на КНАА, заданных над простым конечным полем $GF(p)$. Сравнение с известными постквантовыми алгоритмами ЭЦП показывает, что первые обладают существенно меньшими размерами открытого ключа и подписи и более высокой производительностью [17]. Однако для улучшения этих параметров имеется дополнительный резерв, связанный с использованием в качестве алгебраического носителя КНАА, заданных над конечными полями характеристики два, т. е. над полями $GF(2^z)$, в которых операции сложения и умножению имеют

3 Post-Quantum Cryptography. 7th International Conference, PQCrypto 2016, Fukuoka, Japan, February 24-26, 2016, Proceedings // Lecture Notes in Computer Science. Springer, 2019. Vol. 9606.

4 Post-Quantum Cryptography. 10th International Conference, PQCrypto 2019, Chongqing, China, May 8–10, 2019. Proceedings // Lecture Notes in Computer Science. Springer, 2019. Vol. 11505.

5 Post-Quantum Cryptography. 12th International Conference, PQCrypto 2021. Daejeon, South Korea, July 20–22, 2021. Proceedings // Lecture Notes in Computer Science. Springer, 2021. Vol. 12841.

6 Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms // Federal Register, December 20, 2016.Vol. 81. No. 244. P. 92787–92788.https://www.gpo.gov/fdsys/pkg/FR-2016-12-20/pdf/2016-30615.pdf. (обращение 17 февраля 2022).

существенно меньшую вычислительную сложность по сравнению с аналогичными операциями в поле $GF(p)$ при примерно равном размере порядка поля.

Постановка цели исследования

В данной работе рассматриваются вопросы задания КНАА, пригодных для использования в качестве алгебраических носителей алгоритмов ЭЦП со скрытой группой, над конечными полями $GF(2^z)$. За счет использования КНАА над конечными полями характеристики два (с вычислительно эффективными операциями сложения и умножения) обеспечивается уменьшение времени выполнения операций умножения векторов и возведения вектора в степень большого размера. Последнее потенциально приводит к повышению производительности алгоритмов ЭЦП и снижению схемотехнической сложности их аппаратной реализации при заданном уровне стойкости по сравнению с аналогичными реализациями с использованием КНАА, заданных над простым конечным полем $GF(p)$ при примерно равном размере порядка поля (т. е. при $\log_2 p \approx z$)

Для достижения указанной цели решаются следующие частные задачи:

- формулировка требований к выбору таблиц умножения базисных векторов (ТУБВ) и параметров задания конечных полей $GF(2^z)$;
- изучение возможности задания КНАА над полем $GF(2^z)$, содержащих большое число коммутативных подалгебр, мультипликативная группа которых обладает двухмерной цикличностью;
- разработка постквантовых алгоритмов ЭЦП на КНАА, заданных над конечными полями характеристики два.

1. Задание КНАА над полями $GF(2^z)$

Коечная m-мерная алгебра определяется как m-мерное векторное пространство над конечным полем, в котором задана дополнительная операция – векторное умножение всевозможных пар векторов (или просто операция умножения), обладающая свойствами замкнутости и дистрибутивности слева и справа относительно операции сложения. Операция умножения векторов $\mathrm{A}=\sum_{i=0}^{m-1} a_i \mathrm{e}_i$ и $\mathrm{B}=\sum_{j=0}^{m-1} b_j \mathrm{e}_j$, где e_i – формальные базисные векторы, может быть определена по следующей формуле:

$$\mathrm{AB}=\sum_{i=0}^{m-1}\sum_{j=0}^{m-1} a_i b_j \left(\mathrm{e}_i \mathrm{e}_j\right), \qquad (1)$$

где каждое из всевозможных произведений пар базисных векторов заменяется на некоторый базисный вектор $\mathbf{e}_i$ или на однокомпонентный вектор вида $\lambda\mathbf{e}_j$, где $\lambda \neq 1$ называется структурной константой, по правилу, задаваемому некоторой ТУБВ. Для построения алгебраических алгоритмов ЭЦП в соответствии с концепцией [16] в качестве алгебраического носителя следует использовать КНАА.

Известно большое число различных ТУБВ для задания КНАА четной размерности над простыми конечными полями $GF(p)$ нечетной характеристики p. Как правило, эти ТУБВ могут быть применены и для задания КНАА над полями $GF(2^z)$. Исключение составляют ТУБВ с симметричным распределением (относительно диагонали, проходящей из верхнего левого угла в нижний правый) базисных векторов, в которых свойство некоммутативности операции умножения связано с несимметричным распределением структурной константы $\lambda = -1$. Примерами последнего случая являются ТУБВ, описанные в работе [19]. В целом имеется достаточно широкий выбор ТУБВ для задания КНАА различных четных размерностей над конечными полями $GF(2^z)$, в том числе ТУБВ, сгенерированные с помощью унифицированных способов их построения [19,20].

При построении алгоритмов ЭЦП со скрытой группой в качестве последней могут быть заданы коммутативные группы с различным строением, однако в соответствии с работами [16,18] предпочтительным является использование коммутативных групп с двухмерной цикличностью (т. е. групп, порождаемых базисом, включающим два групповых элемента одинакового порядка). Для ряда четырехмерных КНАА, заданных над простыми конечными полями $GF(p)$, существование в них большого числа таких групп показано полным исследованием их строения с точки зрения декомпозиции на коммутативные подалгебры. Примером является КНАА, заданная по ТУБВ, представленной как табл. 1 [13].

Рассмотрение основных свойств четырехмерной КНАА, заданной по табл. 1 над конечным полем вида $GF(2^z)$, выполненное по аналогии с исследованием [13], показало следующее:

1. Глобальной двухсторонней единицей данной алгебры является вектор $\mathbf{E}$ = (1, 1, 0, 0).

2. Вектор $\mathbf{A}$ = (a_0, a_1, a_2, a_3) является обратимым при выполнении условия

$$a_0 a_1 \neq a_2 a_3. \qquad (2)$$

3. Число обратимых векторов в алгебре (порядок мультипликативной группы алгебры) равно значению $\Omega = 2^z(2^z - 1)(2^{2z} - 1)$.

4. Векторы вида **L** = (s, s, 0, 0) при всевозможных $s \in GF(2^z)$ являются скалярными векторами (вектор **L** *называется скалярным, если для любого вектора* **V** *выполняется соотношение* **LV** = **VL** = s**V** при некотором скалярном значении s).

5. Данная КНАА разбивается на множество коммутативных подалгебр порядка 2^{2z}, которые пересекаются строго в множестве скалярных векторов.

6. *Коммутативные подалгебры* порядка 2^{2z} относятся к трем различным типам, отличающимся строением и порядком их мультипликативной группы. Последние разделяются на

а) *группы с двухмерной цикличностью*, имеющие порядок $\Omega_1 = (2^z - 1)^2$;

б) *циклические группы порядка* $\Omega_2 = 2^{2z} - 1$;

в) *циклические группы порядка* $\Omega_3 = 2^z(2^z - 1)$.

7. Общее число коммутативных подалгебр порядка 2^{2z} равно $2^{2z} + 2^z + 1$.

Таблица 1

Задание операции умножения четырехмерной КНАА ($\lambda \neq 0$) [13]

·	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_0$	$\mathbf{e}_0$	0	0	$\mathbf{e}_3$
$\mathbf{e}_1$	0	$\mathbf{e}_1$	$\mathbf{e}_2$	0
$\mathbf{e}_2$	$\mathbf{e}_2$	0	0	$\lambda_{\mathbf{e}1}$
$\mathbf{e}_3$	0	$\mathbf{e}_3$	$\lambda_{\mathbf{e}0}$	0

2. Выбор параметров поля $GF(2^z)$

Формула (1) показывает, что уменьшение вычислительной сложности операции умножения векторов может быть достигнуто выбором конечных полей, над которыми задаются КНАА, с более быстрыми операциями сложения и умножения, в частности выбором полей $GF(2^z)$ с умножением по модулю неприводимого двоичного трехчлена или пятичленна (если для заданной степени неприводимый трехчлен не существует) степени *z*. При выборе модуля такого вида операция модульного умножения двоичных многочленов может быть осуществлена путем выполнения арифметического умножения, двух операций арифметического сдвига и двух сложений, т. е. без выполнения операции арифметического деления многочленов.

Для выбора неприводимого двоичного трехчлена или пятичленна следует определиться с выбором значения степени расширения. Для этого следует учесть наше намерение использовать в качестве скрытой группы коммутативные группы с двухмерной цикличностью, порядок которых равен $\Omega_1 = (2^z - 1)^2$. Для алгоритмов ЭЦП со скрытой группой, стойкость которых основывается на вычислительной трудности решения систем из многих квадратных уравнений с многими неизвестными, факторизация порядка скрытой группы не является критическим моментом. Однако для снижения числа операций экспоненцирования выполняемых в ходе процедуры генерации ЭЦП будем по аналогии с алгоритмами, разработанными в [18], использовать генерацию случайных элементов скрытой группы путем возведения элементов базиса скрытой группы в случайные степени.

Этот прием позволяет вычислить значение ЭЦП, выполняя только две операции возведения в степени, значения которых предварительно вычисляются по модулю, равному порядку векторов, входящих в базис скрытой группы. При вычислении значения степеней требуется выполнить операцию обращения по указанному модулю. Если обращаемый элемент, который принимает случайные значения, окажется не взаимно простым с модулем, то потребуется повторить процедуру генерации подписи. Чтобы устранить эту проблему можно выбрать значение степени расширения *z* поля $GF(2^z)$, равное степени Мерсенна, при которой число $2^z - 1$ является простым. При использовании четырехмерных КНАА в качестве алгебраических носителей для разработки алгоритмов с различным уровнем стойкости представляет интерес рассмотрение степеней *z* в интервале значений от 100 до 400, в котором имеются только две степени Мерсенна, равные 107 и 127. Следующие по порядку возрастания степени Мерсенна равны 521 и 607.

Если использовать такие значения *z* при требуемом уровне стойкости 2^{192}, 2^{128} и менее, то это не позволит обеспечить повышение производительности при снижении задаваемого уровня стойкости. Для устранения этого ограничения заметим, что вполне приемлемы также значения *z*, при которых число $2^z - 1$ содержит только два или три больших простых делителя. С учетом того, что размер этих простых делителей должен обеспечить достаточно малую вероятность повтора процедуры генерации ЭЦП и не связан со стойкостью алгоритмов ЭЦП рассматриваемого типа, можно считать большими простые делители, размер которых превышает 24 бит. При таком подходе мы получаем

Таблица 2

Значения степени расширения поля $GF(2^z)$, представляющие интерес при разработке алгоритмов ЭЦП второго типа

Степень z	**Число простых делителей значения $2^z - 1$ (и их размер, бит)**	**Неприводимый двоичный многочлен минимального веса***
61	1 (61)	$x^{61} + x^5 + x^2 + x + 1$
89	1 (89)	$x^{89} + x^{38} + 1$
101	2 (43 и 59)	$x^{101} + x^7 + x^6 + x + 1$
103	2 (39 и 63)	$x^{103} + x^9 + 1$
107	1 (107)	$x^{107} + x^9 + x^7 + x^4 + 1$
109	2 (30 и 80)	$x^{109} + x^5 + x^4 + x^2 + 1$
127	1 (127)	$x^{127} + x + 1$
137	2 (65 и 73)	$x^{137} + x^{21} + 1$
139	2 (43 и 97)	$x^{139} + x^8 + x^5 + x^3 + 1$
149	2 (67 и 83)	$x^{149} + x^{10} + x^9 + x^7 + 1$
173	3 (41, 56 и 78)	$x^{173} + x^8 + x^5 + x^2 + 1$
199	2 (38 и 162)	$x^{199} + x^{34} + 1$
241	2 (25 и 217)	$x^{241} + x^{70} + 1$
257	3 (49, 80 и 129)	$x^{257} + x^{12} + 1$
271	2 (34 и 238)	$x^{271} + x^{58} + 1$
293	2 (86 и 208)	$x^{293} + x^{11} + x^6 + x + 1$
331	3 (44, 50 и 238)	$x^{331} + x^{10} + x^6 + x^2 + 1$
347	2 (74 и 274)	$x^{347} + x^{11} + x^{10} + x^3 + 1$
349	3 (41, >130, >150)	$x^{349} + x^6 + x^5 + x^2 + 1$
373	2 (25 и 349)	$x^{373} + x^8 + x^7 + x^2 + 1$
379	2 (38 и 342)	$x^{379} + x^{10} + x^8 + x^5 + 1$
389	3 (26, 33 и 332)	$x^{389} + x^{10} + x^9 + x^5 + 1$

* Table of Low-Weight Binary Irreducible Polynomials. https://www.hpl.hp.com/techreports/98/HPL-98-135.pdf (обращение 17 февраля 2022)

достаточно большое число пригодных для использования значений степени z, которые достаточно «удачно» распределены в интервале значений от 60 до 400. В табл. 2 приведены приемлемые значения z и соответствующие им неприводимые двоичные многочлены минимального веса.

3. Постквантовый алгоритм ЭЦП

В качестве скрытой группы в разработанном алгоритме ЭЦП используется одна из множества коммутативных групп, обладающих *двухмерной цикличностью и имеющих порядок* $\Omega_1 = (2^z - 1)^2$. Значение z выбирается по табл. 2 в зависимости от требуемого уровня стойкости. Задание скрытой группы реализуется как генерация базиса<**G**, **H**>, включающего два перестановочных вектора одного и того же порядка, равного значению $q = 2^z - 1$. Алгоритм генерации случайного базиса<**G**, **H**> описывается следующим образом:

1. Сгенерировать случайный обратимый вектор **V** порядка $q = 2^z - 1$.

2. Если вектор **V** содержится в множестве скалярных векторов, то перейти к шагу 1.

3. Сгенерировать случайное целое число k $(0 < k < q)$ и случайный двоичный многочлен $\beta \in GF(2^z)$ порядка $2^z - 1$.

4. Вычислить вектор $\mathbf{H} = \beta\mathbf{V}^k$.

5. Взять в качестве базиса скрытой группы пару векторов **H** и **G** = **V**.

Этот алгоритм может быть применен в случае использования КНАА различных типов и размерностей в качестве алгебраического носителя схемы ЭЦП со скрытой группой, если они содержат достаточно большое число коммутативных групп с двухмерной цикличностью. В случае КНАА, заданной по табл. 1, этот факт установлен исследованием ее строения. Аналогичное исследование может быть выполнено для произвольных четырехмерных КНАА с глобальной двухсторонней единицей. Детальное изучение строения КНАА размерности $m \geq 6$ достаточно проблематично. Однако для многих частных случаев КНАА с глобальной двухсторонней единицей может быть показано теоретически, что они содержат коммутативные группы с двухмерной цикличностью. Наличие многочисленных автоморфизмов в таких КНАА означает существование в этих алгебрах многочисленных коммутативных групп с двухмерной цикличностью. Таким образом, предлагаемый алгоритм генерации случайного базиса скрытой группы с двухмерной цикличностью имеет применение для достаточно широкого круга алгебраических носителей алгоритмов ЭЦП со скрытой группой.

В предлагаемом алгоритме ЭЦП операция умножения в поле GF(2^z) выполняется по модулю неприводимого двоичного многочлена степени *z*, выбираемого по табл. 2, а генерация открытого ключа выполняется в соответствии со следующей процедурой.

Процедура формирования открытого ключа:

1. Сгенерировать базис <**G**, **H**> примарной коммутативной группы порядка $q^2 = (2^z - 1)^2$, обладающей двухмерной цикличностью.

2. Используя условие обратимости (2), сгенерировать случайные обратимые векторы **A**, **B**, **D**, и **F**, которые удовлетворяют следующим неравенствам $\mathbf{AB} \neq \mathbf{BA}$, $\mathbf{AD} \neq \mathbf{DA}$, $\mathbf{AF} \neq \mathbf{FA}$, $\mathbf{AG} \neq \mathbf{GA}$, $\mathbf{BD} \neq \mathbf{DB}$, $\mathbf{BF} \neq \mathbf{FB}$, $\mathbf{BG} \neq \mathbf{GB}$, $\mathbf{DF} \neq \mathbf{FD}$,$\mathbf{DG} \neq \mathbf{GD}$ и $\mathbf{FG} \neq \mathbf{GF}$.

3. Вычислить векторы $\mathbf{A}^{-1}$,$\mathbf{B}^{-1}$,$\mathbf{D}^{-1}$ и $\mathbf{F}^{-1}$.

4. Сгенерировать случайные неотрицательные целые числа $\mathbf{x} < \mathbf{q}$ и $\mathbf{w} < \mathbf{q}$. Затем вычислить открытый ключ в виде шестерки векторов ($\mathbf{Y}_1$, $\mathbf{Z}_1$, $\mathbf{Y}_2$, $\mathbf{Z}_2$, $\mathbf{Y}_3$, **T**) по формулам:

$$\mathbf{Y}_1 = \mathbf{AGB};\ \mathbf{Z}_1 = \mathbf{DHA}^{-1};\ \mathbf{Y}_2 = \mathbf{FH}^x\mathbf{B};$$
$$\mathbf{Z}_2 = \mathbf{DH}^w\mathbf{GF}^{-1};\ \mathbf{Y}_3 = \mathbf{AG}^w\mathbf{B};\mathbf{T} = \mathbf{DG}^x\mathbf{HB}. \quad (3)$$

Секретным ключом является набор значений *x*, *w* , **G**, **H**, **A**, **B**, **D** и **F**. Вычисление ЭЦП к некоторому электронному документу *M* выполняется с использованием секретного ключапо следующему алгоритму.

Алгоритм генерации ЭЦП.

1. Сгенерировать случайные неотрицательные целые числа $k < q$ и $t < q$ и вычислить вектор

$$\mathbf{R} = \mathbf{AG}^k\mathbf{H}^t\mathbf{F}^{-1}. \quad (4)$$

2. Используя некоторую специфицированную 2*z*-битную хэш-функцию *f*, вычислить первый элемент ЭЦП $e = e_1 \| e_2 = f(M, \mathbf{R})$, где хэш-значение *e* представлено как конкатенация двух *z*-битных целых чисел e_1 и e_2.

3. Вычислить натуральные числа *n* и *d*:

$$n = \frac{k - e_1 - xe_1 - e_2 - w - 1}{2e_1 + e_2 + 1} \bmod q; \quad (5)$$

$$d = \frac{t - 2e_1 - xe_2 - we_2 - w}{2e_1 + e_2 + 1} \bmod q. \quad (6)$$

4. Вычислить второй элемент подписи в виде вектора **S**:

$$\mathbf{S} = \mathbf{B}^{-1}\mathbf{G}^n\mathbf{H}^d\mathbf{D}^{-1}. \quad (7)$$

Подписью к документу *M* является пара (*e*, **S**), т. е. хэш-значение *e* и вектор **S**. Длина подписи равна 6*z* бит. Вычислительная сложность алгоритма генерации ЭЦП примерно равна 4 операциям возведения в *z*-битную степень в КНАА, используемой в качестве алгебраического носителя (или 48*z* умножений по модулю неприводимого двоичного многочлена степени *z*, указанного в табл. 2).

Верификация ЭЦП к документу *M* осуществляется по открытому ключу ($\mathbf{Y}_1$, $\mathbf{Z}_1$, $\mathbf{Y}_2$, $\mathbf{Z}_2$, $\mathbf{Y}_3$, **T**) в соответствии со следующей вычислительной процедурой.

Алгоритм проверки подлинности ЭЦП.

1. Вычислить вектор

$$\mathrm{R}' = \left(\mathrm{Y}_1\mathrm{STSZ}_1\right)^{e_1}\ \mathrm{Y}_3\mathrm{SZ}_2\left(\mathrm{Y}_2\mathrm{SZ}_2\right)^{e_2} \quad (8)$$

2. Вычислить значение *e'* хэш-функции *f*от документа *M* с присоединенным к нему вектором **R**': *e'*= *f*(*M*, **R**').

3. Если *e'*= *e*, то подпись признается подлинной, иначе она отвергается.

Вычислительная сложность алгоритма верификации ЭЦП примерно равна 2 операциям возведения четырехмерных векторов в *z*-битную степень (или 24*z* умножений по модулю неприводимого двоичного многочлена).

Корректность работы описанной схемы ЭЦП доказывается путем демонстрации того, что подпись, сформированная в соответствии с алгоритмом генерации ЭЦП, проходит процедуру верификации как подлинная подпись.

Доказательство корректности.

Вычислим значения

$$\mathrm{J}_1 = \left(\mathrm{Y}_1\mathrm{STSZ}_1\right)^{e_1} = \left(\mathrm{AGBB}^{-1}\mathrm{G}^n\mathrm{H}^d\mathrm{D}^{-1} \times \right.$$
$$\left. \times \mathrm{DG}^x\mathrm{HBB}^{-1}\mathrm{G}^n\mathrm{H}^d\mathrm{D}^{-1}\mathrm{DHA}^{-1}\right)^{e_1} =$$
$$= \left(\mathrm{AGG}^n\mathrm{H}^d\mathrm{G}^x\mathrm{HG}^n\mathrm{H}^d\mathrm{HA}^{-1}\right)^{e_1} =$$
$$= \left(\mathrm{AG}^{2n+x+1}\mathrm{H}^{2d+2}\mathrm{A}^{-1}\right)^{e_1} =$$
$$= \mathrm{AG}^{2ne_1+xe_1+e_1}\mathrm{H}^{2de_1+2e_1}\mathrm{A}^{-1};$$

$$J_2 = Y_3SZ_2 = AG^wBB^{-1}G^nH^dD^{-1}DH^wGF^{-1} = \\ = AG^{n+w+1}H^{d+w}F^{-1};$$

$$J_3 = \left(Y_2SZ_2\right)^{e_2} = \\ = \left(FH^xBB^{-1}G^nH^dD^{-1}DH^wGF^{-1}\right)^{e_2} = \\ = \left(FG^{n+1}H^{d+x+w}F^{-1}\right)^{e_2} = \\ = FG^{ne_2+e_2}H^{de_2+xe_2+we_2}F^{-1};$$

Затем вычислим значение **R′**:

$$R' = J_1J_2J_3 = AG^{2ne_1+xe_1+e_1}H^{2de_1+2e_1}A^{-1} \times \\ \times AG^{n+w+1}H^{d+w}F^{-1} \times \\ \times FG^{ne_2+e_2}H^{de_2+xe_2+we_2}F^{-1} = \\ = AG^{2ne_1+xe_1+e_1+n+w+1+ne_2+e_2} \times \\ \times H^{2de_1+2e_1+d+w+de_2+xe_2+we_2}F^{-1} = \\ = AG^{n(2e_1+e_2+1)+e_1+xe_1+e_2+w+1} \times \\ \times H^{d(2e_1+e_2+1)+2e_1+xe_2+we_2+w}F^{-1}.$$

$$R' = AG^kH^tF^{-1} = R \Rightarrow \\ \Rightarrow f\left(M \| R'\right) = f\left(M \| R\right) \Rightarrow \\ \Rightarrow e' = e.$$

В соответствии с процедурой верификации ЭЦП последнее равенство означает подлинность подписи, т. е. корректность предложенного постквантового алгоритма ЭЦП доказана.

4. Обсуждение

Разработанный алгоритм ЭЦП со скрытой группой основан на вычислительной сложности решения систем многих квадратных уравнений с многими неизвестными и представляет собой частную реализацию недавно предложенной концепции построения постквантовых схем ЭЦП на КНАА [16], отличающейся использованием проверочного уравнения с несколькими вхождениями значения подписи. В ранее предложенных в работе [18] частных реализациях упомянутой концепции в качестве алгебраического носителя используются КНАА, заданные над простыми полями. В данной статье впервые рассмотрены особенности использования КНАА, заданных над конечными полями характеристики два, что потенциально обеспечивает дополнительное повышение производительности алгоритмов ЭЦП со скрытой группой и снижение схемотехнической сложности их аппаратной реализации при заданном уровне стойкости.

Детальная оценка значения стойкости требует рассмотрения конкретной системы квадратных уравнений, вытекающей из формул (3) и условий перестановочности элементов скрытой группы, входящих в формулы (3). Однако для предварительной оценки ожидаемой стойкости алгоритмов, основанных на вычислительной трудности решения систем многих квадратных уравнений, включая алгоритмы ЭЦП, разработанные в рамках концепции [16], и двухключевые алгоритмы многомерной криптографии [17], представляет интерес неформальный показатель уровня стойкости Ψ, предложенный в [18] как произведение двоичного логарифма от порядка поля, над которым заданы уравнения, на число неизвестных.

Алгоритмы ЭЦП с примерно одинаковыми значениями показателя Ψ могут быть отнесены к одному уровню ожидаемой стойкости (к атакам, направленным на вычисление секретного ключа). Применение этого неформального показателя не могут заменить детальное исследование стойкости каждого отдельного алгоритма ЭЦП (включая атаки с использованием коллизий хэш-функции), но представляет интерес для получения экспрессных сравнительных оценок. С учетом разрядности значения используемой хэш-функции, равной $2z$, можно оценить, что предложенный алгоритм ЭЦП обеспечивает z-битную стойкость к атакам на основе парадокса о днях рождения (формирование двух документов с одинаковым значением хэш-функции).

В отличии от двухключевых алгоритмов многомерной криптографии, для которых является возможным такое их построение, при котором число квадратных уравнений может быть меньше, равно или больше числа неизвестных, в алгоритмах ЭЦП, построенных в соответствии с концепцией [16], требуется задать число квадратных уравнений равное или большее числа неизвестных. В случае разработанного алгоритма ЭЦП со скрытой группой, использующего в качестве алгебраического носителя четырехмерную КНАА, заданную над конечными полями характеристики два, имеем систему из 11 квадратных векторных уравнений (6 уравнений задаются формулами (3) и еще 5 уравнений задаются условием перестановочности следующих шести неизвестных векторов **G**, **H**, **H′**= $\mathbf{H}^x$, **H″** = $\mathbf{H}^w\mathbf{G}$, **G′** = $\mathbf{G}^w$ и **G″** = $\mathbf{G}^x\mathbf{H}$) с 10 неизвестными векторами (включая попарно неперестановочные векторы **A**, **B**, **D**, и **F**).

Последняя система сводится к системе из 44 квадратных уравнений в поле $GF(2^z)$ с 40 неизвестными (которыми являются координаты неизвестных векторов). С учетом этого получаем значение неформального показателя стойкости $\Psi = 40z$, которое существенно больше значения Ψ для следующих извест-

Таблица 3

Параметры предложенного постквантового алгоритма при различных значениях z

Степень z	Размер ЭЦП, байт	Размер открытого ключа, байт	Размер секретного ключа, байт
107	81	321	348
127	95	381	413
149	112	447	497
173	130	619	663
257	193	771	836

Таблица 4

*Вычислительная сложность (*в умножениях в поле $GF(2^{107})$) процедур генерации и верификации ЭЦП при различных значениях z.*

Степень z	Генерация ЭЦП, умножений*	Верификация ЭЦП, умножений*	Значение ψ
107	5136	2568	4280
127	8595	4297	5080
149	13875	6937	5960
173	21707	10853	6920
257	71179	35589	10280

ных постквантовых алгоритмов ЭЦП, основанных на вычислительной трудности решения систем квадратных уравнений: Rainbow[7] (от $\Psi = 384$ до $\Psi = 1632$ для разных версий этого алгоритма) и QUARTZ[8] ($\Psi = 428$).

В предложенном алгоритме предполагается выбор различных значений степени расширения *z*, для обеспечения различных значений требуемого уровня стойкости. Значение *z* влияет на размер открытого ключа, секретного ключа и подписи, а также на вычислительную сложность процедур генерации и верификации ЭЦП, что отражено в табл. 3 и табл. 4.

Выводы

В рамках концепции [16] разработан новый постквантовый алгебраический алгоритм ЭЦП со скрытой группой. Впервые в качестве алгебраического носителя алгоритмов такого типа использованы четырехмерные КНАА, заданные над конечными полями характеристики два. Показано, что благодаря некритичному влиянию факторизации порядка скрытой группы на стойкость алгоритма, имеются достаточно широкие возможности выбора полей $GF(2^z)$ с различными степенями расширения для задания над ними КНАА, представляющих практический интерес для использования в качестве алгебраического носителя. Реализация КНАА над полями $GF(2^z)$ является существенным моментом для повышения производительности и снижения схемотехнической сложности аппаратной реализации постквантовых алгоритмов ЭЦП со скрытой группой по сравнению с аналогичными реализациями над простыми конечными полями $GF(p)$.

Дополнительное повышение производительности может быть достигнуто переходом к использованию в качестве алгебраического носителя шестимерных и восьмимерных КНАА, заданных над полями $GF(2^z)$ с размерами степени расширения *z* от 56 до 137 бит, включая случай задания КНАА по

7 Rainbow Signature. One of three NIST Post-quantum Signature Finalists [on line] 2021. https://www.pqcrainbow.org/ (обращение 17 февраля 2022)

8 Jintai D., Dieter S.Multivariable Public Key Cryptosystems (2004) https://eprint.iacr.org/2004/350.pdf (обращение 17 февраля 2022)

прореженным ТУББ. Однако это представляет собой предмет самостоятельного исследования, включающего вопросы изучения строения указанных алгебр и разработки прореженных ТУББ для задания ассоциативного умножения шестимерных и восьмимерных векторов.

Литература

1. Yan S.Y. Quantum Computational Number Theory. – Springer International Publishing. 2015. – 252 p. DOI: 10.1007/978-3-319-25823-2.
2. Yan S.Y. Quantum Attacks on Public-Key Cryptosystems . – Springer. 2013. – 207 p. DOI: 10.1007/978-1-4419-7722-9.
3. Kuzmin A.S., Markov V.T., Mikhalev A.A., Mikhalev A.V., Nechaev A.A. Cryptographic Algorithms on Groups and Algebras // Journal of Mathematical Sciences. 2017. V. 223. N. 5. P. 629–641.
4. Moldovyan D.N. Post-quantum public key-agreement scheme based on a new form of the hidden logarithm problem // Computer Science Journal of Moldova. 2019. V.27. No.1(79). P. 56-72.
5. Alamelou Q., Blazy O., Cauchie S., Gaborit Ph. A code-based group signature scheme // Designs, Codes and Cryptography. 2017. V. 82. N. 1–2. P. 469-493. DOI: 10.1007/s10623-016-0276-6.
6. Kosolapov Y.V., Turchenko O.Y. On the construction of a semantically secure modification of the McEliece cryptosystem // Прикладная дискретная математика. 2019. № 45. С. 33–43. DOI: 10.17223/20710410/45/4.
7. Hoffstein J., Pipher J., Schanck J.M., Silverman J.H., Whyte W., Zhang Zh. Choosing parameters for NTRU Encrypt. Cryptographers› Track at the RSA Conference - CTA-RSA 2017 // Lecture Notes in Computer Science. Springer, 2017. V. 10159. P. 3–18.
8. Agibalov G.P. ElGamal cryptosystems on Boolean functions // Прикладная дискретная математика. 2018. № 42. С. 57–65. DOI: 10.17223/20710410/42/4.
9. Alagic, G., Alperin-Sheriff, J., Apon, D., Cooper, D., Dang, Q., Miller, C., Moody, D., Peralta, R., Perlner, R., Robinson, A., Smith-Tone, D. and Liu, Y. (2019), Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process, NIST Interagency/Internal Report (NISTIR 8240), National Institute of Standards and Technology, Gaithersburg, MD, [online]. https://doi.org/10.6028/NIST.IR.8240/https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=927303 (обращение 17 февраля 2022)
10. Moody, D., Alagic, G., Apon, D., Cooper, D., Dang, Q., Kelsey, J., Liu, Y., Miller, C., Peralta, R., Perlner, R., Robinson, A., Smith-Tone, D. and Alperin-Sheriff, J. (2020), Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process, NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.IR.8309 (обращение 17 февраля 2022)
11. Moody, D. NIST Status Update on the 3rd Round. Available at: https://csrc.nist.gov/CSRC/media/Presentations/status-update-on-the-3rd-round/images-media/session-1-moody-nist-round-3-update.pdf (обращение 17 февраля 2022).
12. Moldovyan D.N. New Form of the Hidden Logarithm Problem and Its Algebraic Support // Bulletin of Academy of Sciences of Moldova. Mathematics. 2020. N. 2(93). P.3-10.
13. Moldovyan D.N. A practical digital signature scheme based on the hidden logarithm problem // Computer Science Journal of Moldova. 2021. V. 29. N. 2(86). P. 206–226.
14. Moldovyan N. A., Moldovyan A.A. Candidate for practical post-quantum signature scheme // Вестник Санкт-Петербургского университета. Прикладная математика. Информатика. Процессы управления. 2020. Т. 16. Вып. 4. С. 455–461. DOI: 10.21638/11701/spbu10.2020.410.
15. Moldovyan D.N., Moldovyan A.A., Moldovyan N.A. An enhanced version of the hidden discrete logarithm problem and its algebraic support // Quasigroups and Related Systems. 2020. V. 28. N. 2. P. 269-284.
16. Молдовян Д.Н., Молдовян А.А., Молдовян Н.А. Новая концепция разработки постквантовых алгоритмов цифровой подписи на некоммутативных алгебрах // Вопросы кибербезопасности. 2022. № 1(47). С. 18–25. DOI: 10.21681/2311-3456-2022-1-18-25.
17. Shuaiting Q., Wenbao H., Yifa Li, Luyao J. Construction of Extended Multivariate Public Key Cryptosystems // International Journal of Network Security. 2016. V. 18. N. 1. P. 60-67.
18. Молдовян Д.Н., Молдовян А.А. Алгебраические алгоритмы ЭЦП, основанные на трудности решения систем уравнений // Вопросы кибербезопасности. 2022. № 2(48). С. 7–17. DOI: 10.21681/2311-3456-2022-2-7-17.
19. Moldovyan N.A. Signature Schemes on Algebras, Satisfying Enhanced Criterion of Post-quantum Security // Bulletin of Academy of Sciences of Moldova. Mathematics. 2020. N. 2 (93). P. 62-67.
20. Moldovyan D.N. A unified method for setting finite non-commutative associative algebras and their properties // Quasigroups and Related Systems. 2019. V.27. N.2. P. 293-308

SIGNATURE ALGORITHMS ON FINITE NON-COMMUTATIVE ALGEBRAS OVER FIELDS OF CHARACTERISTIC TWO

Moldovyan A.A.[9] and Moldovyan N.A.[10]

Abstract

Purpose *of work is the increase in performance and decrease in the hardware implementation cost of the of post-quantum algebraic signature algorithms based on the computational difficulty of solving systems of many quadratic equations with many unknowns.*

Research method *is i) the development of post-quantum signature algorithms on finite non-commutative associative algebras defined over finite fields of characteristic two, which have high performance and small sizes of signature and public and secret keys; ii) using the concept of constructing algebraic signature algorithms with a hidden commutative group, characterized by the use of a power-type vector verification equation with multiple occurrences of the signature S as a factor; iii) the choice of the degree of extension z of the field GF(2z) in which the order of the hidden group is divisible only by prime divisors of at least 24 bits.*

Results *of the study are the formulated main provisions for the implementation of post-quantum signature algorithms with a hidden group, the security of which is based on the computational difficulty of solving systems of many quadratic equations with many unknowns, when using the finite non-commutative algebras given over the GF(2z) fields as algebraic support. The values of the extension degree z are established for which the order of the hidden commutative group is divisible only by prime divisors of a sufficiently large size. A new post-quantum signature algorithm with relatively high performance and small sizes of the signature and public and secret keys have been developed. Using an informal security index in the form of a product of the binary logarithm of the order of the field and the number of unknowns, the developed and known post-quantum algorithms for a given level of security are compared.*

Practical relevance. *The main provisions for constructing signature algorithms with a hidden group are formulated for the case of using finite non-commutative algebras with computationally efficient operations of multiplication and exponentiation, providing prerequisites for improving performance and reducing the hardware implementation cost of post-quantum signature algorithms.*

Keywords: *finite non-commutative algebra; associative algebra; computationally difficult problem; hidden commutative group; digital signature; multivariate cryptography; post-quantum cryptography*

References

1. Yan S.Y. Quantum Computational Number Theory. – Springer International Publishing. 2015. – 252 p. DOI: 10.1007/978-3-319-25823-2.
2. Yan S.Y. Quantum Attacks on Public-Key Cryptosystems . – Springer. 2013. – 207 p. DOI: 10.1007/978-1-4419-7722-9.
3. Kuzmin A.S., Markov V.T., Mikhalev A.A., Mikhalev A.V., Nechaev A.A. Cryptographic Algorithms on Groups and Algebras // Journal of Mathematical Sciences. 2017. V. 223. N. 5. P. 629–641.
4. Moldovyan D.N. Post-quantum public key-agreement scheme based on a new form of the hidden logarithm problem // Computer Science Journal of Moldova. 2019. V.27. No.1(79). P. 56-72.
5. Alamelou Q., Blazy O., Cauchie S., Gaborit Ph. A code-based group signature scheme // Designs, Codes and Cryptography. 2017. V. 82. N. 1-2. P. 469-493. DOI: 10.1007/s10623-016-0276-6.
6. Kosolapov Y.V., Turchenko O.Y. On the construction of a semantically secure modification of the McEliece cryptosystem // Prikladnaja diskretnaja matematika. 2019. № 45. S. 33–43. DOI: 10.17223/20710410/45/4.
7. Hoffstein J., Pipher J., Schanck J.M., Silverman J.H., Whyte W., Zhang Zh. Choosing parameters for NTRU Encrypt. Cryptographers' Track at the RSA Conference - CTA-RSA 2017 // Lecture Notes in Computer Science. Springer, 2017. V. 10159. P. 3–18.
8. Agibalov G.P. ElGamal cryptosystems on Boolean functions // Prikladnaja diskretnaja matematika. 2018. № 42. S. 57–65. DOI: 10.17223/20710410/42/4.

9 Alexander A. Moldovyan, Dr.Sc.(in Tech.) chief researcher of laboratory of cybersecurity and post-quantum cryptosystems, St. Petersburg Federal Research Center of the Russian Academy of Sciences, St. Petersburg, Russia. E-mail: maa1305@yandex.ru

10 Nikolay A. Moldovyan, Dr.Sc. (in Tech.) chief researcher of laboratory of cybersecurity and post-quantum cryptosystems, St. Petersburg Federal Research Center of the Russian Academy of Sciences, St. Petersburg, Russia. E-mail: nmold@mail.ru

9. Alagic, G., Alperin-Sheriff, J., Apon, D., Cooper, D., Dang, Q., Miller, C., Moody, D., Peralta, R., Perlner, R., Robinson, A., Smith-Tone, D. and Liu, Y. (2019), Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process, NIST Interagency/Internal Report (NISTIR 8240), National Institute of Standards and Technology, Gaithersburg, MD, [online]. https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=927303 (obrashhenie 17 fevralja 2022) https://doi.org/10.6028/NIST.IR.8240/
10. Moody, D., Alagic, G., Apon, D., Cooper, D., Dang, Q., Kelsey, J., Liu, Y., Miller, C., Peralta, R., Perlner, R., Robinson, A., Smith-Tone, D. and Alperin-Sheriff, J. (2020), Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process, NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.IR.8309 (obrashhenie 17 fevralja 2022)
11. Moody, D. NIST Status Update on the 3rd Round. Available at: https://csrc.nist.gov/CSRC/media/Presentations/status-update-on-the-3rd-round/images-media/session-1-moody-nist-round-3-update.pdf (obrashhenie 17 fevralja 2022).
12. Moldovyan D.N. New Form of the Hidden Logarithm Problem and Its Algebraic Support // Bulletin of Academy of Sciences of Moldova. Mathematics. 2020. N. 2(93). P.3-10.
13. Moldovyan D.N. A practical digital signature scheme based on the hidden logarithm problem // Computer Science Journal of Moldova. 2021. V. 29. N. 2(86). P. 206–226.
14. Moldovyan N. A., Moldovyan A.A. Candidate for practical post-quantum signature scheme // Vestnik Sankt-Peterburgskogo universiteta. Prikladnaja matematika. Informatika. Processy upravlenija. 2020. T. 16. Vyp. 4. S. 455–461. DOI: 10.21638/11701/spbu10.2020.410.
15. Moldovyan D.N., Moldovyan A.A., Moldovyan N.A. An enhanced version of the hidden discrete logarithm problem and its algebraic support // Quasigroups and Related Systems. 2020. V. 28. N. 2. P. 269-284.
16. Moldovjan D.N., Moldovjan A.A., Moldovjan N.A. Novaja koncepcija razrabotki postkvantovyh algoritmov cifrovoj podpisi na nekommutativnyh algebrah // Voprosy kiberbezopasnosti. 2022. № 1(47). S. 18–25. DOI: 10.21681/2311-3456-2022-1-18-25.
17. Shuaiting Q., Wenbao H., Yifa Li, Luyao J. Construction of Extended Multivariate Public Key Cryptosystems // International Journal of Network Security. 2016. V. 18. N. 1. P. 60-67.
18. Moldovjan D.N., Moldovjan A.A. Algebraicheskie algoritmy JeCP, osnovannye na trudnosti reshenija sistem uravnenij // Voprosy kiberbezopasnosti. 2022. № 2(48). S. 7–17. DOI: 10.21681/2311-3456-2022-2-7-17.
19. Moldovyan N.A. Signature Schemes on Algebras, Satisfying Enhanced Criterion of Post-quantum Security // Bulletin of Academy of Sciences of Moldova. Mathematics. 2020. N. 2 (93). P. 62-67.
20. Moldovyan D.N. A unified method for setting finite non-commutative associative algebras and their properties // Quasigroups and Related Systems. 2019. V.27. N.2. P. 293-308