МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М. В. ЛОМОНОСОВА

На правах рукописи

Чередник Игорь Владимирович

Использование бинарных функциональных сетей при построении кратно транзитивных множеств блочных преобразований

Специальность 05.13.19 — «Методы и системы защиты информации, информационная безопасность»

АВТОРЕФЕРАТ

диссертации на соискание ученой степени
кандидата физико-математических наук

Москва — 2021

Работа выполнена на кафедре математической теории интеллектуальных систем Механико-математического факультета ФГБОУ ВО «Московский государственный университет имени М. В. Ломоносова».

Научные руководители:

Черемушкин Александр Васильевич,
доктор физико-математических наук,
профессор,
член-корреспондент Академии криптографии РФ

Галатенко Алексей Владимирович,
кандидат физико-математических наук,
старший научный сотрудник кафедры МаТИС
Механико-математического факультета
МГУ имени М. В. Ломоносова

Официальные оппоненты:

Логачев Олег Алексеевич,
доктор физико-математических наук,
ведущий научный сотрудник Института проблем
информационной безопасности факультета ВМК
МГУ имени М. В. Ломоносова

Пудовкина Марина Александровна,
доктор физико-математических наук,
профессор отделения интеллектуальных
кибернетических систем офиса образовательных
программ Института интеллектуальных
кибернетических систем НИЯУ «МИФИ»

Афонин Сергей Александрович,
кандидат физико-математических наук,
ведущий научный сотрудник НИИ механики
МГУ имени М. В. Ломоносова

Защита состоится 24 ноября 2021 г. в 16 часов 45 минут на заседании диссертационного совета МГУ.05.01 на базе ФГБОУ ВО «Московский государственный университет имени М. В. Ломоносова» по адресу: 119234, Москва, ГСП-1, Ленинские горы, д. 1, ФГБОУ ВО «Московский государственный университет имени М. В. Ломоносова», Механико-математический факультет, аудитория 14-08.
E-mail: vasenin@msu.ru

С диссертацией можно ознакомиться в отделе диссертаций научной библиотеки МГУ имени М. В. Ломоносова (Москва, Ломоносовский проспект, д. 27) и на сайте ИАС «ИСТИНА»: https://istina.msu.ru/dissertations/397192299/

Автореферат разослан 20 октября 2021 г.

Ученый секретарь
диссертационного совета
МГУ.05.01
канд. физ.-мат. наук — Кривчиков Максим Александрович

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы. Диссертация посвящена поиску новых решений по синтезу кратно транзитивных классов блочных преобразований, архитектура которых представляет собой уникальную (для класса) сеть, с узлами отвечающими одной бинарной операции.

Эффективно реализуемые кратно транзитивные классы преобразований имеют важное значение для проектирования узлов переработки информации в области защиты конфиденциальных данных, поскольку отсутствие кратной транзитивности у семейства преобразований, выполняемых узлом, фактически означает наличие запретов в выходных последовательностях данных узлов и в некоторых случаях позволяет идентифицировать начальные состояния и/или часть постоянных параметров изучаемых узлов. Это обстоятельство обосновывает актуальность построения эффективно реализуемых кратно транзитивных семейств блочных преобразований.

Степень разработанности темы. В последнее время при разработке систем защиты информации активно исследуется возможность использования неассоциативных алгебраических структур. Особое место при таких исследованиях занимают квазигруппы[1, 2]. В ряде работ[3, 4, 5, 6] определяются и исследуются семейства блочных преобразований $\Omega^n \to \Omega^n$, реализуемые следующими наборами формул

$$\Big(a * x_1, (a * x_1) * x_2, \ldots, \big((a * x_1) * \ldots\big) * x_n\Big), \quad a \in \Omega, \tag{1}$$

где $*$ — квазигрупповая операция на конечном множестве Ω. При этом квазигрупповая операция $*$ является фиксированной и параметризация класса преобразований достигается за счет выбора «начального» элемента $a \in \Omega$. Глигороски, Марковски, Щербаков и др. предлагают использовать рассмотренную конструкцию в качестве основы для построения таких различных узлов переработки информации, как блочные шифры[7], поточные шифры[8], однонаправленные

[1] *Глухов М. М.* О применении квазигрупп в криптографии / М. М. Глухов // ПДМ. — 2008. — №2. — С. 28–32.

[2] *Shcherbakov V. A.* Quasigroups in cryptology / V. A. Shcherbakov // arXiv:1007.3572v1

[3] *Gligoroski D.* Quasigroup String Processing: Part1 / Gligoroski D., Markovski S. and Bakeva V. // Proc. of Maked. Academ. of Sci. and Arts for Math. And Tech. Sci. XX. — 1999. — 1–2. — P. 13–28.

[4] *Markovski S.* Quasigroup String Processing: Part2 / Markovski S. and Kusacatov V. // Proc. of Maked. Academ. of Sci. and Arts for Math. And Tech. Sci. XXI. — 2000. — 1–2. — P. 15–32.

[5] *Markovski S.* Quasigroup String Processing: Part3 / Markovski S. and Kusacatov V. // Proc. of Maked. Academ. of Sci. and Arts for Math. And Tech. Sci. XXIII. — 2002. — 1–2. — P. 7–27.

[6] *Markovski S.* Quasigroup String Processing: Part4 / Markovski S. and Bakeva V. // Proc. of Maked. Academ. of Sci. and Arts for Math. And Tech. Sci. XXVII. — 2006. — 1–2. — P. 41–53.

[7] *Gligoroski D.* A public key block cipher based on multivariate quadratic quasigroups / Gligoroski D., Markovski S. and Knapskog S. J. // http://arxiv.org/0808.0247:22 pages, 2008

[8] *Gligoroski D.* Stream cipher based on quasigroup string transformations / Gligoroski D. // arXiv:cs/0403043v2

функции[9], и пр.[10, 11]. В качестве хеш-функций они предлагают[12] использовать сжимающие отображения, реализуемые «цепными» формулами типа

$$((a * x_1) * \dots) * x_n, \quad a \in \Omega. \tag{2}$$

При первичном анализе стойкости узлов переработки/защиты информации, которые основаны на блочных преобразованиях, реализуемых наборами формул вида (1), и сжимающих отображениях вида (2), возникает классическая задача исследования функциональной полноты квазигруппы $*$. И в этом направлении можно отметить значительные результаты, полученные В. А. Артамоновым[13], а также А. В. Галатенко, А. Е. Панкратьевым и С. Б. Родиным[14, 15]. Однако, как было отмечено выше, для семейств преобразований, используемых в узлах защиты информации, одной из значимых характеристик является кратная транзитивность данного семейства. А в случае преобразований, реализуемых простыми наборами формул вида (1), во-первых, неизвестно являются ли данные классы блочных преобразований хотя бы транзитивными, и, во-вторых, отсутствуют практически эффективные методы, которые позволяли бы это выяснить или гарантировать.

Кроме того, при проведении анализа реальных узлов защиты информации редко возникает задача исследования семейств преобразований, которые допускают описание в терминах примитивных формул вида (1) или (2). Поэтому в диссертации рассматривается существенно более общая модель построения классов блочных преобразований, которые определяются фиксированным набором формул и параметрически зависят от выбора бинарной операции.

Пусть Ω — произвольное конечное множество, $\mathcal{B}(\Omega)$ — множество всех бинарных операций, определенных на Ω, $\{x_1, \dots, x_n\}$ — множество переменных и $*$ — общий символ бинарной операции. Произвольная формула $w(x_1, \dots, x_n)$ в алфавите $\{x_1, \dots, x_n, *\}$ при сопоставлении символу $*$ конкретной бинарной операции $F \in \mathcal{B}(\Omega)$ реализует функцию $w^F \colon \Omega^n \to \Omega$, а набор формул $(w_1, \dots, w_m)$ реализует отображение $(w_1^F, \dots, w_m^F) \colon \Omega^n \to \Omega^m$.

---

[9] *Gligoroski D.* Candidate one-way functions and one-way permutations based on quasigroup string transformations / Gligoroski D. // arXiv:cs/0510018v1

[10] *Dimitrova V.* On Quasigroup Pseudo Random Sequence Generators. / Dimitrova V., Markovski S. // In Proceedings of the 1st Balkan Conference in Informatics. — 2003. — P. 393–401.

[11] *Shcherbakov V. A.* Quasigroups in cryptology / V. A. Shcherbakov // arXiv:1007.3572v1

[12] *Gligoroski D.* Edon-R, An infinite family of cryptographic hash functions / Gligoroski D., Markovski S. and Kocarev L. // http://csrc.nist.gov.gov/pki/HashWorkshop/2006/Papers

[13] *Артамонов В. А.* Квазигруппы и их приложения / В. А. Артамонов // Чебышевский сб. — 2018. — т. 19. — №2. — С. 111–122.

[14] *Галатенко А. В.* О полиномиально полных квазигруппах простого порядка / А. В. Галатенко, А. Е. Панкратьев, С. Б. Родин // Алгебра и логика. — 2018. — т. 57. — №5. — С. 509–521.

[15] *Галатенко А. В.* О сложности проверки полиномиальной полноты конечных квазигрупп / А. В. Галатенко, А. Е. Панкратьев // Дискрет. матем. — 2018. — т. 30. — №4. — С. 3–11.

Объект исследований. Объектом исследований диссертации являются классы блочных преобразований

$$\{(w_1^F, \ldots, w_m^F) \,:\, F \in \mathcal{K}\}, \quad \mathcal{K} \subset \mathcal{B}(\Omega), \tag{3}$$

реализуемые произвольным фиксированным набором формул $(w_1, \ldots, w_n)$ при выборе различных бинарных операций $F \in \mathcal{K}$.

Один из способов построения произвольного набора формул $(w_1, \ldots, w_m)$ состоит в последовательном преобразовании набора переменных $(x_1, \ldots, x_n)$. Каждая последовательность преобразований набора переменных $(x_1, \ldots, x_n)$ в набор формул $(w_1, \ldots, w_m)$ допускает наглядное представление в виде подходящей бинарной функциональной сети Σ, у которой степень захода каждой вершины не превосходит 2. При этом удобно говорить, что сеть Σ описывает преобразование набора переменных $(x_1, \ldots, x_n)$ в набор формул $(w_1, \ldots, w_m)$, а при выборе бинарной операции $F \in \mathcal{B}(\Omega)$ реализует отображение $\Sigma^F = (w_1^F, \ldots, w_m^F)$.

Если сеть Σ описывает преобразование набора переменных $(x_1, \ldots, x_n)$ в набор формул $(w_1, \ldots, w_n)$, при котором каждый промежуточный набор содержит ровно n формул (каждый слой сети Σ содержит ровно n вершин), то будем называть Σ сетью постоянной ширины. Сети постоянной ширины представляют особый интерес с точки зрения удобства практической реализации.

Предложенный «сетевой» подход к описанию класса преобразований (3) является достаточно естественным развитием конструкции классической сети Фейстеля[16, 17, 18, 19] и ее известных обобщений[20, 21, 22, 23] с той отличительной особенностью, что бинарные операции (используемые в узлах сети) предполагаются зависящими нетривиальным образом от секретных параметров системы защиты информации и уникальными для каждой реализации — указанная особенность не позволяет составить между обрабатываемыми данными и секретны-

[16] *Shimizu A., Miyaguchi S.* Fast Data Encipherment Algorithm FEAL / A. Shimizu // Advances in Cryptology — EUROCRYPT '87: Workshop on the Theory and Application of Cryptographic Techniques — 1988. — P. 267–278.

[17] *Y. Zheng, T. Matsumoto, and H. Imai* On the construction of block ciphers provably secure and not relying on any unproved hypotheses / Y. Zheng // CRYPTO '89, LNCS 435. — 1990. — P. 461–480.

[18] *Beaulieu R., Shors D., Smith J., Treatman-Clark S., Weeks B., and Wingers L.* The SIMON and SPECK Families of Lightweight Block Ciphers / R. Beaulieu // Cryptology ePrint Archive, Report 2013/404, 2013. http://eprint.iacr.org/2013/404.pdf

[19] *Menezes A. J., Oorschot P. C., Vanstone S. A.* Handbook of applied cryptography / A. J. Menezes // CRC Press. — 1996. — 816 p.

[20] *Nyberg K.* Generalized Feistel Networks / K. Nyberg // In: Kim, K.-c., Matsumoto, T. (eds.) ASIACRYPT 1996. LNCS. — vol. 1163. — P. 90–104.

[21] *Takeshi S., Naofumi H., Takafumi A., Akashi S.* High-performance ASIC Implementations of the 128-bit Block Cipher CLEFIA / S. Takeshi // 2008 IEEE International Symposium on Circuits and Systems — 2008.

[22] *Tomoyasu Suzaki, Kazuhiko Minematsu* Improving the Generalized Feistel / Tomoyasu Suzaki // International Workshop on Fast Software Encryption FSE 2010: Fast Software Encryption (Lecture Notes in Computer Science book series) vol. 6147. — P. 19–39.

[23] *Viet Tung Hoang, Phillip Rogaway* On Generalized Feistel Networks / Viet Tung Hoang // Annual Cryptology Conference CRYPTO 2010: Advances in Cryptology — CRYPTO 2010 (Lecture Notes in Computer Science book series) vol. 6223. — P. 613–630.

ми параметрами простые функциональные соотношения, из которых возможно эффективно определить хотя бы часть секретных параметров. Таким образом, предложенную в работе модель классов блочных преобразований (3) можно рассматривать в качестве аппроксимации классов блочных преобразований, которые реализуются в некоторых известных узлах защиты информации[24, 25, 26]. Также стоит отметить, что конструкция сети Фейстеля давно уже используется не только в качестве базы при проектировании блочных шифров, но и для построения специальных усложняющих преобразований, используемых в узлах обработки и защиты информации[27, 28, 29], случайных подстановок[30, 31], и даже линейных отображений[32].

Предмет исследований. Как известно, одним из трех основных принципов информационной безопасности является конфиденциальность обрабатываемой/передаваемой информации. Кратная транзитивность множества преобразований узла обработки и защиты информации является практическим приближением и следствием предложенного Шенноном теоретического понятия совершенной секретности и соответственно играет важную роль в обеспечении конфиденциальности. Предметом исследований является построение кратно транзитивных классов блочных преобразований

$$\{\Sigma^F \ : \ F \in \mathcal{R}(\Omega)\},$$

которые реализуются произвольной фиксированной бинарной функциональной сетью Σ постоянной ширины, а в качестве параметрического множества бинарных операций $\mathcal{R}(\Omega)$ используются следующие семейства бинарных операций:

- $\mathcal{Q}(\Omega)$ — все бинарные операции обратимые по обеим переменным (бинарные квазигруппы);

[24] *Schneier B.* Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish) / B. Schneier // Fast Software Encryption: Cambridge Security Workshop Cambridge, U. K., December 9–11,c1993 Proceedings / R. J. Anderson (Lecture Notes in Computer Science) — 1994. — vol. 809. — P. 191–204.

[25] *Schneier B., Kelsey J., Whiting D., Wagner D., Hall C., Ferguson N.* Twofish: A 128-bit Block Cipher / B. Schneier // http://www.counterpane.com/twofish.html

[26] *Adams C. M.* Constructing Symmetric Ciphers Using the CAST Design Procedure / C. M. Adams // Designs, Codes, and Cryptography — 1997. — vol. 12. — №3. — P. 283–316.

[27] *Fomin D. B.* New classes of 8-bit permutations based on a butterfly structure / D. B. Fomin // Матем. вопр. криптогр. — 2019. — т. 10. — №2. — С. 169–180.

[28] *Biryukov A., Perrin L., Udovenko A.* Reverse-engineering the s-box of Streebog, Kuznyechik and STRIBOBr1 / A. Biryukov // EUROCRYPT 2016, Lect. Notes Comput. Sci. — 2016. — vol. 9665. — №2. — P. 372–402.

[29] *Canteaut A., Duval S., Leurent G.* Construction of lightweight s-boxes using Feistel and MISTY structures (full version) / A. Canteaut // Cryptology ePrint Archive. Report 2015/711, http://eprint.iacr.org/2015/711.

[30] *Luby M., Rackoff C.* How to Construct Pseudo-random Permutations from Pseudo-random functions / M. Luby // SIAM J. Computing. — 1988. — vol. 17. — №2. — P. 373–386.

[31] *Naor M., Reingold O.* On the construction of pseudo-random permutations: Luby-Rackoff revisited / M. Naor // Journal of Cryptology, Springer. — 1997. — vol. 12. — №1. — P. 29–66.

[32] *Adnan Baysal, Mustafa Coban, and Mehmet Ozen* Feistel Like Construction of Involutory Binary Matrices With High Branch Number / Adnan Baysal // Cryptology ePrint Archive. Report 2016/751, https://eprint.iacr.org/2016/751.pdf

- $\mathcal{B}^*(\Omega)$ — все бинарные операции обратимые по правой переменной.

Использование класса $\mathcal{Q}(\Omega)$ в качестве параметризующего множества бинарных операций позволяет исследовать бинарные функциональные сети наиболее общего строения — данное обстоятельство обуславливает теоретическую значимость рассмотрения класса $\mathcal{Q}(\Omega)$. Однако, если обратимость глобальных преобразований, реализуемых сетью, является естественным требованием, то обратимость операции-параметра по обеим переменным в случаях некоторых сетей может оказаться завышенным требованием. Для достаточно широкого класса сетей в качестве параметризующего множества бинарных операций разумно рассматривать класс $\mathcal{B}^*(\Omega)$, который является максимальным в смысле обеспечения обратимости глобальных блочных преобразований, реализуемых сетью. При этом в случае класса $\mathcal{B}^*(\Omega)$ существенно упрощается генерация бинарной операции-параметра — данное обстоятельство обуславливает практическую значимость рассмотрения класса $\mathcal{B}^*(\Omega)$. В заключение, отметим, что в работе показана нецелесообразность использования каких-либо других классов бинарных операций (отличных от $\mathcal{Q}(\Omega)$ и $\mathcal{B}^*(\Omega)$) в качестве множества параметров.

Цели и задачи исследования. Основные цели исследования относятся к сфере анализа и синтеза систем защиты информации. В области анализа целью является разработка методов исследования кратной транзитивности произвольного класса блочных преобразований вида $\{\Sigma^F : F \in \mathcal{R}(\Omega)\}$. В области синтеза — построение на основе бинарных функциональных сетей кратно транзитивных классов блочных преобразований вида $\{\Sigma^F : F \in \mathcal{R}(\Omega)\}$.

Для достижения поставленных целей решаются следующие задачи:

1. Описание бинарных функциональных сетей постоянной ширины, которые определяют биективное преобразование при выборе любой бинарной операции из множества $\mathcal{R}(\Omega)$ (далее $\mathcal{R}$-биективные сети).

2. Разработка эффективных методов проверки кратной транзитивности класса блочных преобразований $\{\Sigma^F : F \in \mathcal{R}(\Omega)\}$, определяемых произвольной $\mathcal{R}$-биективной сетью Σ.

3. Разработка алгоритмов построения $\mathcal{R}$-биективных сетей Σ, для которых соответствующие классы преобразований $\{\Sigma^F : F \in \mathcal{R}(\Omega)\}$ обладают требуемой кратной транзитивностью.

4. Построение классов $\mathcal{R}$-биективных сетей Σ с небольшим количеством вершин, для которых соответствующие классы $\{\Sigma^F : F \in \mathcal{R}(\Omega)\}$ обладают требуемой кратной транзитивностью.

Научная новизна. Классы блочных преобразований, определяемые фиксированной бинарной функциональной сетью и некоторым семейством бинарных операций, впервые введены автором и ранее не изучались. Вследствие этого все теоретические результаты и практические приложения являются новыми, как по исходной теоретической постановке задач, так и по методам их решения. В частности, новым является полученный критерий биективности всех преобразований семейства $\{\Sigma^F : F \in \mathcal{R}(\Omega)\}$ в терминах строения $\mathcal{R}$-биективной сети Σ. Другим важным новым результатом является разработанный автором эффективный метод проверки кратной транзитивности класса блочных преобразований $\{\Sigma^F : F \in \mathcal{R}(\Omega)\}$, определяемых произвольной $\mathcal{R}$-биективной сетью Σ. Кроме того, в диссертации предложены алгоритмы построения $\mathcal{R}$-биективных сетей, для которых соответствующие классы блочных преобразований являются кратно транзитивными с требуемой кратностью.

Теоретическая и практическая значимость. Теоретическая значимость диссертации заключается в построении наглядной модели реализации класса блочных преобразований вида $\{\Sigma^F : F \in \mathcal{R}(\Omega)\}$ и разработанном аппарате разметки $\mathcal{R}$-биективных сетей, которые позволяют эффективно исследовать кратную транзитивность произвольных семейств преобразований вида $\{\Sigma^F : F \in \mathcal{R}(\Omega)\}$, а, кроме того, сравнительно просто строить разнообразные классы блочных преобразований вида $\{\Sigma^F : F \in \mathcal{R}(\Omega)\}$, обладающие требуемой кратной транзитивностью.

С точки зрения анализа, исследуемые в работе классы блочных преобразований $\{\Sigma^F : F \in \mathcal{R}(\Omega)\}$ можно использовать для аппроксимации множества блочных преобразований, реализуемых в некоторых известных узлах защиты информации, — указанное обстоятельство определяет практическую значимость разработанного в диссертации эффективного метода проверки кратной транзитивности произвольного класса преобразований вида $\{\Sigma^F : F \in \mathcal{R}(\Omega)\}$. С точки зрения синтеза, классы блочных преобразований $\{\Sigma^F : F \in \mathcal{R}(\Omega)\}$ допускают компактную и простую техническую реализацию, в большинстве своем обладают высокой аналитической сложностью и потому могут быть использованы в качестве определенных компонент узлов защиты информации — указанное обстоятельство определяет практическую значимость предложенных в работе алгоритмов построения кратно транзитивных классов преобразований $\{\Sigma^F : F \in \mathcal{R}(\Omega)\}$.

Соответствие диссертации паспорту специальности. Диссертация посвящена расширению арсенала математических методов в задачах анализа и синтеза узлов защиты информации и соответствует паспорту специальности 05.13.19 — «Методы и системы защиты информации, информационная безопасность» (физико-математические науки). А именно, в п. 1 паспорта в качестве

области исследований указана «Теория и методология обеспечения информационной безопасности и защиты информации», что соответствует развитию в диссертации теории так называемых бинарных функциональных сетей и их применению в узлах защиты информации. Далее, в п. 9 паспорта указаны «Модели и методы оценки защищенности информации и информационной безопасности объекта», что в полной мере отвечает разработанному методу проверки кратной транзитивности класса блочных преобразований $\{\Sigma^F : F \in \mathcal{R}(\Omega)\}$, определяемых произвольной $\mathcal{R}$-биективной сетью Σ. И, наконец, в п. 13 паспорта отмечены «Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности» — данному пункту соответствуют результаты второй и третьей глав диссертации, в которых предложены новые решения по синтезу транзитивных и кратно транзитивных классов блочных преобразований.

Основные методы исследования. Диссертационное исследование проводилось алгебраическими, комбинаторными и другими методами из области дискретной математики, включая использование теории графов.

Степень достоверности. Достоверность всех полученных результатов обосновывается корректностью постановок задач и строгими математическими доказательствами теоретических утверждений.

Основные положения, выносимые на защиту. На защиту выносятся обоснование актуальности решаемой задачи, методология, принятая для исследования, научная новизна, теоретическая и практическая значимость работы, а также следующие положения, которые подтверждаются результатами исследования, представленными в Заключении.

1. Предложена формальная модель для построения просто реализуемых классов блочных преобразований, параметрически зависящих от выбора бинарной операции. В рамках данной модели разработан эффективный метод проверки кратной транзитивности полного класса блочных преобразований.

2. Сформулированы и строго обоснованы алгоритмы построения кратно транзитивных классов блочных преобразований, архитектура которых представляет собой уникальную (для класса) сеть с узлами, отвечающими одной бинарной операции.

3. Построены практически значимые кратно транзитивные классы блочных преобразований, архитектура которых представляет собой уникальную (для класса) сеть небольшой сложности с узлами, отвечающими одной бинарной

операции из специальной репрезентативной выборки.

Апробация работы. Результаты диссертационного исследования докладывались на следующих семинарах и конференциях:

1. Всероссийская конференция «Сибирская научная школа-семинар с международным участием "Компьютерная безопасность и криптография"» — SIBECRYPT'17 (г. Красноярск, 4–8 сентября 2017 г.)

2. Всероссийская конференция «Сибирская научная школа-семинар с международным участием "Компьютерная безопасность и криптография"» — SIBECRYPT'18 (г. Абакан, 3–8 сентября 2018 г.)

3. семинар «Компьютерная безопасность» под руководством старшего научного сотрудника А.В. Галатенко, механико-математический факультет МГУ имени М. В. Ломоносова, 2020 г.;

4. семинар «Теория автоматов» под руководством д.ф.-м.н., проф. В.Б. Кудрявцева, механико-математический факультет МГУ имени М. В. Ломоносова, 2020 г.;

5. XXII научно-практическая конференция «РусКрипто'2020», (г. Солнечногорск, 27–29 марта 2020 г.).

Публикации по теме диссертации. Основное содержание диссертации опубликовано в 6 работах [1–6], из которых [1–4] — статьи в рецензируемых научных изданиях, рекомендованных для защиты в диссертационном совете МГУ по специальности 05.13.19 — «Методы и системы защиты информации, информационная безопасность» и входящих в списки Scopus и/или WoS, RSCI, а [5, 6] — публикации в материалах конференций.

Структура и объем диссертации. Диссертация состоит из введения, трех глав, заключения и списка литературы, включающего 66 наименований. Общий объем диссертации составляет 125 страниц.

СОДЕРЖАНИЕ РАБОТЫ

Во введении обосновывается актуальность диссертационной работы, формулируются цели и аргументируется научная новизна исследований, показывается теоретическая и практическая значимость полученных результатов, представляются выносимые на защиту научные положения.

В первой главе определяются основные понятия бинарных функциональных сетей, приводится описание класса биективных бинарных функциональных сетей постоянной ширины и предлагаются методы исследования бинарных функциональных сетей, которые используются в последующих главах диссертации.

В §1.1 строго определяются основные понятия бинарных функциональных сетей, которые позволяют наглядно представлять классы блочных преобразований вида $\{(w_1^F, \ldots, w_m^F) : F \in \mathcal{R}(\Omega)\}$ (определения 1.1–1.9).

Кратко опишем рассматриваемую в диссертации модель и проиллюстрируем ее наглядными примерами; при определении общих понятий и формулировке утверждений, справедливых для обоих классов $\mathcal{Q}(\Omega)$ и $\mathcal{B}^*(\Omega)$, будет использоваться универсальное обозначение $\mathcal{R}(\Omega)$.

Пусть Ω — произвольное конечное множество, $\mathcal{B}(\Omega)$ — множество всех бинарных операций, определенных на Ω, $\{x_1, \ldots, x_n\}$ — множество переменных и $*$ — общий символ бинарной операции. Произвольная формула $w(x_1, \ldots, x_n)$ в алфавите $\{x_1, \ldots, x_n, *\}$ при сопоставлении символу $*$ конкретной бинарной операции $F \in \mathcal{B}(\Omega)$ реализует функцию $w^F \colon \Omega^n \to \Omega$, а набор формул $(w_1, \ldots, w_m)$ реализует отображение $(w_1^F, \ldots, w_m^F) \colon \Omega^n \to \Omega^m$. При проведении анализа узлов переработки информации часто возникает задача исследования семейств отображений вида $\{(w_1^F, \ldots, w_m^F) : F \in \mathcal{R}(\Omega)\}$.

Один из способов построения произвольного набора формул $(w_1, \ldots, w_m)$ состоит в последовательном преобразовании набора переменных $(x_1, \ldots, x_n)$. Каждая последовательность преобразований набора переменных $(x_1, \ldots, x_n)$ в набор формул $(w_1, \ldots, w_m)$ допускает наглядное представление в виде подходящей бинарной функциональной сети Σ, у которой степень захода каждой вершины не превосходит 2. При этом удобно говорить, что сеть Σ описывает преобразование набора переменных $(x_1, \ldots, x_n)$ в набор формул $(w_1, \ldots, w_m)$, а при выборе бинарной операции $F \in \mathcal{B}(\Omega)$ реализует отображение $\Sigma^F = (w_1^F, \ldots, w_m^F)$.

Если сеть Σ описывает последовательность преобразований набора переменных $(x_1, \ldots, x_n)$ в набор формул $(w_1, \ldots, w_m)$, при которых каждый промежуточный набор содержит ровно n формул (иными словами каждый слой сети Σ содержит ровно n вершин), то такую сеть естественно называть сетью постоянной ширины. Такие сети представляют особый интерес с точки зрения удобства практической реализации.

Пример 1.1. Преобразование набора переменных $(x_1, x_2, x_3, x_4, x_5, x_6)$ в набор формул $((x_1 * x_3) * x_1, x_1 * x_3, x_2 * x_1, (x_4 * x_6) * x_6, (x_4 * x_6) * x_1, x_2 * (x_5 * x_2))$ может быть описано, например, бинарной функциональной сетью постоянной ширины, изображенной на рисунке 1.

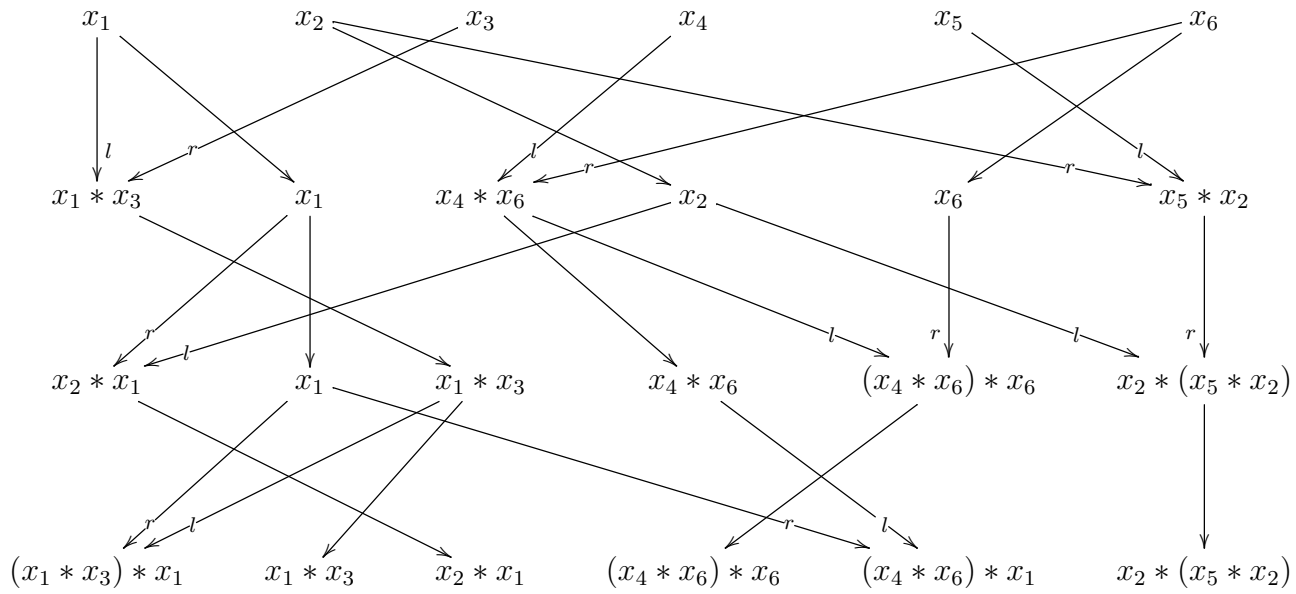

Рис. 1

Определение 1.6. Сеть Σ будем называть *$\mathcal{R}$-биективной для множества* Ω, если при выборе произвольной операции $F \in \mathcal{R}(\Omega)$ отображение Σ^F является биективным. Сеть Σ будем называть *$\mathcal{R}$-биективной*, если она $\mathcal{R}$-биективна для любого множества Ω.

В §1.2 доказывается критерий $\mathcal{R}$-биективности произвольной бинарной сети постоянной ширины в терминах ее матрицы смежности (теорема 1.1) и доказывается существование эквивалентного представления в виде произведения элементарных и перестановочной сетей (теорема 1.2).

Теорема 1.2. *Пусть $\mathcal{R}$-биективная сеть Σ ширины n описывает преобразование набора переменных $(x_1, \ldots, x_n)$ в набор формул $(w_1, \ldots, w_n)$ и содержит t вершин со степенью захода 2. Тогда существуют такие элементарные сети $\Sigma_{R1}, \ldots, \Sigma_{Rt}$ $(\Sigma_{L1}, \ldots, \Sigma_{Lt})$ и однослойная перестановочная сеть Π_R (Π_L), что произведение*

$$\Sigma_{R1} \cdot \ldots \cdot \Sigma_{Rt} \cdot \Pi_R \quad (\Pi_L \cdot \Sigma_{L1} \cdot \ldots \cdot \Sigma_{Lt}),$$

описывает преобразование набора переменных $(x_1, \ldots, x_n)$ в набор формул $(w_1, \ldots, w_n)$.

Пример 1.2. В качестве примера, иллюстрирующего теорему 1.2, отметим, что преобразование набора переменных $(x_1, x_2, x_3, x_4, x_5, x_6)$ в набор формул $((x_1 * x_3) * x_1, x_1 * x_3, x_2 * x_1, (x_4 * x_6) * x_6, (x_4 * x_6) * x_1, x_2 * (x_5 * x_2))$, рассмотренное в примере 1.1, может быть также описано произведением элементарных и перестановочной сетей, изображенным на рисунке 2.

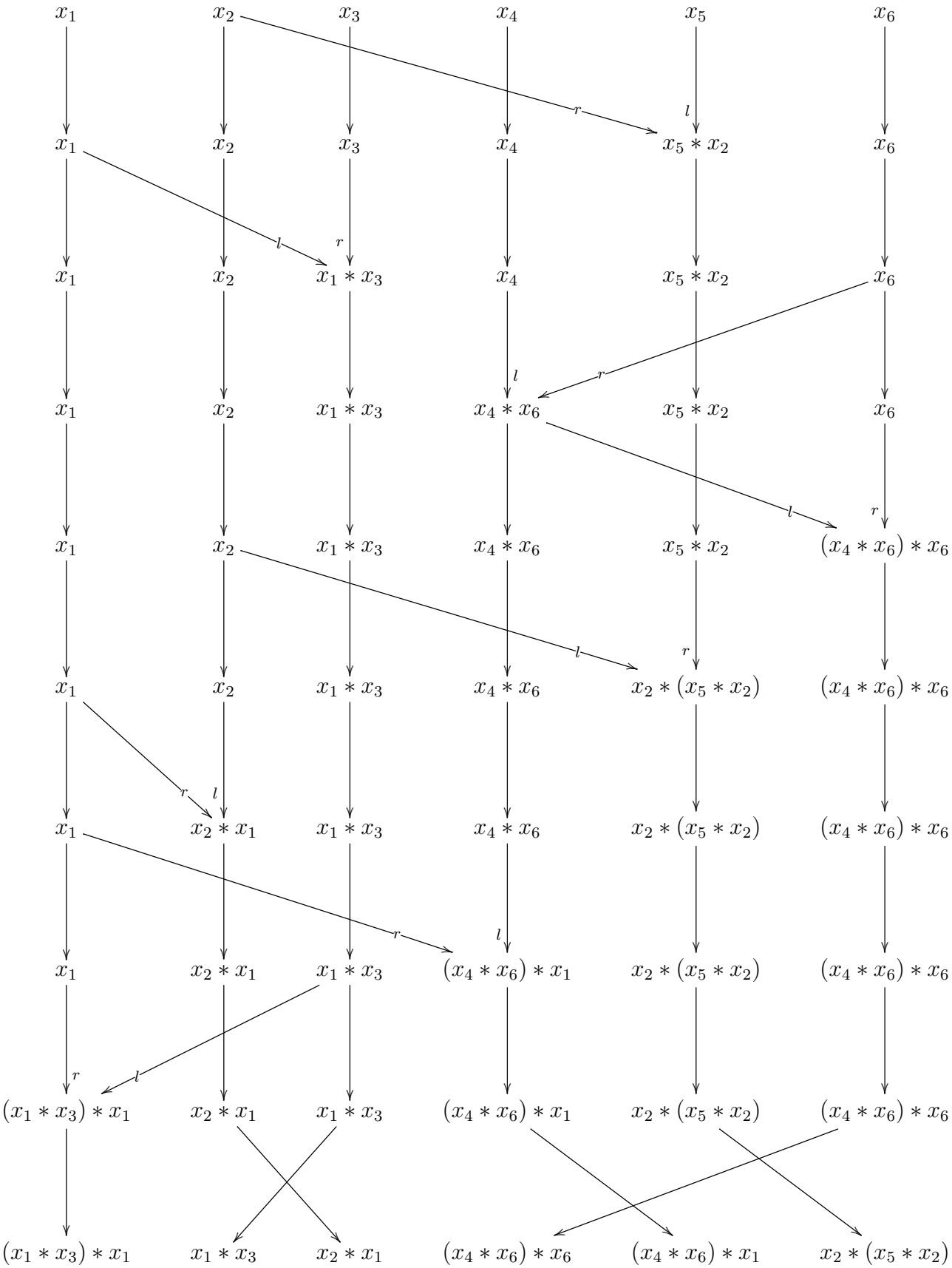
x_1 x_2 x_3 x_4 x_5 x_6
x_1 x_2 x_3 x_4 $x_5 * x_2$ x_6
x_1 x_2 $x_1 * x_3$ x_4 $x_5 * x_2$ x_6
x_1 x_2 $x_1 * x_3$ $x_4 * x_6$ $x_5 * x_2$ x_6
x_1 x_2 $x_1 * x_3$ $x_4 * x_6$ $x_5 * x_2$ $(x_4 * x_6) * x_6$
x_1 x_2 $x_1 * x_3$ $x_4 * x_6$ $x_2 * (x_5 * x_2)$ $(x_4 * x_6) * x_6$
x_1 $x_2 * x_1$ $x_1 * x_3$ $x_4 * x_6$ $x_2 * (x_5 * x_2)$ $(x_4 * x_6) * x_6$
x_1 $x_2 * x_1$ $x_1 * x_3$ $(x_4 * x_6) * x_1$ $x_2 * (x_5 * x_2)$ $(x_4 * x_6) * x_6$
$(x_1 * x_3) * x_1$ $x_2 * x_1$ $x_1 * x_3$ $(x_4 * x_6) * x_1$ $x_2 * (x_5 * x_2)$ $(x_4 * x_6) * x_6$
$(x_1 * x_3) * x_1$ $x_1 * x_3$ $x_2 * x_1$ $(x_4 * x_6) * x_6$ $(x_4 * x_6) * x_1$ $x_2 * (x_5 * x_2)$
r
l
r
l
r
l
r
l
r
l
r
l
r
l
r
l
r
l

Рис. 2

В §1.3 вводится понятие разметки $\mathcal{R}$-биективной сети — инструмента, который позволяет обнаруживать особенности $\mathcal{R}$-биективной сети, нарушающие её транзитивность, (определения 1.10–1.14) и доказываются основные утверждения о свойствах разметок (теоремы 1.6 и 1.7).

С использованием аппарата разметок доказывается однозначность состава произведения элементарных и перестановочной сетей, описывающего некоторое семейство преобразований вида $\{(w_1^F, \ldots, w_m^F) \,:\, F \in \mathcal{R}(\Omega)\}$ (теорема 1.9) и, как следствие, уточняется основная теорема 1.2 о строении $\mathcal{R}$-биективной сети постоянной ширины (следствие 1.8).

Следствие 1.8. *Пусть $\mathcal{R}$-биективная сеть Σ ширины n описывает преобразование набора переменных $(x_1, \ldots, x_n)$ в набор формул $(w_1, \ldots, w_n)$. Тогда существуют такие элементарные сети $\Sigma_{R1}, \ldots, \Sigma_{Rt}$ $(\Sigma_{L1}, \ldots, \Sigma_{Lt})$ и однослойная перестановочная сеть Π_R (Π_L), что произведение*

$$\Sigma_{R1} \cdot \ldots \cdot \Sigma_{Rt} \cdot \Pi_R \quad (\Pi_L \cdot \Sigma_{L1} \cdot \ldots \cdot \Sigma_{Lt}),$$

описывает преобразование набора переменных $(x_1, \ldots, x_n)$ в набор формул $(w_1, \ldots, w_n)$. При этом указанное произведение определено однозначно с точностью до возможной перестановки элементарных сетей, а количество элементарных сетей в данном произведении равно количеству вершин сети Σ со степенью захода 2.

Количество вершин $\mathcal{R}$-биективной сети Σ со степенью захода 2 будем называть *весом сети* Σ или её *сложностью* и обозначать $\|\Sigma\|$.

Во второй главе продолжается развитие аппарата разметок и с его помощью исследуется вопрос о транзитивности множества блочных преобразований $\{\Sigma^F \,:\, F \in \mathcal{R}(\Omega)\}$ для произвольной $\mathcal{R}$-биективной сети.

Определение 2.1. $\mathcal{R}$-биективную сеть Σ будем называть *$\mathcal{R}$-транзитивной для множества* Ω, если множество отображений $\{\Sigma^F \,:\, F \in \mathcal{R}(\Omega)\}$ является транзитивным.

Поскольку отображение, реализуемое перестановочной сетью, не зависит от выбора операции $F \in \mathcal{B}(\Omega)$, то, учитывая результаты теоремы 1.2 и следствия 1.8, произвольная $\mathcal{R}$-биективная сеть Σ при изучении вопроса о транзитивности, не ограничивая общности, полагается равной произведению элементарных сетей $\Sigma_1 \cdot \ldots \cdot \Sigma_t$ (кратко будем писать $\Sigma = \Sigma_1 \cdot \ldots \cdot \Sigma_t$).

В §2.1 с использованием аппарата разметок формулируются и доказываются критерии $\mathcal{B}^*$-транзитивности сети (утверждение 2.2), $\mathcal{Q}$-транзитивности сети (утверждение 2.3) и универсальный критерий $\mathcal{R}$-транзитивности сети (утверждение 2.4).

Утверждение 2.4. *Пусть $\Sigma = \Sigma_1 \cdot \ldots \cdot \Sigma_t$ — $\mathcal{R}$-биективная сеть ширины n. Тогда для любого множества Ω, мощность которого не менее чем $t + n$, следующие утверждения эквивалентны:*

1. *сеть Σ является $\mathcal{R}$-транзитивной для множества Ω;*
2. *сеть Σ допускает $\mathcal{R}$-разметку элементами множества Ω при любых ограничениях $\left(\begin{smallmatrix} v_1 & \ldots & v_n \\ w_1 & \ldots & w_n \end{smallmatrix}\right)$ из множества Ω;*
3. *сеть Σ допускает $\mathcal{R}$-разметку элементами множества $\mathbb{N}$ при любых ограничениях $\left(\begin{smallmatrix} v_1 & \ldots & v_n \\ w_1 & \ldots & w_n \end{smallmatrix}\right)$ из множества $\mathbb{N}$.*

Далее в §2.1 доказывается существование более эффективного (с теоретической точки зрения) способа проверки условия 3 утверждения 2.4 (теорема 2.6).

Теорема 2.6. *Сеть $\Sigma = \Sigma_1 \cdot \ldots \cdot \Sigma_t$ допускает $\mathcal{R}$-разметки при всех возможных ограничениях $\left(\begin{smallmatrix} v_1 & \ldots & v_n \\ w_1 & \ldots & w_n \end{smallmatrix}\right)$ из $\mathbb{N}$ в том и только в том случае, когда сеть Σ допускает $\mathcal{R}$-разметки при всех возможных ограничениях $\left(\begin{smallmatrix} \bar{v}_1 & \ldots & \bar{v}_n \\ \bar{w}_1 & \ldots & \bar{w}_n \end{smallmatrix}\right)$ из Ω_2.*

И в заключение предлагается эффективный (с практической точки зрения) способ проверки условия 3 утверждения 2.4 (теорема 2.7). В результате ряд условий, эквивалентных $\mathcal{R}$-транзитивности сети Σ, (см. утверждение 2.4) можно дополнить еще одним условием, которое допускает эффективную проверку (условие 4 в следствии 2.4).

Следствие 2.4. *Пусть $\Sigma = \Sigma_1 \cdot \ldots \cdot \Sigma_t$ — $\mathcal{R}$-биективная сеть ширины n. Тогда для любого множества Ω, мощность которого не менее чем $t + n$, следующие утверждения эквивалентны:*

1. *сеть Σ является $\mathcal{R}$-транзитивной для множества Ω;*
2. *сеть Σ допускает $\mathcal{R}$-разметку элементами множества Ω при любых ограничениях $\left(\begin{smallmatrix} v_1 & \ldots & v_n \\ w_1 & \ldots & w_n \end{smallmatrix}\right)$ из множества Ω;*
3. *сеть Σ допускает $\mathcal{R}$-разметку элементами множества Ω при любых ограничениях $\left(\begin{smallmatrix} \bar{v}_1 & \ldots & \bar{v}_n \\ \bar{w}_1 & \ldots & \bar{w}_n \end{smallmatrix}\right)$ из множества $\Omega_2 \subset \Omega$;*
4. *сеть Σ допускает свободную $\mathcal{R}$-разметку элементами множества $\mathbb{N}$ при любых ограничениях $\left(\begin{smallmatrix} \bar{v}_1 & \ldots & \bar{v}_n \\ \bar{w}_1 & \ldots & \bar{w}_n \end{smallmatrix}\right)$ из множества Ω_2.*

В §2.2 определяется каноническое представление произвольной $\mathcal{R}$-биективной сети (утверждение 2.9 и определение 2.5), которое фактически является естественным упорядочением представления из теоремы 1.2 и следствия 1.8.

Введенное понятие канонического представления вместе с разработанным аппаратом разметок позволяют строго описать алгоритмы построения $\mathcal{Q}$-биективных и $\mathcal{B}^*$-биективных сетей, действующих транзитивным образом для всех достаточно больших множеств (на вход алгоритма подается произвольная $\mathcal{R}$-биективная сеть в своем каноническом представлении; в ходе работы алгоритма, в зависимости от результатов минимальной свободной $\mathcal{R}$-разметки сети Σ, в каноническое представление сети Σ добавляются подходящие элементарные сети; в результате работы выполнения алгоритма получается $\mathcal{R}$-биективная сеть $\widehat{\Sigma}$, действующая $\mathcal{R}$-транзитивным образом для всех достаточно больших множеств).

Кроме того, аппарат разметок $\mathcal{R}$-биективных сетей позволяет строго обосновать корректность предлагаемых алгоритмов (теорема 2.10).

Теорема 2.10. *Пусть* $\Sigma = (\Sigma_{11} \cdot \ldots \cdot \Sigma_{1k_1}) \cdot \ldots \cdot (\Sigma_{n1} \cdot \ldots \cdot \Sigma_{nk_n})$ *— произвольная* $\mathcal{R}$*-биективная сеть ширины* n*. Тогда её модификация* $\widehat{\Sigma}$ *имеет сложность не более чем* $\|\Sigma\| + 3n - 3$ *и является* $\mathcal{R}$*-транзитивной для произвольного множества* Ω*, мощность которого не менее чем* $\|\Sigma\| + 4n - 3$*.*

В §2.3 доказывается нетривиальная нижняя оценка веса $\mathcal{R}$-транзитивной сети (теорема 2.13).

Теорема 2.13. *Пусть* $\mathcal{R}$*-биективная сеть* $\Sigma = \Sigma_1 \cdot \ldots \cdot \Sigma_t$ *имеет ширину* n *и является* $\mathcal{R}$*-транзитивной для множества* Ω*,* $|\Omega| \geqslant 2$*. Тогда* $t \geqslant \frac{3}{2}n$*.*

Кроме того, в §2.3 для произвольного $n \in \mathbb{N}$ определяются две универсальные конструкции $\mathcal{B}^*$-биективных сетей ширины n и веса $2n-1$: Δ_n (пример 2.4) и Ψ_n (пример 2.5). С применением аппарата разметки, доказывается, что каждая из сетей Δ_n и Ψ_n при любом $n \in \mathbb{N}$ является $\mathcal{B}^*$-транзитивной для всех достаточно больших множеств, а сеть Δ_n является также $\mathcal{Q}$-транзитивной для всех достаточно больших множеств.

Рассмотренные сети Δ_n, Ψ_n, $n \in \mathbb{N}$ могут быть использованы для эффективного построения широких классов $\mathcal{R}$-транзитивных сетей с требуемыми особенностями архитектуры (теорема 2.14).

Теорема 2.14. *Пусть* $\Sigma = \Sigma_1 \cdot \ldots \cdot \Sigma_t$ *—* $\mathcal{R}$*-биективная сеть ширины* n *и при проведении свободной разметки* μ *сети* Σ *с начальным условием* $(v, \ldots, v)$ *метка* $\mu(x_1^{(t)})$ *не является координатой какого-либо набора из области определения ее минимального правила* $F_{\Sigma,\mu}$*. Тогда произведение* $\Sigma \cdot \Delta_n$ *является* $\mathcal{R}$*-транзитивным для любого множества* Ω *мощности не менее чем* $t+3n-1$*.*

Если, дополнительно, Σ *—* $\mathcal{B}^*$*-биективная сеть, то произведение* $\Sigma \cdot \Psi_n$ *является* $\mathcal{B}^*$*-транзитивным для любого множества* Ω *мощности не менее чем* $t + 3n - 1$*.*

В заключение второй главы отмечается, что для $\mathcal{R}$-транзитивных сетей в качестве транзитивного множества преобразований можно использовать не только полные классы $\{\Sigma^F : F \in \mathcal{R}(\Omega)\}$, но и специальные репрезентативные выборки $\{\Sigma^F : F \in \mathcal{K}\}$, где $\mathcal{K} \subset \mathcal{R}(\Omega)$ и $|\mathcal{K}| \leqslant |\Omega|^{2n}$ (замечание 2.7).

Третья глава диссертации посвящена исследованию k-транзитивности множества блочных преобразований $\{\Sigma^F : F \in \mathcal{R}(\Omega)\}$ при $k \geqslant 2$.

Определение 3.1. $\mathcal{R}$-биективную сеть Σ будем называть *$k\mathcal{R}$-транзитивной для множества* Ω, если множество отображений $\{\Sigma^F : F \in \mathcal{R}(\Omega)\}$ является k-транзитивным.

Аппарат разметок $\mathcal{R}$-биективных сетей, введенный и разработанный в главах 1, 2, на самом деле позволяет исследовать не только $\mathcal{R}$-транзитивность сетей, но и более сложное свойство $k\mathcal{R}$-транзитивности при $k \geqslant 2$. Однако для удобства проведения рассуждений при исследовании $k\mathcal{R}$-транзитивности $\mathcal{R}$-биективных сетей в §3.1 формулируются естественные k-мерные обобщения основных понятий аппарата разметок (определения 3.2 и 3.3) и доказываются k-мерные обобщения основных технических результатов (теоремы 3.3 и 3.4). Кроме того, в §3.1 определяются несколько различных способов построения свободной k-разметки и доказывается, что все они по существу эквивалентны между собой (теорема 3.2).

В §3.2 с использованием k-мерных инструментов аппарата разметок, предложенных в §3.1, формулируются и доказываются критерии $k\mathcal{B}^*$-транзитивности сети (утверждение 3.6), $k\mathcal{Q}$-транзитивности сети (утверждение 3.7) и универсальный критерий $k\mathcal{R}$-транзитивности сети (утверждение 3.8).

Утверждение 3.8. *Пусть $\Sigma = \Sigma_1 \cdot \ldots \cdot \Sigma_t$ — $\mathcal{R}$-биективная сеть ширины n. Тогда для любого множества Ω, мощность которого не менее чем $k(t+n)$, следующие утверждения эквивалентны:*

1. *сеть Σ является $k\mathcal{R}$-транзитивной для множества Ω;*
2. *сеть Σ допускает $k\mathcal{R}$-разметку элементами множества Ω при произвольных невырожденных ограничениях $\binom{v_{11}\ \ldots\ v_{1n}}{w_{11}\ \ldots\ w_{1n}}, \ldots, \binom{v_{k1}\ \ldots\ v_{kn}}{w_{k1}\ \ldots\ w_{kn}}$ из множества Ω;*
3. *сеть Σ допускает $k\mathcal{R}$-разметку при произвольных невырожденных ограничениях $\binom{v_{11}\ \ldots\ v_{1n}}{w_{11}\ \ldots\ w_{1n}}, \ldots, \binom{v_{k1}\ \ldots\ v_{kn}}{w_{k1}\ \ldots\ w_{kn}}$ из множества $\mathbb{N}$.*

Далее в §3.2 доказывается существование более эффективного (с теоретической точки зрения) способа проверки условия 3 утверждения 3.8 (теорема 3.10).

Теорема 3.10. *Сеть* $\Sigma = \Sigma_1 \cdot \ldots \cdot \Sigma_t$ *допускает* $k\mathcal{R}$*-разметки при всех возможных невырожденных ограничениях* $\left(\begin{smallmatrix} v_{11} & \ldots & v_{1n} \\ w_{11} & \ldots & w_{1n} \end{smallmatrix}\right), \ldots, \left(\begin{smallmatrix} v_{k1} & \ldots & v_{kn} \\ w_{k1} & \ldots & w_{kn} \end{smallmatrix}\right)$ *из* $\mathbb{N}$ *в том и только в том случае, когда сеть* Σ *допускает* $k\mathcal{R}$*-разметки при всех возможных невырожденных ограничениях* $\left(\begin{smallmatrix} \bar{v}_{11} & \ldots & \bar{v}_{1n} \\ \bar{w}_{11} & \ldots & \bar{w}_{1n} \end{smallmatrix}\right), \ldots, \left(\begin{smallmatrix} \bar{v}_{k1} & \ldots & \bar{v}_{kn} \\ \bar{w}_{k1} & \ldots & \bar{w}_{kn} \end{smallmatrix}\right)$ *из* Ω_{k+1}.

И в заключение предлагается эффективный (с практической точки зрения) способ проверки условия 3 утверждения 3.8 (теорема 3.12). В результате ряд условий, эквивалентных $k\mathcal{R}$-транзитивности сети Σ, (см. утверждение 3.8) можно дополнить еще одним условием, которое допускает эффективную проверку (условие 4 в следствии 3.5).

Следствие 3.5. *Пусть* $\Sigma = \Sigma_1 \cdot \ldots \cdot \Sigma_t$ *—* $\mathcal{R}$*-биективная сеть ширины* n. *Тогда для любого множества* Ω, *мощность которого не менее чем* $k(t+n)$, *следующие утверждения эквивалентны:*

1. *сеть* Σ *является* $k\mathcal{R}$*-транзитивной для множества* Ω;
2. *сеть* Σ *допускает* $k\mathcal{R}$*-разметку элементами множества* Ω *при любых невырожденных ограничениях* $\left(\begin{smallmatrix} v_{11} & \ldots & v_{1n} \\ w_{11} & \ldots & w_{1n} \end{smallmatrix}\right), \ldots, \left(\begin{smallmatrix} v_{k1} & \ldots & v_{kn} \\ w_{k1} & \ldots & w_{kn} \end{smallmatrix}\right)$ *из множества* Ω;
3. *сеть* Σ *допускает* $k\mathcal{R}$*-разметку элементами множества* Ω *при любых невырожденных ограничениях* $\left(\begin{smallmatrix} \bar{v}_{11} & \ldots & \bar{v}_{1n} \\ \bar{w}_{11} & \ldots & \bar{w}_{1n} \end{smallmatrix}\right), \ldots, \left(\begin{smallmatrix} \bar{v}_{k1} & \ldots & \bar{v}_{kn} \\ \bar{w}_{k1} & \ldots & \bar{w}_{kn} \end{smallmatrix}\right)$ *из множества* $\Omega_{k+1} \subset \Omega$;
4. *сеть* Σ *допускает свободную* $k\mathcal{R}$*-разметку элементами множества* $\mathbb{N}$ *при любых невырожденных ограничениях* $\left(\begin{smallmatrix} \bar{v}_{11} & \ldots & \bar{v}_{1n} \\ \bar{w}_{11} & \ldots & \bar{w}_{1n} \end{smallmatrix}\right), \ldots, \left(\begin{smallmatrix} \bar{v}_{k1} & \ldots & \bar{v}_{kn} \\ \bar{w}_{k1} & \ldots & \bar{w}_{kn} \end{smallmatrix}\right)$ *из множества* Ω_{k+1}.

В §3.3 предлагается универсальный алгоритм модификации канонического представления произвольной $\mathcal{R}$-биективной сети Σ, в результате работы которого получается $\mathcal{R}$-биективная сеть $\widehat{\Sigma}$, действующая $k\mathcal{R}$-транзитивным образом для всех достаточно больших множеств. Разработанный в диссертации аппарат разметок $\mathcal{R}$-биективных сетей позволяет привести строгое описание алгоритма и обоснование его корректности (теорема 3.14).

Теорема 3.14. *Пусть* $\Sigma = (\Sigma_{11} \cdot \ldots \cdot \Sigma_{1k_1}) \cdot \ldots\ldots \cdot (\Sigma_{n1} \cdot \ldots \cdot \Sigma_{nk_n})$ *— произвольная* $\mathcal{R}$*-биективная сеть ширины* n. *Тогда её модификация* $\widehat{\Sigma}$ *имеет сложность не более чем* $\|\Sigma\| + 3n - 3$ *и является* $k\mathcal{R}$*-транзитивной для любого множества* Ω, *мощность которого не менее чем* $k\,(\|\Sigma\| + 7n - 6)$.

Отметим, что предложенный в настоящей диссертации алгоритм построения $k\mathcal{R}$-транзитивной сети является «гибким» по содержанию выполняемых

действий — добавляемые на промежуточных шагах элементарные сети можно выбирать различными способами (что особенно важно при использовании данного алгоритма для построения $k\mathcal{Q}$-транзитивных сетей). Другими словами, предложенный алгоритм следует рассматривать как общую схему, на основе которой можно выстроить целое семейство алгоритмов построения $k\mathcal{R}$-транзитивных сетей схожей архитектуры, но с различными «оттенками» внутренних элементов.

Кроме того, в §3.3 определяется серия $\mathcal{R}$-биективных сетей ∇_n, $n \in \mathbb{N}$, в которой каждая сеть ∇_n имеет ширину n и вес $4n-4$ (пример 3.1). С использованием аппарата разметок доказывается, что каждая сеть ∇_n, $n \in \mathbb{N}$ является $k\mathcal{R}$-транзитивной при любом $k \geqslant 2$ для всех достаточно больших множеств. В заключение доказывается, что рассмотренные сети ∇_n, $n \in \mathbb{N}$ могут быть использованы для эффективного построения широких классов $k\mathcal{R}$-транзитивных сетей с требуемыми особенностями архитектуры (теорема 3.16).

Теорема 3.16. *Пусть $\Sigma = \Sigma_1 \cdot \ldots \cdot \Sigma_t$ — $\mathcal{R}$-биективная сеть ширины n. Тогда произведение $\Sigma \cdot \nabla_n$ является $k\mathcal{R}$-транзитивным для любого множества Ω мощности не менее чем $k(t+5n-4)$.*

ЗАКЛЮЧЕНИЕ

Перечислим основные результаты, полученные автором в диссертации.

1. Описано строение $\mathcal{R}$-биективных сетей — бинарных функциональных сетей постоянной ширины, которые определяют биективное преобразование при выборе любой бинарной операции из множества $\mathcal{R}(\Omega)$.

2. Разработан эффективный метод проверки кратной транзитивности полного класса блочных преобразований $\{\Sigma^F : F \in \mathcal{R}(\Omega)\}$, определяемых произвольной $\mathcal{R}$-биективной сетью Σ.

3. Предложены и строго обоснованы алгоритмы построения $\mathcal{R}$-биективных сетей, для которых соответствующие полные классы блочных преобразований обладают требуемым показателем кратной транзитивности при достаточно большом множестве Ω.

4. Построены практически значимые классы $\mathcal{R}$-биективных сетей с небольшой сложностью, для которых соответствующие классы блочных преобразований обладают требуемым показателем кратной транзитивности, в том числе и при использовании специальных репрезентативных выборок из множества $\mathcal{R}(\Omega)$.

Результаты диссертационного исследования могут найти применение в области синтеза и анализа узлов защиты информации. С одной стороны, полученные в работе результаты позволяют создавать компоненты узлов защиты и переработки информации, которые обеспечивают высокие показатели конфиденциальности. С другой стороны, при исследовании некоторых известных узлов защиты информации для аппроксимации множества преобразований, реализуемых данными узлами, можно использовать предложенную в работе модель классов блочных преобразований — в рамках указанной модели разработанный аппарат разметки позволяет достаточно эффективно выявлять кратную транзитивность.

Благодарности. Автор выражает глубокую благодарность своим научным руководителям: член-корреспонденту Академии криптографии РФ, доктору физико-математических наук, профессору Черемушкину Александру Васильевичу за постановку задачи и обсуждение результатов, кандидату физико-математических наук, старшему научному сотруднику Галатенко Алексею Владимировичу за оказанную поддержку и внимание к работе, а также всем сотрудникам кафедры математической теории интеллектуальных систем Механико-математического факультета МГУ им. М.В. Ломоносова за внимание и доброжелательное отношение.

ПУБЛИКАЦИИ АВТОРА ПО ТЕМЕ ДИССЕРТАЦИИ

Научные статьи, опубликованные в рецензируемых научных изданиях, рекомендованных для защиты в диссертационном совете МГУ по специальности 05.13.19 — «Методы и системы защиты информации, информационная безопасность»

[1] **Чередник, И. В.** Один подход к построению транзитивного множества блочных преобразований / И. В. Чередник // Прикладная дискретная математика. — 2017. — №38. — С. 5–34. (WoS, RSCI, ИФ РИНЦ 0.370)

[2] **Чередник, И. В.** Один подход к построению кратно транзитивного множества блочных преобразований / И. В. Чередник // Прикладная дискретная математика. — 2018. — №42. — С. 18–47. (WoS, RSCI, ИФ РИНЦ 0.507)

[3] **Чередник, И. В.** Об использовании бинарных операций при построении транзитивного множества блочных преобразований / И. В. Чередник // Дискретная математика. — 2019. — т. 31 №3. — С. 93–113.
(WoS, RSCI, ИФ РИНЦ 0.518)

(Пер. на англ. яз.: **Cherednik, I. V.** Using binary operations to construct a transitive set of block transformations / I. V. Cherednik // Discrete Mathematics and Applications. — 2020. — **30: 3**. — P. 375–389.) (Scopus, WoS)

[4] **Чередник, И. В.** Об использовании бинарных операций при построении кратно транзитивного множества блочных преобразований / И. В. Чередник // Дискретная математика. — 2020. — т. 32 №2. — С. 85–111.
(WoS, RSCI, ИФ РИНЦ 0.390)

(Пер. на англ. яз.: **Cherednik, I. V.** On the use of binary operations for the construction of a multiply transitive class of block transformations / I. V. Cherednik // Discrete Mathematics and Applications. — 2021. — **31: 2**. — P. 91–111.) (Scopus, WoS)

Прочие публикации (по теме диссертации)

[5] **Чередник, И. В.** Об одном подходе к построению транзитивного множества блочных преобразований / И. В. Чередник // Материалы Всероссийской конференции SIBECRYPT'17 — Прикладная дискретная математика. Приложение — 2017. — №10. — С. 27–29.

[6] **Чередник, И. В.** k-транзитивность одного класса блочных преобразований / И. В. Чередник // Материалы Всероссийской конференции SIBECRYPT'18 — Прикладная дискретная математика. Приложение — 2018. — №11. — С. 21–23.