2012 Математические методы криптографии №3(17)

DOI 10.17223/20710410/17/6

УДК 681.03

ЛАТИНСКИЕ КВАДРАТЫ И ИХ ПРИМЕНЕНИЕ В КРИПТОГРАФИИ

М. Э. Тужилин

Российский государственный гуманитарный университет, г. Москва, Россия

E-mail: mtmt@rambler.ru

Сделан обзор публикаций, посвящённых применению латинских квадратов в криптографии.

Ключевые слова: *латинский квадрат, квазигруппа, криптография.*

1. История

Определение 1. Латинским квадратом n-го порядка $L = (l_{ij})$ называется таблица размера $n \times n$, заполненная n символами упорядоченного множества M таким образом, что в каждой строке и в каждом столбце каждый символ встречается ровно один раз.

Пример латинского квадрата:

$$\begin{array}{ccc} A & B & C \\ C & A & B \\ B & C & A \end{array}$$

Впервые латинские квадраты (4-го порядка) были опубликованы в книге «Шамс аль Маариф» («Книга о Солнце Гнозиса»), написанной Ахмадом аль-Буни в Египте приблизительно в 1200 г.

В настоящее время в качестве множества M обычно берется множество натуральных чисел от 1 до n, однако Леонард Эйлер (1707–1783) использовал буквы латинского алфавита, откуда латинские квадраты и получили своё название [1].

Отметим, что многие подходы к изучению и построению латинских квадратов восходят к Эйлеру. Он строил латинские квадраты из латинских прямоугольников. Важной вехой в исследовании латинских квадратов была работа А. Кэли [2], в которой он привёл формулу для числа таких прямоугольников из двух строк. Следующее продвижение — вывод формулы для числа прямоугольников из трёх строк — произошло в 1953 г. [3].

В 20–30-е годы XX века стали интенсивно изучаться неассоциативные алгебраические структуры. Эти исследования, в которых принимали участие и советские математики [4], привели к созданию теории квазигрупп [5].

2. Число латинских квадратов

Формула для подсчёта числа $L(n)$ латинских квадратов порядка n не найдена. В таблице приведены известные на настоящее время точные значения $L(n)$ [6].

Число латинских квадратов

n	$L(n)$	Автор (год)
1	1	
2	2	
3	12	
4	576	
5	161280	Euler (1682)
6	812851200	Frolov (1890)
7	61479419904000	Sade (1948)
8	108776032459082956800	Wells (1967)
9	5524751496156892842531225600	Bammel, Rothstein (1975)
10	9982437658213039871725064756920320000	McKay, Rogoyski (1995)
11	776966836171770144107444346734230682311065600000	McKay, Wanless (2005)

Справедливы оценки для величины $L(n)$ [7]:

$$\prod_{k=1}^{n}(k!)^{n/k} \leqslant L(n) \leqslant \frac{(n!)^{2n}}{n^{n^2}}.$$

3. Отношения эквивалентности на множестве латинских квадратов

Определение 2. Латинский квадрат называется нормализованным, если первая строка и первый столбец квадрата заполнены в соответствии с порядком, заданным на M.

Пример нормализованного латинского квадрата:

$$\begin{array}{ccc} A & B & C \\ B & C & A \\ C & A & B \end{array}$$

Число нормализованных латинских квадратов порядка n в $n!(n-1)!$ меньше, чем $L(n)$.

Определение 3. Два латинских квадрата называют изотопными, если один из них может быть получен из другого в результате изотопии — композиции из перестановки строк, перестановки столбцов и замены элементов M по подстановке из симметрической группы S_n.

Изотопия является отношением эквивалентности, поэтому все множество латинских квадратов разбивается на непересекающиеся изотопные классы. Из одного латинского квадрата можно получить с помощью изотопии $(n!)^3$ эквивалентных, но некоторые из них при этом могут совпасть, это называется автопаратопией. Доля латинских квадратов с нетривиальной группой автопаратопий стремится к нулю с ростом n [6].

Латинский квадрат можно рассматривать как ортогональный массив. Меняя порядок элементов в каждой упорядоченной тройке этого массива, получаем 6 латинских квадратов, которые называются парастрофами. Это новое отношение эквивалентности, его классы называются главными классами. Каждый из них содержит 1, 2, 3 или 6 изотопных классов. Композиция изотопии и парастрофии называется изострофией. В случае совпадения латинского квадрата и изострофного ему говорят об автострофии. Доказано, что с ростом n почти все латинские квадраты имеют тривиальную группу автострофий [8].

4. Ортогональные латинские квадраты

Определение 4. Два латинских квадрата L и K называются ортогональными, если все упорядоченные пары (l_{ij}, k_{ij}) различны.

Впервые пары ортогональных латинских квадратов были опубликованы в 1725 г. [9] в связи с решением задачи о расположении 16 игральных карт.

Ортогональные квадраты существуют для всех n, отличных от 2 и 6. Эйлер не смог построить два ортогональных латинских квадрата порядка 6 и сформулировал задачу их построения в виде «задачи о 36 офицерах» [1]. Он не смог построить и ортогональные латинские квадраты порядка 10 и высказал гипотезу о том, что не существует пар ортогональных квадратов для $n = 4r + 2$. В 1900 г. она была доказана для $n = 6$, а опровергнута в 1959 г. путём построения двух ортогональных квадратов для $n = 22$. В 1960 г. с помощью ЭВМ было построено два ортогональных квадрата для $n = 10$.

Для $n = q$, где q — степень простого числа, существуют так называемые полные системы из $(n-1)$ попарно ортогональных латинских квадратов. Способ их построения в 1938 г. опубликовал Р. Боуз [10] (хотя, как потом выяснилось, этот способ был открыт Муром в 1896 г.): достаточно рассмотреть многочлены $f_a(x, y) = ax+y$ над полем $\mathrm{GF}(q)$ при ненулевых a.

Пример полной системы попарно ортогональных латинских квадратов, построенной по методу Боуза, α — примитивный элемент $\mathrm{GF}(4)$

0	1	α	$\alpha+1$	0	1	α	$\alpha+1$	0	1	α	$\alpha+1$
1	0	$\alpha+1$	α	α	$\alpha+1$	0	1	$\alpha+1$	α	1	0
α	$\alpha+1$	0	1	$\alpha+1$	α	1	0	1	0	$\alpha+1$	α
$\alpha+1$	α	1	0	1	0	$\alpha+1$	α	α	$\alpha+1$	0	1

Для других значений n известны только нижние оценки числа попарно ортогональных квадратов, входящих в систему. Например, для $n = 10$ это 2, для 12 — 5, 14 — 3, 15 — 4, 18 — 3, 20 — 4, 21 — 5, 22 — 3, 24 — 6, 26 — 4, 28 — 5, 30 — 4.

Предложено много способов построения ортогональных латинских квадратов, их можно разбить на две группы. К первой группе относятся способы построения латинского квадрата, для которого с помощью изотопии можно получить ортогональный ему латинский квадрат. Ко второй группе относятся методы конструирования на основе ортогональных квадратов меньших порядков.

5. Частичные латинские квадраты

Квадрат, в котором каждый элемент множества M в каждой строке и в каждом столбце встречается не более одного раза, называется частичным. В [11] введено понятие критического множества, соответствующего частичному квадрату, который однозначно может быть дополнен до латинского, причём никакое его подмножество условию однозначности не удовлетворяет. Для небольших значений n известна мощность критического множества, для $n = 1$ это 0, для 2 — 1, 3 — 3, 4 — 7, 5 — 11, 6 — 18. Задача распознавания того, может ли частичный квадрат быть дополнен до латинского, NP-полна.

6. Применение латинских квадратов в криптографии

Латинские квадраты находят применение в комбинаторике, алгебре (изучение латинских квадратов тесно связано с изучением квазигрупп), теории кодов, статистике и многих других областях [12].

Впервые в криптографии латинский квадрат был применён в шифре Тритемия [13]. Тритемий построил таблицу (соответствующую таблице Кэли группы $(\mathbb{Z}_{26}, +)$) и использовал её для многоалфавитного шифрования, когда первая буква открытого текста шифруется первым алфавитом (первой строкой таблицы), вторая — вторым и т. д. Впоследствии этот шифр усовершенствовал Дж. Белазо [14], который придумал пароль. В совокупности с идеей Л. Б. Альберти использовать произвольный алфавит это привело к появлению нового шифра на основе квазигруппы, который стал важной вехой на пути развития криптографии.

Значение латинских квадратов для криптографии иллюстрирует теорема Шеннона, в соответствии с которой единственными совершенными шифрами являются шифры гаммирования, наложение гаммы в которых определяется латинским квадратом: «Perfect systems in which the number of cryptograms, the number of messages, and the number of keys are all equal are characterized by the properties that (1) each M is connected to each E by exactly one line, (2) all keys are equally likely. Thus the matrix representation of the system is a Latin square» [15, p. 681].

Попытка обобщить подход Шеннона и ввести понятие «сильно совершенный шифр» предпринята в [16].

В ряду примеров применения латинских квадратов для построения поточных шифров необходимо выделить предложенный в 2005 г. шифр Edon80 [17], который дошёл до третьего тура конкурса ESTREAM. Разработчики шифра из 576 существующих латинских квадратов 4-го порядка тщательно выбрали 4, на основе которых в криптосхеме строится конвейер из 80 латинских квадратов, он используется для выработки гаммы.

При разработке блочного шифра IDEA [18] авторы использовали три квазигруппы, соответствующие операциям сложения по модулю 2, сложения по модулю 2^{16} и умножения по модулю $2^{16} + 1$. При этом высокие криптографические свойства шифра они обосновывали тем, что среди соответствующих квазигрупп первая и вторая не изотопны, первая и третья не изотопны, а единственной изотопией между второй и третьей квазигруппами является функция логарифма.

Квазигруппа лежит в основе конструкции, предложенной в 2005 г. в качестве однонаправленной функции [19]. Там введено понятие e-преобразования с лидером l: вектор $A = (a_0, a_1, \ldots, a_{t-1})$ оно преобразует с помощью квазигруппы $(Q, *)$ в вектор $B = ((l*a_0), ((l*a_0)*a_1), \ldots, ((l*a_0)*a_1)*\ldots*a_{t-1})$. Затем с помощью e-преобразования вводятся функции R_1 и R_2:

$$R_1(A) = e_{a_{t-1}}(\ldots(e_{a_1}(e_{a_0}(A))\ldots),$$
$$R_2(A) = e_{a_{t-1}}(\ldots(e_{a_1}(e_{a_0}(e_{a_{t-1}}(\ldots(e_{a_1}(e_{a_0}(A))\ldots).$$

Доказана теорема о том, что если квазигруппа $(Q, *)$ неассоциативна и некоммутативна, то для вычисления обратной к R_1 функции требуется $\mathrm{O}(n^{\lfloor t/3 \rfloor})$ обращений в память (т. е. к латинскому квадрату, соответствующему квазигруппе Q), а для вычисления обратной к R_2 функции требуется $\mathrm{O}(n^t)$ обращений в память.

В [20] предложена схема аутентификации сообщений. Сообщение в этой схеме делится на блоки по t знаков. Для каждого j-го блока вида $a_1a_2\ldots a_t$ вычисляется в квазигруппе $(Q, *)$ значение $b_j = (\ldots((a_1 * a_2) * a3) * \ldots * a_{t-1}) * a_t$, которое является j-м элементом подписи. Имеется ряд работ, посвящённых анализу и усовершенствованию данной схемы.

Латинские квадраты являются привлекательным средством для построения схем разделения секрета. Секретом является латинский квадрат, а все участники схемы

получают соответствующие ему частичные квадраты [21]. Предложенная схема может быть усовершенствована [22]. В свою очередь, на основе таких схем разделения секрета можно строить и криптографические хеш-функции [23]. Другой пример построения криптографической хеш-функции на основе случайного латинского квадрата приведён в [24].

Разработанное в 2008 г. для участия в конкурсе SHA-3 на новый американский стандарт хеш-функции семейство Edon-R [25] не прошло во второй тур, но интересно тем, что в основе конструкции лежит построение и использование некоммутативной, неассоциативной, нелинейной квазигруппы. Авторы использовали квазигруппы порядков 2^{256} и 2^{512}, изотопные группам сложения в восьмимерных векторных пространствах над соответствующими полями, и два ортогональных латинских квадрата 8-го порядка.

В [26] предложен протокол с нулевым разглашением. Каждый участник a имеет открытый ключ, которым являются два изотопных латинских квадрата L_a и L'_a. Секретным ключом является изотопия между двумя этими латинскими квадратами. Для аутентификации доказывающий участник протокола многократно вырабатывает из L_a случайным образом изотопный ему латинский квадрат H, направляет его проверяющему и доказывает ему в зависимости от вопроса, что H изотопен L_a или H изотопен L'_a.

В заключение отметим, что о растущем внимании к теме свидетельствует появление обзоров [27 – 29].

ЛИТЕРАТУРА

1. *Euler L.* Recherches sur une nouvelle espèce de quarrés magiques. Middelburg, 1782.
2. *Cayley A.* On Latin Squares // Messenger of mathematics. 1890. V. XIX. P. 135–137.
3. *Touchard J.* Permutations, discordant with two given permutations // Scripta Math. 1953. No. 19. P. 109–111.
4. *Suschkewitsch A. K.* On the number of Latin Squares // Trans. Amer. Math. Soc. 1929. V. 31. P. 204–214.
5. *Moufang R.* Zur Struktur von Alternativkoerpern // Math. Ann. 1935. V. 110. No. 1. P. 416–430.
6. *McKay B. D. and Wanless I. M.* On the number of Latin Squares // Ann. Combin. 2005. No. 9. P. 335–344.
7. *Van Lint J. H. and Wilson R. M.* A Course in Combinatorics. Cambridge University Press, 1992.
8. *Черемушкин А. В.* Почти все латинские квадраты имеют тривиальную группу автострофий // Прикладная дискретная математика. 2009. № 3(5). С. 29–32.
9. *Ozanam J.* Récréations mathématiques et physiques. Paris, 1725.
10. *Bose R. S.* On the applications of the properties of Galois fields to the problems of construction of Hyper-Graeco-Latin squares // Indian J. Stat. 1938. No. 3. Part 4. P. 323–338.
11. *Nelder J.* Critical sets in latin squares // CSIRO Division Math. Stats, Newsletter. 1977. V. 38. P. 4.
12. *Laywine C. F. and Mullen G. L.* Discrete mathematics using Latin squares. New York: Wiley, 1998.
13. *Trithemius J.* Polygraphiae. Trittelheim, 1518.
14. *Bellaso G. B.* Il vero modo di scrivere in cifra con facilità, prestezza, et securezza di Misser Giovan Battista Bellaso, gentil'huomo bresciano // Iacobo Britannico. Bressa, 1564.

15. *Shannon C.* Communication Theory of Secrecy Systems // Bell System Technical J. 1949. V. 28. P. 656–715.
16. *Massey J.L., Maurer U., and Wang M.* Non-Expanding, Key-Minimal, Robustly-Perfect, Linear and Bilinear Ciphers // Adv. Cryptology — EUROCRYPT'87. Berlin; Heidelberg: Springer Verlag, 1988. P. 237–247.
17. *Gligoroski D., Markovski S., Kocarev L., and Gusev M.* Edon80 // `http://www.ecrypt.eu.org/stream/edon80p3.html`
18. *Lai X. and Massey J.* A Proposal for a New Block Encryption Standard // Adv. Cryptology — EUROCRYPT'90. New York: Springer Verlag, 1991. P. 55–70.
19. *Gligoroski D.* Candidate One-Way Functions and One-Way Permutations Based on Quasigroup String Transformations // `http://eprint.iacr.org/2005/352.pdf`
20. *Dènes J. and Keedwell A. D.* A new Authentication Scheme based in Latin Squares // Discrete Math. 1992. V. 106/107. P. 157–162.
21. *Cooper J., Donovan D., and Seberry J.* Secret Sharing Schemes Arising From Latin Squares // Bulletin of the ICA. 1994. V. 12. P. 33–43.
22. *Chum C.S. and Zhang X.* The Latin squares and the secret sharing schemes // Groups Complex. Cryptol. 2010. V. 2. P. 175–202.
23. *Chum C. S.* Hash functions, Latin squares and secret sharing schemes. New York: ProQuest, 2010.
24. *Pal S. K., Bhardwaj D., Kumar R., and Bhatia V.* A New Cryptographic Hash Function based on Latin Squares and Non-linear Transformations // Adv. Comput. Conf. IACC. Patiala, 2009. P. 862–867.
25. *Gligoroski D., Ødegård R.S., Mihova M., et al.* Cryptographic Hash Function Edon-R // Proc. IWSCN. Trondheim, 2009. P. 1–9.
26. *Dènes J. and Dènes T.* Non-associative algebraic system in cryptology. Protection against "meet in the middle" attack // Quasigroups and Related Systems. 2001. No. 8. P. 7–14.
27. *Глухов М. М.* О применениях квазигрупп в криптографии // Прикладная дискретная математика. 2008. № 2(2). С. 28–32.
28. *Shcherbacov V. A.* Quasigroups in cryptology // Comput. Sci. J. Moldova. 2009. V. 17. No. 2(50). P. 193–228.
29. *Малых А. Е., Данилова В. И.* Об историческом процессе развития теории латинских квадратов и некоторых их приложениях // Вестник Пермского университета. 2010. Вып. 4(4). С. 95–104.