ОТЗЫВ

научного руководителя на диссертацию

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).

В настоящее время для защиты информации применяются различные способы преобразования представляющих ее данных. Основное внимание разработчиков концентрируется на создании таких способов преобразования, которые отвечают требованиям к росту объемов и повышению скорости передачи. В связи с этим в качестве базисных элементов применяются, как правило, наиболее просто реализуемые и быстро работающие логические и арифметические операции, а в качестве усложняющих элементов применяются узлы замены блоков исходной последовательности, осуществляющие их нелинейную замену.

Вместе с тем, рост производительности процессоров и объемов оперативной памяти позволяет использовать более сложные базисные элементы, описываемые не унарными, а произвольными случайными неассоциативными и некоммутативными бинарными операциями. Такой подход существенно усложняет задачу анализа перечисленных способов преобразования информации. В частности, для обеспечения надежности защиты передаваемой информации необходимо строить схемы таким образом, чтобы множество применяемых результирующих преобразований удовлетворяло свойству кратной транзитивности.

Это делает задачу разработки способов построения и анализа рассматриваемых в диссертационной работе функциональных систем, удовлетворяющих требованиям биективности и кратной транзитивности, весьма актуальной.

Данная задача является новой как по постановке, так и по методам решения. Изучаемые вопросы практически не затрагивалась в публикациях других авторов. Несмотря на то, что вопросы функциональной и полиномиальной полноты функциональных базисов, в том числе содержащих квазигрупповые операции, уже достаточно полно и подробно изучены, применить их для решения задачи исследования условий кратной транзитивности таких систем не представляется возможным.

Поэтому автору диссертации пришлось разрабатывать собственный достаточно глубокий математический аппарат, включающий понятия полных, правильных и свободных разметок, а также свободных продолжений разметок, являющихся аналогом свободных объектов в алгебре, а также их k-мерных аналогов.

Предложенный автором и описанный в диссертационной работе аппарат разметок оказался эффективным при практическом применении. Он позволил сформулировать и обосновать интересный с теоретической точки зрения способ проверки универсального критерия кратной транзитивности. Оказалось, что формулировки многих результатов, например критериев биективности и транзитивности сети, остаются справедливыми для любых мощностей основного множества, удовлетворяющих естественным нижним ограничениям.

На основе найденного критерия предложены и строго обоснованы алгоритмы построения биективных сетей с условием кратной транзитивности как для случая, когда исходные бинарные операции являются квазигруппами, так и для более общего случая, когда бинарные операции являются подстановками только по одной из переменных. При этом существенную роль для завершения некоторых доказательств сыграли оценки для гипотезы Эванса, доказанные Б. Сметанюком и Л.Д. Андерсоном.

В частности, с помощью данных алгоритмов удалось построить примеры практически значимых биективных сетей с небольшим количеством вершин, для которых соответствующие классы блочных преобразований обладают требуемой кратной транзитивностью, и которые можно использовать для построения широких классов кратно транзитивных сетей с требуемыми особенностями архитектуры.

Диссертация представляет собой завершенную научно-исследовательскую работу, в которой на основании выполненных автором исследований разработан математический аппарат, позволивший получить исчерпывающее решение поставленной перед диссертацией задачи, а полученные результаты дают исчерпывающее представление о возможности и практических аспектах использования бинарных функциональных сетей для обеспечения защиты информации.

Все вышеуказанные результаты являются новыми и получены автором самостоятельно. В процессе работы И.А. Чередник проявил себя самостоятельным сложившимся исследователем, владеющим различными методами теоретического исследования. В работе используются методы алгебры, комбинаторики и теории графов, теории функциональных систем, дискретной математики, и др. Помимо данного исследования им опубликованы серьезные результаты и по другим задачам, не вошедшим в диссертацию, в

области теории автоматов и дискретных функций, теории групп, теории решеток и др., относящиеся к различным проблемам защиты информации.

Диссертация соответствует критериям, установленным в «Положении о присуждении ученых степеней в Московском государственном университете имени М.В. Ломоносова», и рекомендуется к защите в диссертационном совете МГУ 05.01 ФГБОУ ВО МГУ по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность» (физико-математические науки).

Научный руководитель
член-корреспондент Академии криптографии РФ
д.ф.-м.н., профессор А. В. Черемушкин