

О сложности проверки свойства правильности для семейств функций

К. Царегородцев^{1, 2}

¹АО «НПК «Криптонит»

²МГУ им. М.В.Ломоносова
г. Москва, Россия

Алгебра и математическая логика: теория и приложения, 2024

Содержание доклада

- 1 Мотивация и основные определения
- 2 Правильные семейства функций
- 3 Характеризация в терминах несамодвойственности

Алгебраические структуры в криптографии

«Базовые»	«Нестандартные»
коммутативные группы: \mathbb{F}_q^* , $E(\mathbb{F}_q)$	Некоммутативные группы ¹ (пример: группы кос, матрицы над кольцами, ...)
векторные пространства, коды, решётки ²	модули более общего вида ³
ассоциативные структуры (группы, кольца и т.д.)	неассоциативные структуры: квазигруппы, квазигрупповые кольца ⁴

¹Романьков, *Алгебраическая криптология: монография*; Молдовян, Молдовян и Молдовян, «Новая концепция разработки постквантовых алгоритмов цифровой подписи на некоммутативных алгебрах»; Myasnikov, Shpilrain и Ushakov, *Non-commutative cryptography and complexity of group-theoretic problems*.

²Bernstein, Buchmann и Dahmen, *Post-quantum cryptography*.

³Нечаев, «Конечные квазифробениусовы модули, приложения к кодам и линейным рекуррентам».

⁴Глухов, «О применениях квазигрупп в криптографии»; Артамонов, «Квазигруппы и их приложения»; Markov, Mikhalev и Nechaev, «Nonassociative Algebraic Structures in Cryptography and Coding».

Квазигруппа

Квазигруппа

Множество Q с заданной на нем бинарной операцией $\circ: Q \times Q \rightarrow Q$ со следующим свойством: для любых $a, b \in Q$ существуют единственные $x, y \in Q$, такие что:

$$a \circ x = b, \quad y \circ a = b.$$

По сути = группа без ассоциативности и единицы, но с **сокращением** слева/справа.

Примеры квазигрупп:

- Q — любая группа, например $Q = \mathbb{Z}_k$, $\circ = +$;
- $Q = \mathbb{Z}_k$, $\circ = -$ (не группа, т.к. $a - (b - c) \neq (a - b) - c$);
- (G, \cdot) — группа, π, σ, τ — подстановки на G , $x \circ y := \tau(\pi(x) \cdot \sigma(y))$.

Квазигруппы в криптографии: примеры симметричных схем

Основная идея: использовать в качестве нелинейного компонента примитива некоторое квазигрупповое преобразование $f: Q^n \rightarrow Q^n$.

- Строительные блоки: E- и D-преобразования, их свойства⁵;
- «Односторонняя функция», основанная на квазигрупповых преобразованиях; на её основе — хэш-функция Edon-R⁶.

⁵Bakeva и Dimitrova, «Some probabilistic properties of quasigroup processed strings useful for cryptanalysis»; Markovski, Gligoroski и Bakeva, «Quasigroup String Processing: Part 1»; Markovski и Bakeva, «Quasigroup string processing: Part 4».

⁶Gligoroski, Markovski и Kocarev, «Edon-R, An Infinite Family of Cryptographic Hash Functions.»; Gligoroski и др., «Cryptographic hash function Edon-R'»; Gligoroski, «On a family of minimal candidate one-way functions and one-way permutations.»; Gligoroski и Knapskog, «Edon-R (256,384,512)—an efficient implementation of Edon-R family of cryptographic hash functions».

Квазигруппы в криптографии: примеры симметричных схем-2

Основная идея: использовать в качестве нелинейного компонента примитива некоторое квазигрупповое преобразование $f: Q^n \rightarrow Q^n$.

- Генераторы псевдослучайных чисел⁷.
- Блочный шифр INRU⁸ (нелинейное преобразование — умножение в специально подобранной квазигруппе).
- Низкоресурсная (lightweight) хэш-функция GAGE и AEAD-алгоритм InGAGE (см. <http://gageingage.org/>, также⁹).
- Поточный шифр Edon80¹⁰.

⁷Dimitrova и Markovski, «On quasigroup pseudo random sequence generator»; Markovski, «Quasigroup string processing and applications in cryptography»; Markovski, Gligoroski и Kocarev, «Unbiased random sequences from quasigroup string transformations»; Markovski, Gligoroski и Markovski, «Classification of quasigroups by random walk on torus».

⁸Tiwari и др., «INRU: A Quasigroup Based Lightweight Block Cipher».

⁹Gligoroski, *On the S-box in GAGE and InGAGE*; Gligoroski и др., «GAGE and InGAGE».

¹⁰Gligoroski, Markovski и Knapskog, «The stream cipher Edon80».

Квазигруппы в криптографии: примеры асимметричных схем

- Основная идея: подобрать такое нелинейное (обычно квадратичное) преобразование \mathcal{P} , что вычисление \mathcal{P} и \mathcal{P}^{-1} сделать «легко», а затем «скрыть» структуру \mathcal{P} , взяв обратимые линейные преобразования \mathcal{S} и \mathcal{T} и рассмотрев композицию

$$\mathcal{F}(x) = \mathcal{S}(\mathcal{P}(\mathcal{T}(x))).$$

- Асимметричные криптопримитивы — аналоги пост-квантовых схем multivariate cryptography¹¹.

¹¹Chen, Knapskog и Gligoroski, «Multivariate quadratic quasigroups (MQQs): Construction, bounds and complexity»; Faugère и др., «A polynomial-time key-recovery attack on MQQ cryptosystems»; Gligoroski, Markovski и Knapskog, «A public key block cipher based on multivariate quadratic quasigroups», «Multivariate quadratic trapdoor functions based on multivariate quadratic quasigroups»; Gligoroski и др., «MQQ-SIG: An ultra-fast and provably CMA resistant digital signature scheme»; Mohamed и др., «Algebraic attack on the MQQ public key cryptosystem».

Квазигруппы в криптографии: примеры асимметричных схем-2

- Основная идея: построить квазигруппу таким образом, чтобы в ней выполнялось свойство перестановочности (левых/правых/смешанных) степеней.
- Схемы — аналоги протокола Диффи-Хеллмана выработки общего ключа¹², гомоморфное шифрование¹³.
- Также приложения в теории кодирования¹⁴; более подробно вопрос освещен в¹⁵.

¹²Катышев, Марков и Нечаев, «Использование неассоциативных группоидов для реализации процедуры открытого распределения ключей»; Барышников и Катышев, «Использование неассоциативных структур для построения алгоритмов открытого распределения ключей».

¹³Марков, Михалёв и Кислицын, «Неассоциативные структуры в гомоморфной криптографии»; Gribov, Zolotykh и Mikhalev, «A construction of algebraic cryptosystem over the quasigroup ring».

¹⁴Гонсалес и др., «Рекурсивные МДР-коды и рекурсивно дифференцируемые квазигруппы», «Групповые коды и их неассоциативные обобщения»; Markov, Mikhalev и Nechaev, «Nonassociative Algebraic Structures in Cryptography and Coding».

¹⁵Глухов, «О применениях квазигрупп в криптографии»; Артамонов, «Квазигруппы и их приложения»; Shcherbacov, *Elements of Quasigroup Theory and Applications*.

Как задать квазигруппу?

- В общем случае квазигруппа над множеством Q задается таблицей умножения размера $|Q| \times |Q|$; это много.
- Случайная генерация (поиск + отсев) квазигрупп из некоторого узкого класса¹⁶.
- Итеративное построение из более «маленьких» (а-ля прямые произведения)¹⁷.
- Изотопы некоторых «хорошо изученных» групп (например, изотоп группы точек эллиптической кривой¹⁸, модульное вычитание¹⁹).
- Функциональное задание квазигруппы: поговорим о нём подробнее.

¹⁶Chen, Knapskog и Gligoroski, «Multivariate quadratic quasigroups (MQQs): Construction, bounds and complexity»; Gligoroski, Markovski и Knapskog, «A public key block cipher based on multivariate quadratic quasigroups».

¹⁷Грибов, «Алгебраические неассоциативные структуры и их приложения в криптографии»; Gligoroski и др., «Cryptographic hash function Edon-R'».

¹⁸Марков, Михалёв и Нечаев, «Неассоциативные алгебраические структуры в криптографии и кодировании».

¹⁹Snášel и др., «Hash functions based on large quasigroups».

Функциональное задание квазигруппы

- Можно перейти от табличного задания операции к функциональному²⁰:

$$x \circ y = z \Leftrightarrow z_i = f_i(x_1, \dots, x_n, y_1, \dots, y_n).$$

- Рассмотрим для простоты случай $Q = \{0, 1\}^n$: хотим задать структуру квазигруппы на Q с помощью семейства булевых функций.
- Какие условия надо наложить на функции f_i , чтобы операция $x \circ y$ задавала структуру квазигруппы на Q ?

²⁰Носов и Панкратьев, «О функциональном задании латинских квадратов».

Содержание доклада

- 1 Мотивация и основные определения
- 2 Правильные семейства функций
- 3 Характеризация в терминах несамодвойственности

Правильные семейства булевых функций

Правильное семейство

Семейство булевых функций $\mathcal{F}: \{0, 1\}^n \rightarrow \{0, 1\}^n$ называется правильным^a, если для любых двух наборов $x \neq y$ найдется такая координата i , что $x_i \neq y_i$, но $f_i(x) = f_i(y)$.

^aНосов, «Построение классов латинских квадратов в булевой базе данных».

Правильные семейства можно задавать не только над $\{0, 1\}^n$, но над логикой любой значности k ²¹, над произвольными группами²²; над прямыми произведениями квазигрупп²³, d -квазигрупп²⁴.

²¹Носов, «Построение параметрического семейства латинских квадратов в векторной базе данных».

²²Носов и Панкратьев, «Латинские квадраты над абелевыми группами».

²³Galatenko, Nosov и Pankratiev, «Latin squares over quasigroups».

²⁴Плаксина, «Построение параметрического семейства многомерных латинских квадратов».

Правильные семейства задают классы квазигрупп

Если семейство $\mathcal{F} = (f_1, \dots, f_n)$ — правильное, то отображение вида

$$(x, y) \rightarrow z = x \oplus y \oplus \mathcal{F}(\pi_1(x_1, y_1), \dots, \pi_n(x_n, y_n))$$

задает квазигрупповую операцию **при любом выборе** внутренних функций π_1, \dots, π_n .

Примеры правильных семейств

- Константы $f_i \equiv \text{const}_i$.
- Треугольные семейства²⁵ ($\text{const}, f_2(x_1), f_3(x_1, x_2), \dots, f_n(x_1, \dots, x_{n-1})$.)
- Семейства вида²⁶

$$\begin{bmatrix} 0 \\ x_1 \\ x_1 \oplus x_2 \\ \vdots \\ x_1 \oplus x_2 \oplus \dots \oplus x_{n-1} \end{bmatrix} \oplus \begin{bmatrix} \bigoplus_{i < j, i, j \neq 1}^n x_i x_j \\ \bigoplus_{i < j, i, j \neq 2}^n x_i x_j \\ \bigoplus_{i < j, i, j \neq 3}^n x_i x_j \\ \vdots \\ \bigoplus_{i < j, i, j \neq n}^n x_i x_j \end{bmatrix}.$$

²⁵ Носов и Панкратьев, «Латинские квадраты над абелевыми группами».

²⁶ Царегородцев, «О свойствах правильных семейств булевых функций».

О сложности распознавания свойства правильности

- Пусть семейство задано набором КНФ.
- Задача распознавания правильности: на вход подается семейство \mathcal{F} , выдать 1, если \mathcal{F} — правильное, и 0 иначе.
- В таком случае задача распознавания правильности лежит в классе coNP: сертификатом является пара значений x, y , для которых нарушено условие правильности.
- Более того, известно²⁷, что эта задача является coNP-полной.
- Следовательно, надеяться на полиномиальный алгоритм (по числу переменных в семействе) не приходится.

²⁷Носов, «Критерий регулярности булевского неавтономного автомата с разделенным входом»; Gartner и Antonis, «The Complexity of Recognizing Unique Sink Orientations».

Содержание доклада

- 1 Мотивация и основные определения
- 2 Правильные семейства функций
- 3 Характеризация в терминах несамодвойственности

Проекция семейства

- Пусть задано \mathcal{F}_n — семейство размера n на E_k^n .
- Проекция семейства $\Pi_i^a(\mathcal{F}_n)$ — семейство \mathcal{G}_{n-1} , полученное из \mathcal{F}_n подстановкой вместо x_i константы a и вычеркиванием функции f_i :

$$\mathcal{G}_{n-1}(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n) = \Pi_i^a(\mathcal{F}_n) = \begin{bmatrix} f_1(x_1, \dots, x_{i-1}, a, x_{i+1}, \dots, x_n) \\ \vdots \\ f_{i-1}(x_1, \dots, x_{i-1}, a, x_{i+1}, \dots, x_n) \\ f_{i+1}(x_1, \dots, x_{i-1}, a, x_{i+1}, \dots, x_n) \\ \vdots \\ f_n(x_1, \dots, x_{i-1}, a, x_{i+1}, \dots, x_n) \end{bmatrix}.$$

- Кратная проекция семейства:

$$\Pi_{i_1, \dots, i_k}^{a_1, \dots, a_k}(\mathcal{F}_n) = \Pi_{i_1}^{a_1} \left(\dots \Pi_{i_k}^{a_k}(\mathcal{F}_n) \dots \right).$$

Самодвойственные семейства

Самодвойственное семейство

Отображение $F: \mathbb{E}_2^n \rightarrow \mathbb{E}_2^k$ самодвойственно, если для любого набора $x \in \mathbb{E}_2^n$ выполняется свойство $F(\bar{x}) = \overline{F(x)}$.

Лемма

Пусть семейство булевых функций $\mathcal{F}: E_2^n \rightarrow E_2^n$ таково, что найдется набор $\gamma \in E_2^n$, для которого выполнено свойство $\overline{\mathcal{F}(\gamma)} = \mathcal{F}(\bar{\gamma})$. Тогда существует самодвойственная проекция \mathcal{F} .

Характеризация в терминах несамодвойственности

Основная теорема

Семейство $\mathcal{F}_n: \mathbb{E}_2^n \rightarrow \mathbb{E}_2^n$ правильно тогда и только тогда, когда каждая из его проекций $\Pi_{i_1, \dots, i_k}^{a_1, \dots, a_k}(\mathcal{F})$ не является самодвойственным булевым отображением.

- Перебираем все проекции исходного семейства \mathcal{F} , проверяя выполнение свойства самодвойственности на **единственной** паре наборов из проекции.
- Если нашлась проекция, для которой свойство самодвойственности выполнено, то алгоритм останавливает работу и выдаёт результат «семейство \mathcal{F} не является правильным»: по лемме найдётся \mathcal{G} — самодвойственная проекция $\mathcal{F} \Rightarrow \mathcal{F}$ не является правильным.
- Если семейство \mathcal{F} проходит все проверки, то для \mathcal{F} и всех его проекций **не выполнено** свойство самодвойственности: если бы существовал хотя бы один набор α , для которого $\overline{\mathcal{F}(\alpha)} = \mathcal{F}(\bar{\alpha})$, то по лемме нашлась бы **полностью** самодвойственная проекция, что было исключено в ходе проверок.

Алгоритм проверки правильности

Цикл по всем возможным наборам $x \in \{0, 1, 2\}^n$:

- ❶ построить два набора $y, z \in E_2^n$ по правилу:
 - ▶ если $x_i \in \{0, 1\}$, то положить $y_i \leftarrow x_i, z_i \leftarrow x_i$,
 - ▶ в противном случае положить $y_i \leftarrow 0, z_i \leftarrow 1$,
- ❷ если существует номер j , что $y_j \neq z_j$, и $f_j(y) \neq f_j(z)$, вернуть ответ: « \mathcal{F} не является правильным».

Если все проверки пройдены успешно, то вернуть « \mathcal{F} является правильным».

Об алгоритме

- Сложность предложенного алгоритма: 2×3^n операций вычисления значения семейства в точке.
- «Наивный» алгоритм (проверка определения): 4^n операций вычисления значения семейства в точке.
- К сожалению, по видимому результат не верен для логик значности $k > 2$.

Заключение






- Правильные семейства могут быть использованы для задания параметрического класса квазигрупп; квазигруппы, в свою очередь, могут использоваться при построении различных криптографических примитивов.
- Задача распознавания правильности является сложной; в работе удалось немного понизить её сложность для булева случая (но она всё ещё остается экспоненциальной по числу переменных в семействе).
- Пока что не удалось перенести результат на случай k -значной логики при $k > 2$.

Спасибо за внимание!








`github.com/kirtsar/proper_recognition`






Библиография I

-  Нечаев, Александр Александрович. «Конечные квазифробениусовы модули, приложения к кодам и линейным рекуррентам». В: *Фундаментальная и прикладная математика* 1.1 (1995), с. 229—254.
-  Носов, В. А. «Критерий регулярности булевского неавтономного автомата с разделенным входом». В: *Интеллектуальные системы. Теория и приложения* 3.3-4 (1998), с. 269—280.
-  Носов, В. А. «Построение классов латинских квадратов в булевой базе данных». В: *Интеллектуальные системы. Теория и приложения* 4.3-4 (1999), с. 307—320. ISSN: 2075-9460; 2411-4448.
-  Носов, В. А. «Построение параметрического семейства латинских квадратов в векторной базе данных». В: *Интеллектуальные системы. Теория и приложения* 8.1-4 (2006), с. 517—529. ISSN: 2075-9460; 2411-4448.
-  Носов, В. А. и А. Е. Панкратьев. «Латинские квадраты над абелевыми группами». В: *Фундаментальная и прикладная математика* 12.3 (2006), с. 65—71.

Библиография II

-  Глухов, М.М. «О применениях квазигрупп в криптографии». В: *Прикладная дискретная математика* 2 (2) (2008), с. 28—32.
-  Носов, В. А. и А. Е. Панкратьев. «О функциональном задании латинских квадратов». В: *Интеллектуальные системы. Теория и приложения* 12.1-4 (2008), с. 317—332. ISSN: 2075-9460; 2411-4448.
-  Плаксина, И. А. «Построение параметрического семейства многомерных латинских квадратов». В: *Интеллектуальные системы. Теория и приложения* 18.2 (2014), с. 323—330.
-  Катышев, Сергей Юрьевич, Виктор Тимофеевич Марков и Александр Александрович Нечаев. «Использование неассоциативных группоидов для реализации процедуры открытого распределения ключей». В: *Дискретная математика* 26.3 (2014), с. 45—64.
-  Грибов, А. В. «Алгебраические неассоциативные структуры и их приложения в криптографии». Дис. ... док. Московский государственный университет им. М. В. Ломоносова, 2015.

Библиография III

-  Марков, В. Т., А. В. Михалёв и А. А. Нечаев. «Неассоциативные алгебраические структуры в криптографии и кодировании». В: *Фундаментальная и прикладная математика* 21.4 (2016), с. 99—124.
-  Барышников, Андрей Владимирович и Сергей Юрьевич Катышев. «Использование неассоциативных структур для построения алгоритмов открытого распределения ключей». В: *Математические вопросы криптографии* 9.4 (2018), с. 5—30.
-  Артамонов, В. А. «Квазигруппы и их приложения». В: *Чебышевский сборник* 19.2 (66) (2018), с. 111—122.
-  Романьков, Виталий Анатольевич. *Алгебраическая криптология: монография*. ОмГУ им. Ф. М. Достоевского, 2020.
-  Марков, Виктор, Александр Васильевич Михалёв и Евгений Сергеевич Кислицын. «Неассоциативные структуры в гомоморфной криптографии». В: *Фундаментальная и прикладная математика* 23.2 (2020), с. 209—215.
-  Царегородцев, К.Д. «О свойствах правильных семейств булевых функций». В: *Дискретная математика* 33.1 (2021), с. 91—102.

Библиография IV



Молдовян, Дмитрий Николаевич, Александр Андреевич Молдовян и Николай Андреевич Молдовян. «Новая концепция разработки постквантовых алгоритмов цифровой подписи на некоммутативных алгебрах». В: *Вопросы кибербезопасности* 1 (47) (2022), с. 18—25.



Гонсалес, С. и др. «Рекурсивные МДР-коды и рекурсивно дифференцируемые квазигруппы». В: *Дискретная математика* 10.2 (1998), с. 3—29.



Гонсалес, С. и др. «Групповые коды и их неассоциативные обобщения». В: *Дискретная математика* 16.1 (2004), с. 146—156.



Bakeva, Verica и Vesna Dimitrova. «Some probabilistic properties of quasigroup processed strings useful for cryptanalysis». Англ. В: *ICT Innovations 2010: Second International Conference, ICT Innovations 2010, Ohrid Macedonia, September 12-15, 2010. Revised Selected Papers 2*. Springer. 2011, с. 61—70.









Bernstein, Daniel J., Johannes Buchmann и Erik Dahmen. *Post-quantum cryptography*. Springer Berlin, Heidelberg, 2009. DOI: <https://doi.org/10.1007/978-3-540-88702-7>.

Библиография V

-  Chen, Yanling, Svein Johan Knapskog и Danilo Gligoroski. «Multivariate quadratic quasigroups (MQQs): Construction, bounds and complexity». В: *Submitted to ISIT 2010* (2010), с. 14.
-  Dimitrova, V. и J Markovski. «On quasigroup pseudo random sequence generator». Англ. В: *Proceedings of the 1st Balkan Conference in Informatics, Thessaloniki*. 2004.
-  Faugère, Jean-Charles и др. «A polynomial-time key-recovery attack on MQQ cryptosystems». В: *IACR International Workshop on Public Key Cryptography*. Springer. 2015, с. 150—174.
-  Galatenko, A. V., V. A. Nosov и A. E. Pankratiev. «Latin squares over quasigroups». Англ. В: *Lobachevskii Journal of Mathematics* 41.2 (2020), с. 194—203.
-  Gartner, B. и T. Antonis. «The Complexity of Recognizing Unique Sink Orientations». Англ. В: *Leibniz International Proceedings in Informatics, LIPIcs* 30 (март 2015).
-  Gligoroski, D., S. Markovski и S. J. Knapskog. «The stream cipher Edon80». Англ. В: *New stream cipher designs*. Springer, 2008, с. 152—169.






Библиография VI

-  Gligoroski, D., S. Markovski и L. Kocarev. «Edon-R, An Infinite Family of Cryptographic Hash Functions.» . Англ. В: *International Journal of Security and Networks* 8.3 (2009), с. 293—300.
-  Gligoroski, D. и др. «Cryptographic hash function Edon-R' » . Англ. В: *2009 Proceedings of the 1st International Workshop on Security and Communication Networks*. IEEE. 2009, с. 1—9.
-  Gligoroski, Danilo. «On a family of minimal candidate one-way functions and one-way permutations.» . Англ. В: *Int. J. Netw. Secur.* 8.3 (2009), с. 211—220.
-  — . *On the S-box in GAGE and InGAGE*. Англ.
<http://gageingage.org/upload/LWC2019NISTWorkshop.pdf>. 2019.
-  Gligoroski, Danilo и Svein Johan Knapskog. «Edon-R (256,384,512)—an efficient implementation of Edon-R family of cryptographic hash functions» . Англ. В: *Commentationes Mathematicae Universitatis Carolinae* 49.2 (2008), с. 219—239.
-  Gligoroski, Danilo, Smile Markovski и Svein Johan Knapskog. «A public key block cipher based on multivariate quadratic quasigroups» . В: *arXiv preprint arXiv:0808.0247* (2008).





Библиография VII

-  Gligoroski, Danilo, Smile Markovski и Svein Johan Knapskog. «Multivariate quadratic trapdoor functions based on multivariate quadratic quasigroups». В: *Proceedings of the American Conference on Applied Mathematics*. 2008, с. 44—49.
-  Gligoroski, Danilo и др. «GAGE and InGAGE». Англ. В: *A Submission to the NIST Lightweight Cryptography Standardization Process* (2019).
-  Gligoroski, Danilo и др. «MQQ-SIG: An ultra-fast and provably CMA resistant digital signature scheme». В: *International Conference on Trusted Systems*. Springer. 2011, с. 184—203.
-  Gribov, Aleksei Viktorovich, Pavel Andreevich Zolotych и Aleksandr Vasil'evich Mikhalev. «A construction of algebraic cryptosystem over the quasigroup ring». В: *Matematicheskie Voprosy Kriptografii [Mathematical Aspects of Cryptography]* 1.4 (2010), с. 23—32.
-  Markov, V. T., A. V. Mikhalev и A. A. Nechaev. «Nonassociative Algebraic Structures in Cryptography and Coding». Англ. В: *Journal of Mathematical Sciences* 245.2 (2020).
-  Markovski, S, D. Gligoroski и V. Bakeva. «Quasigroup String Processing: Part 1». Англ. В: *Proc. of Maked. Academ. of Sci. and Arts for Math. And Tect. Sci.* XX (1999), с. 157—162.

Библиография VIII

-  Markovski, Smile. «Quasigroup string processing and applications in cryptography». Англ. В: *Proc. 1-st Inter. Conf. Mathematics and Informatics for industry*. Т. 1002. 2003, с. 14—16.
-  Markovski, Smile и Verica Bakeva. «Quasigroup string processing: Part 4». Англ. В: *Contributions, Section of Natural, Mathematical and Biotechnical Sciences 27.1-2* (2017).
-  Markovski, Smile, Danilo Gligoroski и Ljupco Kocarev. «Unbiased random sequences from quasigroup string transformations». Англ. В: *International workshop on fast software encryption*. Springer. 2005, с. 163—180.
-  Markovski, Smile, Danilo Gligoroski и Jasen Markovski. «Classification of quasigroups by random walk on torus». Англ. В: *Journal of applied mathematics and computing* 19.1-2 (2005), с. 57—75.
-  Mohamed, Mohamed Saied Emam и др. «Algebraic attack on the MQQ public key cryptosystem». В: *Cryptology and Network Security: 8th International Conference, CANS 2009, Kanazawa, Japan, December 12-14, 2009. Proceedings 8*. Springer. 2009, с. 392—401.

Библиография IX

-  Myasnikov, Alexei, Vladimir Shpilrain и Alexander Ushakov. *Non-commutative cryptography and complexity of group-theoretic problems*. American Mathematical Soc., 2011.
-  Shcherbacov, V. *Elements of Quasigroup Theory and Applications*. Англ. Chapman и Hall/CRC, 2017.
-  Snášel, Václav и др. «Hash functions based on large quasigroups». Англ. В: *Computational Science–ICCS 2009: 9th International Conference Baton Rouge, LA, USA, May 25-27, 2009 Proceedings, Part I 9*. Springer. 2009, с. 521—529.
-  Tiwari, Sharwan K и др. «INRU: A Quasigroup Based Lightweight Block Cipher». Англ. В: *arXiv preprint arXiv:2112.07411* (2021).