Порождение квадратичных квазигрупп с помощью правильных семейств булевых функций

А. В. ГАЛАТЕНКО
Московский государственный университет им. М. В. Ломоносова
e-mail: agalat@msu.ru

В. А. НОСОВ
Московский государственный университет им. М. В. Ломоносова
e-mail: vnosov40@mail.ru

А. Е. ПАНКРАТЬЕВ
Московский государственный университет им. М. В. Ломоносова
e-mail: apankrat@intsys.msu.ru

УДК 512.548.7+519.143+519.716.32

Ключевые слова: квадратичные квазигруппы, правильные семейства булевых функций.

Аннотация

В работе исследуется построение квадратичных квазигрупп с помощью правильных семейств булевых функций.

Abstract

A. V. Galatenko, V. A. Nosov, A. E. Pankratiev, Generation of multivariate quadratic quasigroups by proper families of Boolean functions, Fundamentalnaya i prikladnaya matematika, vol. 23 (2020), no. 2, pp. 57—73.

This paper is devoted to the generation of multivariate quadratic quasigroups with the use of proper families of Boolean functions.

Памяти Виктора Тимофеевича Маркова

1. Введение

В последние десятилетия наблюдается значительный интерес к многомерной (как правило, квадратичной) криптографии (см., например, [8, 21]). Это связано с тем, что алгоритмы шифрования с открытым ключом и электронной подписи, основанные на многомерных конструкциях, обладают высоким быстродействием, порождают подписи небольшой длины (отметим, что открытые

Фундаментальная и прикладная математика, 2020, том 23, № 2, с. 57—73.
© 2020 *Национальный Открытый Университет «ИНТУИТ»*

ключи, напротив, велики), а также способны противостоять квантовым атакам. В частности, по результатам первого тура выборов стандарта постквантовой криптографии, организованных американским Национальным институтом стандартов и технологий, для дальнейшего анализа был отобран целый ряд многомерных квадратичных алгоритмов [5].

В [11, 12] была предложена система с открытым ключом, основанная на многомерных квадратичных квазигруппах. В [9, 16] система была успешно атакована, после чего исходная конструкция была доработана и преобразована в алгоритм электронной подписи [13]. Одним из параметров алгоритма является многомерная квадратичная квазигруппа (в дальнейшем для краткости слово «многомерная» будет опускаться). Для построения таких квазигрупп имеется ряд известных методов, описанных в разделе 3. Мы предлагаем новый метод, основанный на применении правильных семейств булевых функций. Новая конструкция позволяет порождать большие семейства квадратичных квазигрупп сколь угодно высокого порядка, в том числе и сильно квадратичные квазигруппы, не порождаемые другими известными методами.

Дальнейшее изложение организовано следующим образом. В разделе 2 вводятся необходимые определения. В разделе 3 описываются известные конструкции для порождения квадратичных квазигрупп. В разделе 4 разбирается случай линейных правильных семейств, в разделе 5 анализируются квадратичные треугольные семейства. Раздел 6 посвящён использованию конструкции треугольного расширения. Наконец, раздел 7 является заключением.

Авторы благодарят профессора В. А. Артамонова за ценные замечания и внимание к работе.

Работа поддержана грантом QGSEC.

2. Основные определения

Определение 1. Конечной квазигруппой называется конечное множество Q с заданной на нём бинарной операцией f, такой что для любых a и b из Q уравнения $f(x,a)=b$ и $f(a,y)=b$ однозначно разрешимы.

Определение 2. Пусть Q — конечное множество, (Q,f_1) и (Q,f_2) — пара квазигрупп. Квазигруппы называются изотопными, если существуют перестановки α, β, γ на множестве Q, такие что выполнено тождество

$$f_2(x,y)\equiv\gamma^{-1}\Big(f_1\big(\alpha(x),\beta(y)\big)\Big).$$

Операция перехода от f_1 к f_2 называется изотопией.

В дальнейшем для краткости слово «конечный» будет опускаться.

Пусть $|Q|=2^n$ для некоторого $n\in\mathbb{N}$. Тогда без ограничения общности можно считать, что множество Q состоит из двоичных наборов длины n, а запись $z=f(x,y)$ может быть представлена в виде

$$\begin{aligned} z_1 &= f_1(x_1,\dots,x_n,y_1,\dots,y_n),\\ z_2 &= f_2(x_1,\dots,x_n,y_1,\dots,y_n),\\ &\vdots\\ z_n &= f_n(x_1,\dots,x_n,y_1,\dots,y_n), \end{aligned} \tag{1}$$

где $f_1,\dots,f_n$ — булевы функции. Известно, что любая булева функция может быть однозначно представлена многочленом Жегалкина (см., например, [15, часть II, теорема 1.4.3]). Таким образом, каждой функции f_i, $i=1,\dots,n$, можно однозначно поставить в соответствие степень d_i представляющего эту функцию полинома.

Определение 3. Квазигруппа (Q,f) называется квадратичной типа $\mathrm{Quad}_k\mathrm{Lin}_{n-k}$, $k\in\{1,\dots,n\}$, если ровно k функций f_i квадратичны, а оставшиеся $n-k$ функций линейны.

Известно, что решение системы квадратных уравнений является NP-сложной задачей [10, с. 251]. Однако если в системе есть линейные уравнения, из них можно выразить несколько переменных, понизив таким образом порядок системы. Число линейных уравнений может быть увеличено за счёт рассмотрения линейных комбинаций уравнений. Для отражения «реальной нелинейности» в [6] было введено определение строгого типа.

Определение 4. Квазигруппа (Q,f) называется квадратичной строгого типа $\mathrm{Quad}^s_k\mathrm{Lin}^s_{n-k}$, $k\in\{1,\dots,n\}$, если максимальное число квадратичных f_i, не допускающих нетривиальные линейные комбинации, являющиеся линейными функциями, равно k.

Квадратичные квазигруппы строгого типа $\mathrm{Quad}^s_n\mathrm{Lin}^s_0$ в дальнейшем будут называться сильно квадратичными.

Заметим, что задание квадратичных квазигрупп формулами существенно более компактно, чем табличное задание: таблица занимает $n2^{2n}$ бит, тогда как формула может быть определена битовой маской коэффициентов при квадратичных, линейных и константных членах, т. е. потребуется $2n^3+n^2+n$ бит. Действительно, число квадратичных мономов от $2n$ переменных равно $n(2n-1)$, т. е. $2n^2-n$, число линейных мономов равно $2n$, свободный член один. Таким образом, каждая из n функций потребует $2n^2+n+1$ бит.

Конструкция может быть естественным образом обобщена на случай многочленов над произвольным конечным полем.

Теперь рассмотрим следующий частный случай соотношений (1):

$$\begin{aligned} z_1 &= x_1\oplus y_1\oplus g_1\big(\pi_1(x_1,y_1),\dots,\pi_n(x_n,y_n)\big),\\ z_2 &= x_2\oplus y_2\oplus g_2\big(\pi_1(x_1,y_1),\dots,\pi_n(x_n,y_n)\big),\\ &\vdots\\ z_n &= x_n\oplus y_n\oplus g_n\big(\pi_1(x_1,y_1),\dots,\pi_n(x_n,y_n)\big), \end{aligned} \tag{2}$$

где $\oplus$ означает сложение по модулю 2, $g_1, \ldots, g_n$ — булевы функции от n переменных, $\pi_1, \ldots, \pi_n$ — булевы функции от двух переменных.

Определение 5. Семейство $(g_1, \ldots, g_n)$ n-местных булевых функций называется правильным, если для любой пары различных наборов $s, t \in \{0,1\}^n$, $s = (s_1, \ldots, s_n)$, $t = (t_1, \ldots, t_n)$, найдётся индекс i, $1 \leqslant i \leqslant n$, такой что $s_i \neq t_i$ и $g_i(s) = g_i(t)$.

Из определения немедленно следует, что переменная с номером i фиктивна для g_i.

Очевидно, что если все функции g_i являются константами, семейство правильное.

Определение 6. Семейство $(g_1, \ldots, g_n)$ n-местных булевых функций называется треугольным, если с точностью до согласованной перенумерации переменных и функций оно имеет вид

$$\begin{aligned} g_1 &\equiv \mathrm{const}, \\ g_2 &= g_2(x_1), \\ &\vdots \\ g_n &= g_n(x_1, \ldots, x_{n-1}), \end{aligned} \tag{3}$$

т. е. каждая функция может существенно зависеть только от переменных с меньшими номерами.

Несложно убедиться, что любое треугольное семейство правильное.

Правильные семейства играют важную роль в порождении квазигрупп.

Теорема [2]. *Соотношения* (2) *задают квазигрупповую операцию для любых* $\pi_1, \ldots, \pi_n$ *тогда и только тогда, когда семейство* $(g_1, \ldots, g_n)$ *правильное.*

В булевой алгебре выполняется тождество $x \cdot x \equiv x$, поэтому все функции двух переменных задаются не более чем квадратичными полиномами. Таким образом, возникает две естественные конструкции для порождения квадратичных квазигрупп с помощью правильных семейств:

— использовать линейные правильные семейства и произвольные функции π_i;

— использовать квадратичные правильные семейства и не более чем линейные функции π_i.

В обоих случаях потребуется аккуратно отсеять вырожденные случаи (так, подстановка констант вместо всех функций π_i в соотношения (2) при любом правильном семействе порождает линейную квазигруппу).

Заметим, что для задания квадратичной квазигруппы с помощью квадратичного правильного семейства потребуется $n^3/2 + n^2/2 + 4n$ бит: существует $n(n-1)/2$ квадратичных мономов от n переменных, n линейных мономов и один свободный член, т. е. для хранения n функций g_i достаточно $n^3/2 + n^2/2 + n$ бит, и ещё $3n$ бит позволят задать n функций π_i. Таким образом, пространственная сложность снизится практически в четыре раза по сравнению с заданием (1).

В случае линейного правильного семейства пространственная сложность не превышает $n^2 + 5n$.

3. Известные методы порождения квадратичных квазигрупп

Первый алгоритм для порождения квадратичных квазигрупп был предложен в [12]. Рассматривалась пара $(n \times n)$-матриц A_1 и A_2 и пара n-мерных векторов b_1 и b_2. Элементами A_1 являлись линейные функции от переменных $x_1, \ldots, x_n$, матрица A_2 состояла из линейных функций от переменных $y_1, \ldots, y_n$; элементами b_1 и b_2 были не более чем квадратичные функции от $x_1, \ldots, x_n$ и $y_1, \ldots, y_n$ соответственно. В случае если определители матриц A_1 и A_2 тождественно равны единице и выполнено равенство

$$A_1 \cdot (y_1, \ldots, y_n)^t + b_1 = A_2 \cdot (x_1, \ldots, x_n)^t + b_2,$$

операция, определяемая формулой

$$f(x_1, \ldots, x_n, y_1, \ldots, y_n) = A_1 \cdot (y_1, \ldots, y_n)^t + b_1,$$

задаёт квадратичную квазигруппу. Алгоритм для поиска A_1, A_2, b_1, b_2 был трудоёмким и практически применимым только в случае $n \leqslant 5$.

В [4] был предложен следующий алгоритм. Сперва генерируются n случайных квадратичных многочленов $f_1, \ldots, f_n$ (дополнительно может выставляться ограничение на тип), затем производится проверка, что операция, задаваемая соотношениями (1), является квазигрупповой. В случае отрицательного результата процесс повторяется. Заметим, что в случае больших значений n число итераций может оказаться практически неприемлемым (получение точных оценок является задачей для дальнейших исследований); кроме того, в этом случае неочевидно, как эффективно по времени и памяти проверять квазигрупповое свойство. Авторы протестировали свой метод при n от 2 до 14.

В работе [20] был предложен метод порождения квадратичных квазигрупп с помощью так называемых t-квазигрупп, операция в которых имеет вид

$$\begin{aligned}
z_1 &= x_1 \oplus y_1 \oplus f_1(x_2, \ldots, x_n, y_2, \ldots, y_n),\\
z_2 &= x_2 \oplus y_2 \oplus f_2(x_3, \ldots, x_n, y_3, \ldots, y_n),\\
&\vdots\\
z_{n-1} &= x_{n-1} \oplus y_{n-1} \oplus f_{n-1}(x_n, y_n),\\
z_n &= x_n \oplus y_n \oplus \mathrm{const}.
\end{aligned}$$

В этом соотношении f_i — произвольные не более чем квадратичные функции от указанных в скобках переменных. Несложно показать, что определённая таким образом операция является квазигрупповой; если хотя бы одна из функций f_i

квадратична, квадратична и квазигруппа. Заметим, что функция f_n всегда линейна, поэтому конструкция не порождает сильно квадратичные квазигруппы. Тем не менее мощность порождаемого множества достаточно велика: она составляет $2^{2n^3/3+o(n^3)}$ (отметим, что тривиальная оценка на мощность множества всех квадратичных квазигрупп, получаемая подсчётом всех квадратичных многочленов от $2n$ переменных, равна $2^{2n^3+o(n^3)}$).

В [6, 7] описывается развитие исходного алгоритма из [12]. В уточнённом виде соотношения приняли следующий вид. Пусть f_m^{ij} и g_m^{ij}, $1 \leqslant i, j, m \leqslant n$, являются элементами множества $\{0, 1\}$, $f_m^{ik} = g_j^{im}$, $1 \leqslant i, j, m \leqslant n$. Рассмотрим матрицы

$$A_1' = \mathrm{Id}_n + [(f_1^{ij}, \ldots, f_n^{ij}) \cdot (x_1, \ldots, x_n)^t]_{n \times n}$$

и

$$A_2' = \mathrm{Id}_n + [(g_1^{ij}, \ldots, g_n^{ij}) \cdot (y_1, \ldots, y_n)^t]_{n \times n}$$

(выражения в квадратных скобках представляют собой $(n \times n)$-матрицу, в которой элемент с индексом i, j получается скалярным произведением векторов с соответствующими индексами). Пусть определители обеих матриц тождественно равны 1. Тогда для любых невырожденных $0, 1$-матриц B_1 и B_2 и любого вектора $c = (c_1, \ldots, c_n)^t$ операция

$$A_0 \cdot B_2 \cdot \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} + B_1 \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} + B_2 \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} + \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix},$$

где

$$A_0 = \left[(f_1^{ij}, \ldots, f_n^{ij}) \cdot B_1 \cdot (x_1, \ldots, x_n)^T\right]$$

задаёт квадратичную квазигруппу. Заметим, что при этом все квадратичные члены имеют вид $x_i \cdot y_j$. Таким образом, проблема сводится к выбору коэффициентов f_m^{ij}. В [6] предлагается ряд методов такого выбора, включая рекурсивную конструкцию для построения строго квадратичных квазигрупп, и приводятся нижние оценки мощности порождаемых множеств, имеющие вид $2^{dn^3+o(n^3)}$ для некоторых $d \in \mathbb{R}$.

В [19] t-квазигруппы и билинейная конструкция обобщаются на случай произвольного конечного поля.

Очевидно, что произвольное невырожденное линейное преобразование переменных x, y или z задаёт перестановку на множестве $\{0, 1\}^n$, т. е. порождает квазигруппу, изотопную исходной, причём квадратичность при этом сохраняется (как отмечено в [6], тип может меняться, строгий тип сохраняется). Таким образом, множество порождаемых квадратичных квазигрупп может быть расширено за счёт таких преобразований.

В [22,23] описаны алгоритмы проверки свойств квадратичности и порождённости описанной выше билинейной конструкцией по таблице Кэли квазигруппы

как для булева случая, так и для случая произвольного конечного поля. Заметим, что задание квазигруппы таблицей Кэли в случае больших значений n практически невозможно.

4. Линейные правильные семейства

Рассмотрим квазигруппы, порождённые линейными правильными семействами. В [18] доказано утверждение, которое можно переформулировать следующим образом.

Теорема [18]. *Семейство $(g_1, \ldots, g_n)$ линейных функций является правильным тогда и только тогда, когда оно треугольное.*

Следствием этого утверждения является следующий факт.

Теорема 1. *Число квадратичных квазигрупп типа* $\mathrm{Quad}_{n-k}\mathrm{Lin}_k$, $0 < k < n$, *порождаемых линейными правильными семействами, равно* $2^{n^2/2+o(n^2)}$.

Доказательство. Сперва докажем верхнюю оценку. Рассмотрим систему функций, заданную соотношениями (3). Функция номер i может быть выбрана 2^i способами ($i-1$ коэффициент при переменных $x_1, \ldots, x_{i-1}$ и свободный член). Таким образом, общее число линейных правильных семейств, не требующих перенумерации, равно

$$2^1 \cdot 2^2 \cdot \ldots \cdot 2^n = 2^{1+2+\ldots+n} = 2^{n(n+1)/2} = 2^{n^2/2+o(n^2)}.$$

Каждое правильное семейство порождает не больше чем $16^n = 2^{4n} = 2^{o(n^2)}$ различных квазигрупп с помощью выбора функций $\pi_1, \ldots, \pi_n$. Различных согласованных перенумераций функций и переменных не больше, чем $n!$. Очевидно, что $n! \leqslant n^n = 2^{n \log_2 n} = 2^{o(n^2)}$. Перемножая полученные оценки, получаем требуемую верхнюю оценку на общее число квадратичных квазигрупп, порождаемых линейными правильными семействами.

Докажем нижнюю оценку. Рассмотрим подмножество линейных правильных семейств, задаваемое соотношениями

$$g_1 \equiv 0, \quad g_2 = x_1 + c, \quad g_i = x_{i-1} + g'_i(x_1, \ldots, x_{i-2}), \quad i = 3, \ldots, n,$$

где g'_i — произвольные линейные функции. Зафиксируем значение k из множества $\{1, \ldots, n-1\}$. Заметим, что все функции фиктивно зависят от x_n, поэтому π_n может быть выбрана произвольным образом. Для i из множества $\{k, \ldots, n-1\}$ положим $\pi_i(x, y) = x \cdot y$, оставшиеся функции сделаем линейными: $\pi_i(x, y) = x$, $i = 1, \ldots, k-1$. Заметим, что по построению в силу единственности полиномиального представления различные семейства $(g_1, \ldots, g_n)$ породят различные представления (1), т. е. различные квазигруппы. При этом первые k функций f_i линейны, так как имеют вид $x_i \oplus y_i \oplus g_i(x_1, \ldots, x_{i-1})$, а функции g_i линейны. Оставшиеся функции квадратичны, так как имеют вид

$$x_i \oplus y_i \oplus x_{i-1} \cdot y_{i-1} \oplus g'_i(x_1, \ldots, x_{k-1}, x_k \cdot y_k, \ldots, x_{i-2} \cdot y_{i-2}),$$

а функции g_i' линейны. Оценим число получившихся квазигрупп. Оно определяется числом способов выбора функций $g_2', \ldots, g_n'$, т. е. равно

$$2^1 \cdot 2^2 \cdot \ldots \cdot 2^{n-2} = 2^{1+2+\ldots+(n-2)} = 2^{(n-2)(n-1)/2} = 2^{n^2/2+o(n^2)}.$$

Ввиду произвольности k теорема доказана. □

Замечание 1. Утверждение теоремы 1 сохраняется при замене типа на строгий тип, так как в любой линейной комбинации, включающей хотя бы одну квадратичную функцию, сохраняется квадратичное слагаемое, соответствующее функции со старшим номером.

Замечание 2. В силу треугольности порождаемые квазигруппы с точностью до согласованной перенумерации функций и переменных являются t-квазигруппами, при этом не все t-квазигруппы порождаются треугольными семействами. По сути, треугольные семейства дают выигрыш в пространственной сложности за счёт уменьшения порождаемого множества.

Отметим, что исторически треугольные семейства возникли раньше, чем t-квазигруппы: авторы конструкции t-квазигрупп в качестве источника вдохновения указывают работу [14] 2002 года, тогда как треугольные семейства были введены в работе [1] 1998 года, а связь с квазигруппами была отмечена в работе [2] 1999 года.

Число квадратичных квазигрупп, порождаемых линейными правильными семействами, может быть повышено с помощью следующего соображения. При этом мы останемся в классе t-квазигрупп.

Теорема 2. *Пусть $(g_1, \ldots, g_n)$ — треугольное правильное семейство. Тогда соотношения*

$$\begin{aligned}
z_1 &= x_1 \oplus y_1 \oplus g_1\big(\pi_{1,1}(x_1, y_1), \pi_{1,2}(x_2, y_2), \ldots, \pi_{1,n}(x_n, y_n)\big),\\
z_2 &= x_2 \oplus y_2 \oplus g_2\big(\pi_{2,1}(x_1, y_1), \pi_{2,2}(x_2, y_2), \ldots, \pi_{2,n}(x_n, y_n)\big),\\
&\vdots\\
z_n &= x_n \oplus y_n \oplus g_n\big(\pi_{n,1}(x_1, y_1), \pi_{n,2}(x_2, y_2), \ldots, \pi_{n,n}(x_n, y_n)\big)
\end{aligned} \tag{4}$$

порождают квазигрупповую операцию для любых двуместных функций $\pi_{1,1}, \ldots, \pi_{n,n}$.

Доказательство. Так как согласованная перенумерация переменных и функций является изотопией, т. е. переводит квазигруппы в квазигруппы, без ограничения общности можно считать, что семейство $(g_1, \ldots, g_n)$ имеет вид (3). Ввиду симметричности вхождения x и y в соотношения (4) достаточно показать, что для любой фиксации переменных $y_1, \ldots, y_n$ получившееся преобразование инъективно. Рассмотрим произвольную подстановку функций $\pi_{1,1}, \ldots, \pi_{n,n}$. Пусть значения $y_1, \ldots, y_n$ зафиксированы произвольным образом, $s = (s_1, \ldots, s_n)$ и $t = (t_1, \ldots, t_n)$ — пара различных значений $x_1, \ldots, x_n$. Рассмотрим минимальный индекс i, для которого $s_i \neq t_i$. Рассмотрим значение z_i

на наборах $(s_1, y_1, \ldots, s_n, y_n)$ и $(t_1, y_1, \ldots, t_n, y_n)$. Ввиду выбора i и вида семейства справедливо равенство

$$g_i\big(\pi_{i,1}(s_1, y_1), \pi_{i,2}(s_2, y_2), \ldots, \pi_{i,n}(s_n, y_n)\big) = \\ = g_i\big(\pi_{i,1}(t_1, y_1), \pi_{i,2}(t_2, y_2), \ldots, \pi_{i,n}(t_n, y_n)\big) = c,$$

где c — булева константа. Таким образом, в первом случае z_i принимает значение $s_i \oplus y_i \oplus c$, во втором — $t_i \oplus y_i \oplus c = s_i \oplus 1 \oplus y_i \oplus c$, т. е. значения не совпадают и преобразование инъективно. Ввиду произвольности выбора функций $\pi_{i,j}$ и фиксации $y_1, \ldots, y_n$ теорема доказана. □

Заметим, что условие треугольности является существенным, и в общем случае утверждение теоремы 2 не выполняется. Действительно, рассмотрим правильное семейство

$$\begin{aligned} g_1 &= \bar{x}_2 \cdot x_3, \\ g_2 &= \bar{x}_3 \cdot x_1, \\ g_3 &= \bar{x}_1 \cdot x_2 \end{aligned} \tag{5}$$

(правильность несложно проверить, например, по определению). Выберем

$$\pi_{1,2}(x, y) = \pi_{2,3}(x, y) = \pi_{3,1}(x, y) = \bar{x}, \quad \pi_{1,3}(x, y) = \pi_{2,1}(x, y) = \pi_{3,2}(x, y) = x,$$

остальные функции $\pi_{i,j}$ соответствуют фиктивным переменным и могут быть выбраны произвольным образом. Зафиксируем значение $y_1 = y_2 = y_3 = 0$; значения всех функций f_i из (1) на наборах $x_1 = x_2 = x_3 = 0$ и $x_1 = x_2 = x_3 = 1$ равны нулю, т. е. совпадают. Таким образом, операция не является квазигрупповой по определению.

5. Треугольные квадратичные семейства

Так как все линейные правильные семейства треугольные, их естественным обобщением является класс треугольных квадратичных семейств. В этом случае мощность множества порождаемых квазигрупп существенно возрастает.

Теорема 3. *Число квадратичных квазигрупп, порождаемых квадратичными треугольными семействами порядка n, равно $2^{n^3/6+o(n^3)}$.*

Доказательство. Сперва докажем верхнюю оценку. Аналогично доказательству теоремы 1 рассмотрим систему не более чем квадратичных функций, заданную соотношениями (3). Первая функция, т. е. константа, может быть выбрана двумя способами. Вторая функция, т. е. функция одной переменной, может быть выбрана четырьмя способами. Начиная с третьей функции появляется возможность добавления квадратичных членов, т. е. число способов выбрать функцию номер i равно $2^{\binom{i-1}{2}}$ (выбор коэффициентов при квадратичных мономах) умножить на 2^{i-1} (выбор коэффициентов при линейных мономах) и умножить на

два (выбор свободного члена). Итоговая мощность составляет

$$2^1 \cdot 2^2 \cdot 2^{3+\binom{2}{2}} \cdot \ldots \cdot 2^{n+\binom{n-1}{2}} = 2^{n(n+1)/2} \cdot 2^{S(n)},$$

где

$$S(n) = \sum_{i=2}^{n-1} \binom{i}{2}.$$

Используя известное тождество

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k},$$

с помощью индукции по n легко показать, что

$$S(n) = \binom{n}{3} = \frac{n^3}{6} + o(n^3).$$

Остальные сомножители оцениваются аналогично доказательству теоремы 1. Верхняя оценка доказана.

Для обоснования нижней оценки рассмотрим семейства $(g_1, \ldots, g_n)$, в которых

$$g_1 \equiv 0, \quad g_2 = x_1, \quad g_i = x_{i-2} \cdot x_{i-1} \oplus g'_i(x_1, \ldots, x_{i-2}), \quad i = 3, \ldots, n,$$

где g'_i — произвольные не более чем квадратичные функции, и подстановку $\pi_i(x, y) = x$. По построению функции с номерами от 3 до n будут квадратичными, первые две функции — линейными. Ввиду единственности полиномиального представления различным g'_i будут соответствовать различные квазигруппы. Аналогично рассуждениям при получении верхней оценки количество порождаемых квазигрупп равно

$$2^1 \cdot 2^2 \cdot 2^{3+\binom{2}{2}} \cdot \ldots \cdot 2^{(n-1)+\binom{n-2}{2}} = 2^{n(n-1)/2} \cdot 2^{S(n-1)},$$

где

$$S(n-1) = \binom{n-1}{3} = \frac{n^3}{6} + o(n^3).$$

Теорема доказана. □

Замечание 3. Из доказательства вытекает, что если $k = o(n)$, $k \geqslant 3$, то мощность множества порождаемых квазигрупп строгого типа $\mathrm{Quad}^s_{n-k}\mathrm{Lin}^s_k$ равна $2^{n^3/6+o(n^3)}$. Кроме того, так как рассмотренные при получении нижней оценки функции содержат слагаемое $x_{i-1} \cdot x_i$, такие квазигруппы не порождаются линейными правильными семействами.

Заметим, что замечание 2 справедливо и в случае квадратичных треугольных семейств.

6. Треугольное расширение и сильно квадратичные квазигруппы

Рассмотрим две конструкции, позволяющие строить сильно квадратичные квазигруппы.

Теорема 4. *Пусть $n \in \mathbb{N}$, $n \geqslant 3$. Семейство функций $(g_1, \ldots, g_n)$, определяемое соотношениями*

$$\begin{aligned} g_1 &= \bar{x}_2 \cdot x_3, \\ g_2 &= \bar{x}_3 \cdot x_4, \\ &\vdots \\ g_{n-1} &= \bar{x}_n \cdot x_1, \\ g_n &= \bar{x}_1 \cdot x_2, \end{aligned} \tag{6}$$

является правильным тогда и только тогда, когда n нечётно.

Доказательство. Пусть n чётно. Рассмотрим пару наборов

$$\alpha = (0, 1, 0, 1, \ldots, 0, 1), \quad \beta = (1, 0, 1, 0, \ldots, 1, 0).$$

Несложно увидеть, что на наборе α все функции с нечётными номерами системы (6) обращаются в 0, а все функции с чётными номерами равны 1; на наборе β ситуация противоположная. Таким образом, $g_i(\alpha) \neq g_i(\beta)$, $i = 1, \ldots, n$, и система не является правильной по определению.

Пусть n нечётно. Несложно увидеть, что если для некоторого $\alpha = (\alpha_1, \ldots, \alpha_n)$ справедливо равенство $g_i(\alpha) = 1$, т. е. $\alpha_{i+1} = 0$, $\alpha_{i+2} = 1$, то $g_{i-1}(\alpha) = g_{i+1}(\alpha) = 0$ (в рамках доказательства сложение индексов осуществляется по формуле $i + j = (i + j - 1) \pmod{n} + 1$). Следовательно, для любого входного набора число функций, принимающих значение 1 на этом наборе, не превосходит $(n-1)/2$, и для любой пары входных наборов найдётся функция, которая на обоих наборах принимает значение 0.

Предположим, что семейство (6) не является правильным. Значит, найдётся пара различных наборов $\alpha = (\alpha_1, \ldots, \alpha_n)$, $\beta = (\beta_1, \ldots, \beta_n)$, таких что для любого индекса i, $1 \leqslant i \leqslant n$, для которого $\alpha_i \neq \beta_i$, выполнено $g_i(\alpha) \neq g_i(\beta)$. Рассмотрим индекс i_0, для которого $g_{i_0}(\alpha) = g_{i_0}(\beta) = 0$. По предположению $\alpha_{i_0} = \beta_{i_0}$. Возможны следующие случаи:

1. $\alpha_{i_0} = \beta_{i_0} = 0$. Так как x_{i_0} входит без отрицания в g_{i_0-2}, выполнено равенство $g_{i_0-2}(\alpha) = g_{i_0-2}(\beta) = 0$; по предположению $\alpha_{i_0-2} = \beta_{i_0-2}$;
2. $\alpha_{i_0} = \beta_{i_0} = 1$. Так как x_i входит в g_{i_0-1} с отрицанием, выполнено равенство $g_{i_0-1}(\alpha) = g_{i_0-1}(\beta) = 0$; по предположению $\alpha_{i_0-1} = \beta_{i_0-1}$. Так как g_{i_0-2} существенно зависит только от переменных x_{i_0-1} и x_{i_0}, а также в силу того что $\alpha_{i_0-1} = \beta_{i_0-1}$, $\alpha_{i_0} = \beta_{i_0}$, справедливо равенство $g_{i_0-2}(\alpha) = g_{i_0-2}(\beta)$; значит, вновь $\alpha_{i_0-2} = \beta_{i_0-2}$.

Продолжая рассуждение, делаем вывод, что, в силу нечётности n $\alpha = \beta$, что противоречит предположению. Теорема доказана. □

Замечание 4. Семейство (5), рассмотренное в разделе 4, имеет вид (6). Таким образом, теорема 4 даёт ещё одно доказательство правильности этого семейства.

Замечание 5. Теорема 4 является частным случаем теоремы 5 из [3].

Замечание 6. Правильное семейство (6) даёт возможность построения сильно квадратичных квазигрупп для случая нечётных n. Например, подстановка $\pi_i(x,y) = x$, $i = 1,\ldots,n$, порождает сильно квадратичную квазигруппу, содержащую слагаемое $x_i \cdot x_{i+1}$ (и поэтому не порождаемую билинейной конструкцией). Мощность порождаемого множества оценивается сверху величиной 6^n, т. е. невелика в сравнении с другими методами. Ниже будет представлена конструкция, позволяющая охватить случай чётных n и существенно повысить мощность множества порождаемых сильно квадратичных квазигрупп.

Рассмотрим введённую в [17] конструкцию, которую будем называть треугольным расширением правильных семейств. Пусть $(g_1,\ldots,g_n)$ — правильное семейство порядка n, n' — натуральное число, $n' > n$. Представим n' в виде $n + s_1 + \ldots + s_n$, где $s_i \in \mathbb{N} \cup \{0\}$, $i = 1,\ldots,n$. Рассмотрим семейство порядка n' функций

$$(g'_{1,1},\ldots,g'_{1,s_1},g'_{1,0},g'_{2,1},\ldots,g'_{2,s_2},g'_{2,0},\ldots,g'_{n,1},\ldots,g'_{n,s_n},g'_{n,0})$$

от переменных

$$(x'_{1,1},\ldots,x'_{1,s_1},x'_{1,0},x'_{2,1},\ldots,x'_{2,s_2},x'_{2,0},\ldots,x'_{n,1},\ldots,x'_{n,s_n},x'_{n,0})$$

(если s_i равно нулю, то элементы $g'_{i,j}$ и $x'_{i,j}$ с натуральными индексами отсутствуют), заданное соотношениями

$$\begin{aligned}
g'_{i,1} &= G_{i,1}\big(g_i(x'_{1,0},\ldots,x'_{n,0})\big),\\
g'_{i,2} &= G_{i,2}(g_i(x'_{1,0},\ldots,x'_{n,0}),x'_{i,1}),\\
&\vdots\\
g'_{i,s_i} &= G_{i,s_i}(g_i(x'_{1,0},\ldots,x'_{n,0}),x'_{i,1},\ldots,x'_{i,s_i-1}),\\
g'_{i,0} &= G_{i,0}(g_i(x'_{1,0},\ldots,x'_{n,0}),x'_{i,1},\ldots,x'_{i,s_i}),
\end{aligned} \tag{7}$$

$i = 1,\ldots,n$, где $G_{i,j}$ — произвольные булевы функции от указанных переменных.

Известен следующий факт.

Теорема [17]. *Если семейство $(g_1,\ldots,g_n)$ правильное, то любое его треугольное расширение также является правильным семейством.*

Пример 1. Построим треугольное расширение семейства (5) до семейства порядка 4. В нашем случае

$$n = 3, \quad n' = 4, \quad s_1 = 1, \quad s_2 = s_3 = 0,$$
$$G_{1,1}(x) = G_{2,0}(x) = G_{3,0}(x) = x, \quad G_{1,0}(x,y) = y.$$

В результате возникнет семейство

$$\begin{aligned} g'_{1,1} &= \bar{x}'_{2,0} \cdot x'_{3,0}, \\ g'_{1,0} &= x'_{1,1}, \\ g'_{2,0} &= \bar{x}'_{3,0} \cdot x'_{1,0}, \\ g'_{3,0} &= \bar{x}'_{1,0} \cdot x'_{2,0}, \end{aligned}$$

которое с помощью подстановки $\pi_{i,0}(x,y) = x$, $\pi_{1,1}(x,y) = x \cdot y$ порождает сильно квадратичную квазигруппу с операцией

$$\begin{aligned} z'_{1,1} &= x'_{1,1} \oplus y'_{1,1} \oplus x'_{3,0} \oplus x'_{2,0} \cdot x'_{3,0}, \\ z'_{1,0} &= x'_{1,0} \oplus y'_{1,0} \oplus x'_{1,1} \cdot y'_{1,1}, \\ z'_{2,0} &= x'_{2,0} \oplus y'_{2,0} \oplus x'_{1,0} \oplus x'_{3,0} \cdot x'_{1,0}, \\ z'_{3,0} &= x'_{3,0} \oplus y'_{3,0} \oplus x'_{2,0} \oplus x'_{1,0} \cdot x'_{2,0}, \end{aligned}$$

с помощью согласованного переименования функций и переменных преобразуемую к виду

$$\begin{aligned} z_1 &= x_1 \oplus y_1 \oplus x_4 \oplus x_3 \cdot x_4, \\ z_2 &= x_2 \oplus y_2 \oplus x_1 \cdot y_1, \\ z_3 &= x_3 \oplus y_3 \oplus x_2 \oplus x_4 \cdot x_2, \\ z_4 &= x_4 \oplus y_4 \oplus x_3 \oplus x_2 \cdot x_3 \end{aligned}$$

(сильная квадратичность следует из уникальности квадратичных слагаемых в каждой функции). Число квадратичных слагаемых можно увеличить, используя подстановку $\pi_{i,0}(x,y) = x \oplus y$.

Для упрощения терминологии при фиксированном i, $1 \leqslant i \leqslant n$, назовём последовательность функций $g'_{i,j}$ треугольником.

Пример 1 может быть естественным образом обобщён на случай произвольного n' за счёт увеличения значения n (порождение семейства чётного порядка n' из семейства (6) порядка $n = n'-1$) или за счёт увеличения треугольника, т. е. параметра s_1. Однако для обеспечения сильной квадратичности треугольник должен быть линейным (но не константным!), т. е. множество порождаемых сильно квадратичных квазигрупп будет иметь мощность, не превышающую $2^{n^2/2+o(n^2)}$. Для того чтобы повысить степень в показателе, обобщим теорему 2 на случай треугольных расширений.

Теорема 5. *Пусть $(g_1, \ldots, g_n)$ — правильное семейство, $(g'_{1,1}, \ldots, g'_{n,0})$ — треугольное расширение $(g_1, \ldots, g_n)$, полученное с помощью формул (7). Тогда соотношения*

$$\begin{aligned} z'_{1,1} &= x'_{1,1} \oplus y'_{1,1} \oplus g'_{1,1}\bigl(\pi_{1,1,1,1}(x'_{1,1}, y'_{1,1}), \ldots, \pi_{1,1,n,0}(x'_{n,0}, y'_{n,0})\bigr), \\ &\vdots \\ z'_{n,0} &= x'_{n,0} \oplus y'_{n,0} \oplus g'_{n,0}\bigl(\pi_{n,0,1,1}(x'_{1,1}, y'_{1,1}), \ldots, \pi_{n,0,n,0}(x'_{n,0}, y'_{n,0})\bigr) \end{aligned} \tag{8}$$

задают квазигруппу для любой подстановки функций $\pi_{i,j,k,l}$, *такой что при любом* $k \in \{1, \ldots, n\}$ *для всех* i_1, i_2, j_1, j_2 *выполнено тождество* $\pi_{i_1,j_1,k,0}(x, y) \equiv \equiv \pi_{i_2,j_2,k,0}(x, y)$.

Содержательно говоря, вместо каждой переменной исходного правильного семейства $(g_1, \ldots, g_n)$ нужно подставлять одни и те же функции (как в исходной конструкции), а вместо переменных «треугольников» разрешается подставлять свои функции в каждой строке соотношений (8).

Прежде чем перейти к доказательству теоремы 5, сформулируем и докажем вспомогательное утверждение.

Лемма 1. *Пусть* $(g_1, \ldots, g_n)$ *— правильное семейство,* $\pi_1, \ldots, \pi_n$ *— функции двух переменных,*

$$h_i(x_1, \ldots, x_n, y_1, \ldots, y_n) = g_i\big(\pi_1(x_1, y_1), \ldots, \pi_n(x_n, y_n)\big), \quad i = 1, \ldots, n,$$

$\alpha = (\alpha_1, \ldots, \alpha_n)$, $\beta = (\beta_1, \ldots, \beta_n)$, $\gamma = (\gamma_1, \ldots, \gamma_n)$ *— три двоичных набора,* $\alpha \neq \beta$. *Тогда существует индекс* i_0, $1 \leqslant i_0 \leqslant n$, *такой что* $\alpha_{i_0} \neq \beta_{i_0}$, *но* $h_{i_0}(\alpha, \gamma) = h_{i_0}(\beta, \gamma)$.

Доказательство. Возможны два случая.

В первом случае для любого индекса i, $1 \leqslant i \leqslant n$, справедливо равенство $\pi_i(\alpha_i, \gamma_i) = \pi_i(\beta_i, \gamma_i)$. Следовательно, для любого i выполняется равенство $h_i(\alpha, \gamma) = h_i(\beta, \gamma)$ и в качестве i_0 можно выбрать любой индекс, такой что $\alpha_{i_0} \neq \beta_{i_0}$.

Во втором случае наборы

$$\big(\pi_1(\alpha_1, \gamma_1), \ldots, \pi_n(\alpha_n, \gamma_n)\big), \quad \big(\pi_1(\beta_1, \gamma_1), \ldots, \pi_n(\beta_n, \gamma_n)\big)$$

различны. Заметим, что эти наборы подаются на вход правильного семейства функций и по определению правильного семейства найдётся индекс i_0, такой что $\pi_{i_0}(\alpha_{i_0}, \gamma_{i_0}) \neq \pi_{i_0}(\beta_{i_0}, \gamma_{i_0})$ (значит, и $\alpha_{i_0} \neq \beta_{i_0}$), но

$$g_{i_0}\big(\pi_1(\alpha_1, \gamma_1), \ldots, \pi_n(\alpha_n, \gamma_n)\big) = g_{i_0}\big(\pi_1(\beta_1, \gamma_1), \ldots, \pi_n(\beta_n, \gamma_n)\big),$$

т. е. по определению $h_{i_0}(\alpha, \gamma) = h_{i_0}(\beta, \gamma)$. □

Доказательство теоремы 5. Рассмотрим произвольные семейства

$$(g_1, \ldots, g_n), \quad (g'_{1,1}, \ldots, g'_{n,0})$$

и подстановку $\pi_{i,j,k,l}$, удовлетворяющие условию теоремы. Так как для любого k функции $\pi_{i,j,k,0}$ по условию совпадают для всех i и j, для краткости будем использовать обозначение $\pi_{k,0}$.

Покажем, что для любой фиксации значений переменных $y'_{i,j}$ получающиеся функции задают биекцию. Зафиксируем значения $y'_{i,j}$ произвольным образом и рассмотрим пару наборов $\alpha = (\alpha_{1,1}, \ldots, \alpha_{n,0})$ и $\beta = (\beta_{1,1}, \ldots, \beta_{n,0})$ значений переменных $x'_{i,j}$. Докажем, что левые части соотношений (8) принимают на α и β различные значения. Возможны следующие случаи.

Случай 1. Найдётся индекс k, $1 \leqslant k \leqslant n$, такой что $\alpha_{k,0} \neq \beta_{k,0}$. Предположим, что левые части соотношений (8) принимают на α и β равные значения. По условиям теоремы и леммы 1 найдётся индекс k_0, такой что $\alpha_{k_0,0} \neq \beta_{k_0,0}$, но

$$g_{k_0}\big(\pi_{1,0}(\alpha_{1,0},\gamma_{1,0}),\ldots,\pi_{n,0}(\alpha_{n,0},\gamma_{n,0})\big) = g_{k_0}\big(\pi_{1,0}(\beta_{1,0},\gamma_{1,0}),\ldots,\pi_{n,0}(\beta_{n,0},\gamma_{n,0})\big).$$

Если $s_{k_0} > 0$, покажем, что для любого i от 1 до s_{k_0} справедливо равенство $\alpha_{k_0,i} = \beta_{k_0,i}$. Действительно, в силу того что $z_{k_0,1}$ на наборах α и β совпадают, $\alpha_{k_0,1} = \beta_{k_0,1}$. Продолжая рассуждение для $z_{k_0,i}$ при $i = 2,\ldots,s_{k_0-1}$, делаем вывод, что $\alpha_{k_0,i} = \beta_{k_0,i}$ на множестве натуральных i. Из вида выражения для $z_{k_0,0}$ следует, что $\alpha_{k,0} = \beta_{k,0}$. Полученное противоречие доказывает невозможность рассмотренного случая.

Случай 2. Для любого k от 1 до n выполнено равенство $\alpha_{k,0} = \beta_{k,0}$. Значит, найдётся такой индекс i,j, $1 \leqslant i \leqslant n$, $1 \leqslant j \leqslant s_i$, что $\alpha_{i,j} \neq \beta_{i,j}$. Без ограничения общности можно считать, что значение j выбрано минимальным. По предположению в левой части выражений для $z_{i,j}$ отличаются только первые слагаемые. Значит значения $z_{i,j}$ на наборах α и β различаются.

Случай фиксации значений $x'_{i,j}$ рассматривается аналогично. Теорема доказана. □

Следствие 1. *Пусть в соотношениях* (8) *семейство* $(g_1,\ldots,g_n)$ *квадратично, верхние функции* $G_{i,j}$ *каждого треугольника тождественные, оставшиеся функции каждого треугольника не более чем квадратичны по всем переменным, кроме первой, и не более чем линейны по первой переменной. Пусть подстановки* $\pi_{i,j,k,l}$ *для переменных, входящих в квадратичные члены, не более чем линейны. Тогда порождаемая квазигруппа либо линейная, либо квадратичная.*

Конструкция (8) для любого $n \geqslant 3$ позволяет порождать множества сильно квадратичных квазигрупп мощности не меньше чем $2^{n^3/6+o(n^3)}$. В качестве исходного правильного семейства выберем семейство (5). Пусть

$$s_1 = n-3, \quad s_2 = s_3 = 0, \quad G_{1,1}(x) = G_{2,0}(x) = G_{3,0}(x) = x, \quad G_{1,2}(x,y) = y,$$

а оставшиеся функции $G_{1,j}$ не содержат первую переменную, содержат моном $x'_{1,j-2} \cdot x'_{1,j-1}$ и квадратичны. Вместо переменных исходного семейства подставим функцию $x \oplus y$, вместо $x'_{1,1}$ в соотношении для $z'_{1,2}$ подставим $x \cdot y$, при $i \geqslant 3$ в соотношения для $z'_{1,i}$ вместо каждой переменной подставим $x \oplus y$. Несложно увидеть, что порождённые квазигруппы будут сильно квадратичными (если в линейную комбинацию входят только верхние функции каждого треугольника, квадратичность следует из сильной квадратичности исходного семейства; в противном случае выберем индекс $1,j$ слагаемого с максимальным значением j (считаем, что 0 больше, чем натуральные числа) и увидим, что моном $x'_{1,j-2} \cdot x'_{1,j-1}$ обязан присутствовать в линейной комбинации. Ввиду единственности полиномиального представления разным семействам в этом случае соответствуют разные квазигруппы. Аналогично доказательству теоремы 3 несложно показать, что мощность порождаемого множества есть $2^{n^3/6+o(n^3)}$. Оформим полученную оценку в виде теоремы.

Теорема 6. *Конструкция* (8) *порождает не менее* $2^{n^3/6+o(n^3)}$ *сильно квадратичных квазигрупп порядка* n.

Заметим, что применение изотопий, заданных невырожденными линейными преобразованиями переменных x', y' и z', сохраняет сильную квадратичность; применение таких изотопий позволяет породить квазигруппы с существенно менее «разреженной» структурой. Также заметим, что ввиду сильной квадратичности и наличия мономов вида $x_i \cdot x_j$ квазигруппы, порождённые описанным способом, не являются t-квазигруппами и не задаются билинейной конструкцией.

7. Заключение

Квадратичные квазигруппы используются в ряде криптографических приложений. В работе предложен ряд методов, позволяющих порождать большие семейства квадратичных (в том числе гарантированно сильно квадратичных) квазигрупп произвольного порядка n, $n \geqslant 3$. В дальнейшем планируется продолжить исследование квадратичных правильных семейств булевых функций, не являющихся треугольными, а также перенести результаты на случай произвольных конечных полей.

Литература

[1] Носов В. А. Критерий регулярности булевского неавтономного автомата с разделённым входом // Интеллект. сист. — 1998. — Т. 3, № 3-4. — С. 269—280.

[2] Носов В. А. Построение классов латинских квадратов в булевой базе данных // Интеллект. сист. — 1999. — Т. 4, № 3-4. — С. 307—320.

[3] Носов В. А. Построение параметрического семейства латинских квадратов в векторной базе данных // Интеллект. сист. — 2004. — Т. 8, № 1-4. — С. 517—529.

[4] Ahlawat R., Gupta K., Pal S. K. Fast generation of multivariate quadratic quasigroups for cryptographic applications // Proceeding of Mathematics in Defence. — 2009.

[5] Alagic G., Alperin-Sheriff J., Apron D., Cooper D., Dang Q., Liu Y.-K., Miller C., Moody D., Peralta R., Perlner R., Robinson A., Smith-Tone D. Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process. — National Inst. of Standards and Technology, Dep. of Commerce, 2019.

[6] Chen Y., Gligoroski D., Knapskog S. On a special class of multivariate quadratic quasigroups (MQQs) // J. Math. Cryptology. — 2013. — Vol. 7, no. 8. — P. 111—141.

[7] Chen Y., Knapskog S. J., Gligoroski D. Multivariate quadratic quasigroups (MQQs): Construction, bounds and complexity // Inscrypt, ser. 6th Int. Conf. on Information Security and Cryptology. — Sci. Press of China, 2010. — P. 20—34.

[8] Ding J., Petzoldt A. Current state of multivariate cryptography // IEEE Security Privacy. — 2017. — Vol. 15, no. 4. — P. 28—36.

[9] Faugère J.-C., Ødegård R., Perret L., Gligoroski D. Analysis of the MQQ public key cryptosystem // Int. Conf. on Cryptology and Network Security CANS 2010:

Cryptology and Network Security. — Berlin: Springer, 2010. — (Lect. Notes Comput. Sci.; Vol. 6467). — P. 169—183.

[10] Garey M. R., Johnson D. S. Computers and Intractability. A Guide to the Theory of NP-Completeness. — New York: Freeman, 1979.

[11] Gligoroski D., Markovski S., Knapskog J. Multivariate quadratic trapdoor functions based on multivariate quadratic quasigroups // Proc. of the American Conference on Applied Mathematics (MATH'08). — WSEAS Press, 2008. — P. 44—49.

[12] Gligoroski D., Markovski S., Knapskog J. Public key block cipher based on multivariate quadratic quasigroups. — Cryptology ePrint Archive, Report 2008/320. — 2008. — http://eprint.iacr.org/2008/320.

[13] Gligoroski D., Ødegård R., Jensen R., Perret L., Faugère J.-C., Knapskog S., Markovski S. MQQ-SIG: an ultra-fast and provably CMA resistant digital signature scheme // INTRUST'11: Proc. of the Third Int. Conf. on Trusted Systems. — 2011. — P. 184—203.

[14] Klimov A., Shamir A. A new class of invertible mappings // Int. Workshop on Cryptographic Hardware and Embedded Systems CHES 2002. — Berlin: Springer, 2002. — (Lect. Notes Comput. Sci.; Vol. 2523). — P. 470–483

[15] Lau D. Function Algebras on Finite Sets: A Basic Course on Many-Valued Logic and Clone Theory. — Berlin: Springer, 2006.

[16] Mohamed M., Ding J., Buchmann J., Werner F. Algebraic attack on the (MQQ) public key cryptosystem // CANS '09 Proc. of the 8th Int. Conf. on Cryptology and Network Security. — Berlin: Springer, 2009. — P. 392—401.

[17] Nosov V. A. Constructing families of Latin squares over Boolean domains // Boolean Functions in Cryptology and Information Security. — IOS Press, 2008. — P. 200—207.

[18] Nosov V. A., Pankratiev A. E. Latin squares over Abelian groups // J. Math. Sci. — 2008. — Vol. 149, no. 3. — P. 1230—1234.

[19] Samardjiska S., Chen Y., Gligoroski D. Construction of multivariate quadratic quasigroups (MQQs) in arbitrary Galois fields // 2011 7th Int. Conf. on Information Assurance and Security (IAS). — 2011. — P. 314—319.

[20] Samardjiska S., Markovski S., Gligoroski D. Multivariate quasigroups defined by t-functions // Proc. of SCC2010 — The 2nd Int. Conf. on Symbolic Computation and Cryptography. — 2010. — P. 117—127.

[21] Wolf C., Preneel B. Taxonomy of public key schemes based on the problem of multivariate quadratic equations. — Cryptology ePrint Archive, Report 2005/077. — 2005. — https://eprint.iacr.org/2005/077.

[22] Zhang Y., Zhang H. An algorithm for judging and generating bilinear multivariate quadratic quasigroups // Appl. Math. Inform. Sci. — 2013. — Vol. 7, no. 9. — P. 2071—2076.

[23] Zhang Y., Zhang H. An algorithm for judging and generating multivariate quadratic quasigroups over Galois fields // Springerplus. — 2016. — Vol. 5, no. 1. — P. 1845.