ОТЗЫВ

на автореферат диссертации Царегородцева Кирилла Денисовича на тему
«Правильные семейства функций и порождаемые ими квазигруппы:
комбинаторные и алгебраические свойства»,
представленную на соискание ученой степени кандидата физико-математических наук
по специальности 1.1.5. Математическая логика, алгебра,
теория чисел и дискретная математика

Одним из возможных направлений исследований в современной теоретической криптографии является построение различных криптографических механизмов на основе конечных квазигрупп. Так, например, квазигрупповое умножение может использоваться как основной нелинейный элемент в симметричных криптографических механизмах, таких как поточные и блочные шифры, хэш-функции, генераторы псевдослучайных чисел. Аналогичным образом можно строить и различные асимметричные схемы шифрования и электронной подписи, используя квазигрупповое умножение в качестве сложнообратимой операции. Для указанных приложений важно уметь задавать квазигруппы достаточно больших размеров эффективным образом. Задание квазигруппы с помощью таблицы умножения в таком случае плохо применимо, поскольку используемые квазигруппы могут иметь порядок 2^{64} и более. В исследовательской литературе предлагался ряд подходов для решения задачи эффективного задания квазигруппы. В качестве примеров можно выделить изотопы хорошо изученных групп (например, группы точек эллиптической кривой), прямые и иные виды произведений, линейные регистры сдвига над группами, а также функциональное задание квазигрупповой операции, при котором операция умножения задается с помощью семейства функций k-значной логики. Одним из применяемых в последнем случае способов является задание операции с помощью правильных семейств функций, введенных в работах В.А. Носова 1998-1999 г. Такие семейства активно изучались В.А. Носовым и его учениками, А.Е. Панкратьевым и А.В. Галатенко. Правильные семейства функций являются основным объектом изучения в диссертации К.Д. Царегородцева.

Первая глава диссертации посвящена введению основных понятий, таких как правильное семейство, квазигруппа и т.д. Там же содержится обзор известных результатов, касающихся правильных семейств, а также ряд результатов, посвященных таким важным с точки зрения криптографии характеристикам квазигрупп, как индекс ассоциативности, полиномиальная полнота, наличие подквазигрупп. В главе содержатся и новые результаты: так, например, предлагается новый метод задания квазигрупповой операции с помощью правильных семейств, изучаются некоторые особенности такой операции. Приводится новый класс булевых квадратичных семейств, доказывается правильность каждого элемента класса, изучается такая характеристика, как степень квадратичности. Семейства класса содержат только линейные члены и попарные произведения переменных, а значит, допускают относительно компактное задание, что важно с точки зрения приложений.

Вторая глава посвящена изучению различных эквивалентных определений правильных семейств и следствий из этих эквивалентностей. Основными изучаемыми объектами здесь являются одностоковые ориентации булева куба, булевы сети с наследственно единственными неподвижными точками, клики заданного размера в обобщенных графах Келлера. Показано, что все различные описания дают одни и те объекты (правильные семейства). Полученные биективные соответствия позволяют перенести часть результатов из одной области исследований в другую, зачастую в более общей формулировке. Так, например, автору удается доказать правильность т.н. «рекурсивно треугольных» и «локально треугольных» семейств. Также показано, что булевы правильные семейства могут быть охарактеризованы как семейства, каждая возможная проекция которых не является самодвойственным отображением.

Третья глава посвящена изучению свойств правильных семейств. Доказан важный результат о стабилизаторе множества правильных семейств в классе биективных преобразований. Вычислены мощности образа двух квадратичных булевых правильных семейств, что, в свою очередь, позволяет оценить снизу число различных квазигрупп, порождаемых этими семействами с помощью одной из конструкций построения квазигрупповой операции из правильных семейств. Показано, что множество подстановок, задаваемых правильными семействами, замкнуто относительно взятия обратного элемента.

Четвертая глава посвящена практическому приложению полученных результатов. Автор предлагает новый квазигрупповой алгоритм шифрования с сохранением формата сообщений (т.н. FPE-схема), основанный на конструкции из первой главы. Обратимость подстановок, показанная в третьей главе, позволяет утверждать, что как алгоритм зашифрования, так и алгоритм расшифрования задаются правильными семействами функций. Приведены результаты статистических экспериментов по вычислению различных характеристик квазигрупп, порожденных правильными семействами, таких как индекс ассоциативности, простота, неаффинность, полиномиальная полнота. Экспериментально найдены мощности множеств некоторых классов булевых правильных семейств небольшого размера (треугольные, рекурсивно и локально треугольные семейства).

Считаю, что в своей диссертационной работе К.Д. Царегородцеву удалось получить интересные и содержательные результаты, имеющие как теоретическую значимость, так и практическую ценность.

Автореферат диссертации достаточно полно отражает результаты работы, которые представлялись на 10 конференциях и 6 научных семинарах. По теме диссертации опубликовано 9 статей в рецензируемых журналах, включая 6 статей в изданиях, входящих в ядро РИНЦ, и 2 статьи в изданиях из дополнительного списка Московского государственного университета имени М.В. Ломоносова.

В целом диссертация Царегородцева К.Д. на тему: «Правильные семейства функций и порождаемые ими квазигруппы: комбинаторные и алгебраические свойства» соответствует требованиям, предъявляемым к диссертациям на соискание учёной степени кандидата

физико-математических наук по специальности 1.1.5. Математическая логика, алгебра, теория чисел и дискретная математика.

Учитывая все вышеизложенное, считаю, что Царегородев К.Д. заслуживает присуждения ученой степени кандидата физико-математических наук по специальности 1.1.5. Математическая логика, алгебра, теория чисел и дискретная математика.

Рецензент:
Кандидат физико-математических наук,
Главный специалист ООО «СФБ Лаб»

И.М. Арбеков

Адрес места работы:
127273, Россия, г. Москва, ул. Отрадная, д. 2Б, стр. 1
ООО «СФБ Лаб»
Тел.: +7(495)6454438; e-mail: info@sfblaboratory.ru

Подпись сотрудника И.М. Арбекова удостоверяю.

Генеральный директор
ООО «СФБ Лаб»

О.А. Залунин