Заключение диссертационного совета МГУ.011.4
по диссертации на соискание ученой степени кандидата наук

Решение диссертационного совета от «21» ноября 2025 г. № 15

О присуждении **Царегородцеву Кириллу Денисовичу**, гражданину Российской Федерации, ученой степени кандидата физико-математических наук.

Диссертация «Правильные семейства функций и порождаемые ими квазигруппы: комбинаторные и алгебраические свойства» по специальности 1.1.5. Математическая логика, алгебра, теория чисел и дискретная математика принята к защите диссертационным советом «26» сентября 2025 г., протокол № 6. Соискатель **Царегородцев Кирилл Денисович** 1994 года рождения, в 2017 году соискатель окончил ФГБОУ ВО Московский государственный университет имени М.В. Ломоносова, Механико-математический факультет по кафедре высшей алгебры по программе специалитета, специальность 01.05.01. Фундаментальные математика и механика. Поступил в аспирантуру механико-математического факультета МГУ в 2017 году и окончил ее в 2021 году по специальности 01.01.06 Математическая логика, алгебра и теория чисел. Закреплен за кафедрой математической теории интеллектуальных систем Механико-математического факультета МГУ имени М.В. Ломоносова приказами №960-24/101-ас от 12.12.2024, №206-25/101-ас от 25.03.2025 для подготовки диссертации с 2024 г. по 2025 г.

Соискатель работает криптографом-исследователем в АО «Актив-софт»; инженером 1 категории лаборатории вычислительных методов Механико-математического факультета ФГБОУ ВО «Московский государственный университет имени М.В. Ломоносова» (по совместительству).

Диссертация выполнена на кафедре математической теории интеллектуальных систем механико-математического факультета МГУ имени М.В. Ломоносова.

Научные руководители:

Панкратьев Антон Евгеньевич, кандидат физико-математических наук, кафедра математической теории интеллектуальных систем механико-математического факультета МГУ имени М.В. Ломоносова, доцент,

Галатенко Алексей Владимирович, кандидат физико-математических наук, кафедра математической теории интеллектуальных систем механико-математического факультета МГУ имени М.В. Ломоносова, доцент.

Официальные оппоненты:

Щучкин Николай Алексеевич, доктор физико-математических наук, доцент, кафедра высшей математики и физики Института математики, информатики и физики Волгоградского государственного социально-педагогического университета, профессор,

Камловский Олег Витальевич, доктор физико-математических наук, доцент, кафедра 252 Института искусственного интеллекта РТУ МИРЭА, профессор,

Токарева Наталья Николаевна, кандидат физико-математических наук, кафедра теоретической кибернетики механико-математического факультета Новосибирского национального исследовательского государственного университета, доцент,

дали положительные отзывы на диссертацию.

Выбор официальных оппонентов обосновывался тем, что оппоненты являются известными специалистами в области высшей алгебры, криптографии, в теории булевых функций, и имеют работы, близкие к теме диссертационного исследования, в центральных математических журналах.

Соискатель имеет 16 опубликованных работ, в том числе по теме диссертации 9 работ, из них 8 статей, опубликованных, в рецензируемых научных изданиях, рекомендованных для защиты в диссертационном совете МГУ по специальности 1.1.5. Математическая логика, алгебра, теория чисел и дискретная математика (физико-математические науки).

1. Царегородцев К. О свойствах правильных семейств булевых функций // Дискретная математика. — 2021. — Т. 33, № 1. — С. 91—102.
EDN: JTVVAY; журнал индексируется в RSCI. Импакт-фактор: 0.385 (РИНЦ); общий объем 0.75 п. л.
Перевод:
Tsaregorodtsev K.D. Properties of proper families of Boolean functions // Discrete Mathematics and Applications. — 2022. — vol. 32, no. 5. — p. 369–378.
EDN: INXYMW; журнал индексируется в WOS, Scopus. Импакт-фактор: 0.3 (JIF); общий объем 0.75 п. л.

2. О порождении n-квазигрупп с помощью правильных семейств функций / А. Галатенко, В. Носов, А. Панкратьев, К. Царегородцев // Дискретная математика. — 2023. — Т. 35, № 1. — С. 35—53.
EDN: WWYSEG; журнал индексируется в RSCI Импакт-фактор: 0.385 (РИНЦ); общий объем 1.18 п.л.

Перевод:
Galatenko A.V., Nosov V.A., Pankratiev A.E., Tsaregorodtsev K.D. Generation of n-quasigroups by proper families of functions // Discrete Mathematics and Applications. — 2025. — vol. 35, no. 4. — p. 203–217.
DOI: https://doi.org/10.4213/dm1749, журнал индексируется в WOS, Scopus. Импакт-фактор: 0.3 (JIF); общий объем 1.18 п.л.
Царегородцеву К. Д. принадлежат формулировка и доказательство теоремы 1 и результаты раздела 6, объем 0.34 п. л. (29 %).

3. Proper families of functions and their applications / A. V. Galatenko, V. A. Nosov, A. E. Pankratiev, K. D. Tsaregorodtsev // Математические вопросы криптографии. — 2023. — vol. 14, no. 2. — p. 43—58.
EDN: FUKEYM; журнал индексируется в RSCI. Импакт-фактор: 0.232 (РИНЦ); общий объем 0.98 п. л.
Царегородцеву К. Д. принадлежат разделы 4,5,6, объем 0.25 п. л. (25 %).

4. Царегородцев К. Д. О взаимно однозначном соответствии между правильными семействами булевых функций и рёберными ориентациями булевых кубов // Прикладная дискретная математика. — 2020. — Т. 48. – – С. 16—21.
EDN: VTEBFJ; журнал индексируется в Scopus, RSCI. Импакт-фактор: 0.1 (JIF); общий объем 0.375 п. л.

5. Galatenko A., Pankratiev A., Tsaregorodtsev K. A Criterion of Properness for a Family of Functions // Journal of Mathematical Sciences. — 2024. — vol. 284, no. 4. — p. 451—459.
EDN: ECXXNP; журнал индексируется в Scopus. Импакт-фактор: 0.28 (SJR); общий объем 0.81 п. л.
Царегородцеву К. Д. принадлежат формулировка и доказательство результатов раздела 4, объем 0.31 п. л. (38 %).

6. Tsaregorodtsev K. Format-preserving encryption: a survey // Математические вопросы криптографии. — 2022. — vol. 13, no. 2. — p. 133-153.
EDN: QMBWSF; журнал индексируется в RSCI. Импакт-фактор: 0.232 (РИНЦ); общий объем 1.31 п. л.

7. Царегородцев К. Об индексе ассоциативности конечных квазигрупп // Интеллектуальные системы. Теория и приложения. — 2024. — Т. 28, № 3. — С. 80—101.

EDN: CVMWMA. Импакт-фактор: 0.117 (РИНЦ); 1.37 п. л.

8. Царегородцев К. О соответствии между правильными семействами и реберными ориентациями булевых кубов // Интеллектуальные системы. Теория и приложения. — 2020. — Т. 24, № 1. — С. 97—100.

EDN: EYLHYQ. Импакт-фактор: 0.117 (РИНЦ); общий объем 0.25 п. л.

На диссертацию и автореферат поступило 2 дополнительных отзыва, все положительные.

Диссертационный совет отмечает, что представленная диссертация на соискание ученой степени кандидата физико-математических наук является научно-квалификационной работой, в которой содержатся следующие результаты: установлено естественное соответствие между булевыми правильными семействами и одностоковыми ориентациями графов булевых кубов (USO-ориентации), а также между булевыми правильными семействами и булевыми сетями с наследственно единственной неподвижной точкой (HUFP-сети); установлено естественное соответствие между правильными семействами в логике произвольной значности и кликами в обобщенных графах Келлера. Доказано, что стабилизатором множества правильных семейств функций являются изометрии пространства Хэмминга (согласованные перенумерации и перекодировки); показано, что отображения, задаваемые с помощью правильных семейств булевых функций, всегда имеют четное число неподвижных точек; получена оценка на число правильных семейств булевых функций, предложены оценки доли треугольных семейств среди всех правильных семейств булевых функций. Построены новые классы правильных семейств функций (рекурсивно треугольные, локально треугольные, сильно квадратичное семейство); получены оценки на число рекурсивно треугольных семейств; для некоторых правильных семейств булевых функций получены точные значения мощности образа отображений, задаваемых этими правильными семействами. Предложен новый способ порождения квазигрупп на основе правильных семейств функций; доказан ряд утверждений о числе ассоциативных троек в порождаемых квазигруппах; предложен новый алгоритм шифрования, сохраняющего формат (FPE-схема), основанный на квазигрупповых операциях.

Диссертация представляет собой самостоятельное законченное исследование, обладающее внутренним единством. Положения, выносимые на защиту, содержат новые научные результаты и свидетельствуют о личном вкладе автора в науку:

1. Между булевыми правильными семействами и одностоковыми ориентациями графов булевых кубов (USO-ориентациями), а также между булевыми правильными семействами и булевыми сетями с наследственно единственной неподвижной точкой (HUFP-сетями) существует естественное соответствие. Между правильными семействами в логике произвольной значности и кликами в обобщенных графах Келлера также существует естественное соответствие.
2. Стабилизатор множества правильных семейств функций представляет собой множество пар согласованных изометрий пространства Хэмминга (согласованных перенумераций и перекодировок).
3. Отображения, задаваемые правильными семействами булевых функций, всегда имеют четное число неподвижных точек.

4. Мощность множества правильных семейств булевых функций размера n $T(n)$ удовлетворяет отношению $\log_2 T(n) = \Theta(2^n \cdot \log_2(T(n)))$. Треугольные семейства составляют бесконечно малую долю среди всех правильных семейств булевых функций.
5. Локально треугольные, рекурсивно треугольные и сильно квадратичное семейства являются правильными. Мощность образов рассмотренных в работе квадратичных булевых правильных семейств близка к максимально возможной.
6. Предложенная в работе конструкция позволяет порождать квазигруппы с помощью правильных семейств функций. Алгоритм шифрования, построенный на основе этой конструкции, сохраняет формат исходных сообщений (является FPE-схемой). Ряд утверждений о числе ассоциативных троек в квазигруппах, построенных на основе предложенной конструкции, позволяет свести вопрос об изучении индексов ассоциативности от всех пар правильных семейств к классам эквивалентности пар правильных семейств.

В диссертации применяются методы алгебры, дискретной математики, криптографии, теории графов, теории сложности.

Результаты диссертации имеют законченный характер и снабжены строгими математическими доказательствами, являются новыми, прошли апробацию на международных конференциях и научных семинарах. Основные результаты диссертационной работы изложены в работах, которых опубликованы в центральных научных изданиях, индексируемых в базах данных Web of Science, Scopus, RSCI и рекомендованных для защиты из списка МГУ.

На заседании 21.11.2025 диссертационный совет принял решение присудить Царегородцеву К.Д. ученую степень кандидата физико-математических наук.

При проведении тайного голосования диссертационный совет в количестве 19 человек, из них 9 докторов наук по специальности рассматриваемой диссертации, участвовавших в заседании, из 23 человек, входящих в состав совета, проголосовали: за 19, против нет, недействительных бюллетеней нет.

Председатель
диссертационного совета,
д.ф.-м.н., профессор **Чубариков В.Н.**

Ученый секретарь
диссертационного совета,
к.ф.-м.н. **Кибкало В.А.**

Дата 21.11.2025