ОТЗЫВ

официального оппонента на диссертационную работу
Чередника Игоря Владимировича
«Использование бинарных функциональных сетей при построении кратно транзитивных множеств блочных преобразований», представленную на соискание ученой степени кандидата физико-математических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность» (физико-математические науки)

Диссертационная работа Чередника И. В. посвящена разработке способов построения кратно транзитивных множеств блочных преобразований, основанных на оригинальной «сетевой» модели, в рамках которой архитектура всех преобразований определяется фиксированной для каждого класса бинарной функциональной сетью, а базисная бинарная операция, используемая в узлах функциональной сети, выполняет роль параметра. Подобные классы преобразований естественным образом возникают при функционировании некоторых узлов в системах защиты информации. Стоит отметить, что рассматриваемая автором концепция построения блочных преобразований является нетривиальным обобщением широко известной сети Фейстеля.

С точки зрения информационной безопасности наличие кратной транзитивности у множества преобразований, описывающих функционирование узлов защиты информации, является необходимым свойством. Так как его отсутствие в некоторых случаях может позволить достаточно эффективно восстанавливать начальные состояния и/или значения фиксированных параметров исследуемых узлов и, как следствие, создает потенциальную возможность нарушения конфиденциальности обрабатываемой/передаваемой информации. Таким образом, задача построения кратно транзитивных классов блочных преобразований, реализуемых бинарной функциональной сетью, является актуальной. В диссертации в рамках рассматриваемой «сетевой» модели предлагаются и обосновываются новые подходы к синтезу кратно транзитивных классов блочных преобразований. Кроме того, в работе получены теоретические результаты, которые могут быть использованы при исследовании кратной транзитивности некоторых известных узлов обработки и защиты информации.

Краткая характеристика работы и основные результаты

Диссертация состоит из введения, трех глав и заключения.

Во введении анализируется применение квазигрупп в задачах защиты информации, обосновывается актуальность диссертационной работы, формулируются цели и задачи.

В первой главе определяются основные понятия бинарных функциональных сетей, которые используются в работе, и приводится конструктивное описание множества всех R-биективных бинарных функциональных сетей – бинарных функциональных сетей постоянной ширины, которые определяют биективное преобразование при выборе любой бинарной операции из допустимого множества $R(\Omega)$ (в качестве $R(\Omega)$ предлагается использовать либо семейство $Q(\Omega)$ всех бинарных квазигрупп, заданных на множестве Ω, либо семейство $B^*(\Omega)$ всех бинарных операций, обратимых по правой переменной).

Во второй главе исследуется вопрос о транзитивности полного класса блочных преобразований, определяемого произвольной R-биективной сетью при возможности использования всех бинарных операций из множества $R(\Omega)$. А именно: формулируются и строго обосновываются критерии R-транзитивности полного класса блочных преобразований, определяемого произвольной R-биективной сетью, предлагаются эффективные с практической точки зрения способы проверки указанных критериев, устанавливается нетривиальная нижняя оценка веса (сложности) R-транзитивной сети. Кроме того, формулируется и обосновывается алгоритм построения R-биективных сетей, для которых свойством транзитивности обладают не только соответствующие полные классы блочных преобразований, но даже классы, основанные на небольших репрезентативных выборках из семейства $R(\Omega)$ при достаточно большом множестве Ω (размер множества Ω линейным образом зависит от размера сети).

В третьей главе исследуется свойство кратной транзитивности множества блочных преобразований, определяемого R-биективной сетью: формулируются критерии кратной R-транзитивности полного класса блочных преобразований, определяемого произвольной R-биективной сетью, и предлагаются эффективные способы проверки указанных критериев; формулируется и строго обосновывается алгоритм построения R-биективных сетей, для которых свойством кратной транзитивности обладают не только соответствующие

полные классы блочных преобразований, но даже классы, основанные на небольших репрезентативных выборках из семейства $R(\Omega)$ при достаточно большом множестве Ω (размер множества Ω билинейным образом зависит от размера сети и требуемого показателя кратной транзитивности). Кроме того, определяются практически значимые семейства R-биективных сетей с небольшим количеством вершин, для которых соответствующие классы блочных преобразований обладают требуемым показателем кратной транзитивности (в том числе и при использовании небольших репрезентативных выборок из множества $R(\Omega)$ при достаточно большом множестве Ω).

В заключении диссертации перечислены основные результаты.

1. Описано каноническое строение R-биективных сетей – бинарных функциональных сетей постоянной ширины, которые определяют биективное преобразование при выборе любой бинарной операции из множества $R(\Omega)$ (теорема 1.2 и следствие 1.8).

2. Разработан эффективный метод проверки кратной транзитивности полного класса блочных преобразований, определяемого произвольной R-биективной сетью при использовании всех бинарных операций из множества $R(\Omega)$ (теорема 3.10, теорема 3.12 и следствие 3.5).

3. Предложены и строго обоснованы алгоритмы построения обширных семейств R-биективных сетей, для которых соответствующие полные классы блочных преобразований обладают требуемым показателем кратной транзитивности (алгоритм 3 и теорема 3.14, а также теорема 3.16).

4. Построены бинарные функциональные сети, которые, несомненно, представляют практический интерес, поскольку обладают небольшой сложностью и при этом реализуют классы блочных преобразований с требуемым показателем кратной транзитивности (пример 3.1 и теорема 3.16).

Все полученные в работе результаты являются новыми, ввиду оригинальности постановки задач, разработанного подхода для доказательства корректности результатов и способов их решения.

Диссертация носит теоретический характер. Результаты, представленные в ней, могут быть полезны специалистам в области дискретной математики и криптологии; также их можно использовать для подготовки специального курса

лекций для студентов, обучающихся по укрупненной группе специальностей «Информационная безопасность».

Достоверность результатов и апробация работы

Диссертационная работа Чередника Игоря Владимировича «Использование бинарных функциональных сетей при построении кратно транзитивных множеств блочных преобразований» написана строгим математическим языком и оформлена надлежащим образом. Все полученные в работе результаты сформулированы в виде теорем и снабжены подробными доказательствами.

Результаты диссертационного исследования докладывались на всероссийских конференциях «Сибирская научная школа-семинар с международным участием “Компьютерная безопасность и криптография”» в 2017 и 2018 годах, на XXII научно-практической конференции «РусКрипто’2020», на специальных семинарах механико-математического факультета МГУ, а также на семинаре «Кибербезопасность: теория и практика» института интеллектуальных кибернетических систем НИЯУ «МИФИ».

Замечания

1. В работе отсутствует полное обоснование оценки сложности разработанного метода проверки кратной транзитивности полного класса преобразований, реализуемого бинарной функциональной сетью.

2. В работе отсутствует какие-либо примеры систем защиты информации, к которым применим разработанный в диссертационной работе подхода оценки кратной транзитивности.

3. В работе отсутствует примеры конкретных узлов систем защиты информации, построенных на основе предложенного в диссертационной работе подхода.

4. В автореферате используется фраза об «аппроксимации некоторых известных узлов защиты информации». Что за известные узлы? Как осуществляется аппроксимация? Что это даёт относительно разработанного автором подхода?

5. В диссертационной работе не проводится анализ публикций, посвященных применению сети Фейстеля и её разнообразных обобщений в системах защиты информации, а также нахождению для них оценок кратной

транзитивности. Отсутствует сравнение их с полученными в диссертации оценками.

6. С точки зрения полноты изложения было бы полезно подробнее рассмотреть вопрос о различных способах построения репрезентативной выборки базисных бинарных операций, необходимой для реализации кратно транзитивного класса преобразований на основе подходящей бинарной функциональной сети.

Перечисленные замечания не влияют на общую **положительную** оценку диссертационной работы.

Заключение

Диссертационная работа Чередника Игоря Владимировича «Использование бинарных функциональных сетей при построении кратно транзитивных множеств блочных преобразований» представляет собой самостоятельное, завершенное научное исследование, посвященное актуальным задачам. Результаты работы достоверны и являются новыми.

Основное содержание диссертации опубликовано в 6 печатных работах, из которых 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. Результаты также докладывались на 3 конференциях и 2 специализированных математических семинарах.

Автореферат соответствует содержанию диссертации.

Диссертация Чередника Игоря Владимировича «Использование бинарных функциональных сетей при построении кратно транзитивных множеств блочных преобразований» отвечает всем требованиям, установленным Московским государственным университетом имени М. В. Ломоносова к кандидатским диссертациям. Содержание диссертации соответствует паспорту специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность» (физико-математические науки), а также критериям, определенным пп. 2.1-2.5 Положения о присуждении ученых степеней в Московском государственном университете имени М.В. Ломоносова. Работа оформлена согласно приложениям № 5, 6 Положения о диссертационном совете Московского государственного университета имени М.В. Ломоносова.

Соискатель Чередник Игорь Владимирович заслуживает присуждения ученой степени кандидата физико-математических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность» (физико-математические науки).

Официальный оппонент:
доктор физико-математических наук,
профессор отделения интеллектуальных кибернетических систем
офиса образовательных программ
института интеллектуальных кибернетических систем
НИЯУ «МИФИ» М. А. Пудовкина

29 октября 2021 г.

Контактные данные:
тел. +7 (495) 788-56-99, e-mail: mapudovkina@mephi.ru.
Адрес места работы:
115409, Москва, Каширское ш., 31.
Специальность, по которой официальным оппонентом защищена диссертация:
05.13.19 – «Методы и системы защиты информации, информационная безопасность» (физико-математические науки).

Подпись М. А. Пудовкиной удостоверяю