Министерство образования и науки Российской Федерации

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕСКОГО»

РЕЦЕНЗИЯ

на статью «Конструкции некоторых схем разделения секрета на основе линейных кодов» доктора физико-математических наук, профессора кафедры информационной безопасности и теории управления Ульяновского государственного университета Рацеева Сергея Михайловича.

Статья посвящена исследованию структуры схем разделения секрета, построенных на линейных кодах помехоустойчивого кодирования.

Актуальность построения и анализа схем разделения секрета, преследующие различные прикладные цели в области защиты информации, в текущий момент развития информационных технологий не вызывает сомнений, хотя по-прежнему ещё не получили широкого применения во многих прикладных задачах и ситуациях, где могли бы уже хорошо выполнять свои функциональные возможности.

Статья состоит из введения и пяти пунктов.

В Введение представлено развёрнутое определение структуры доступа, которое является отправной точкой для построения схем разделения секрета на основе линейного кода, соответствующих выбранной структуре доступа.

В первых четырёх разделах, по сути, представлены критерии, обслуживающие правила построения схемы разделения секрета на основе линейного кода при заданной системе доступа. Причём, эти результаты снабжены иллюстрирующими примерами.

В пятом разделе рассмотрен случай, когда участники не доверяют дилеру (раздающему доли секрета), и представлена схема, позволяющая каждому участнику иметь возможность проверить корректность своей доли.

Автором, несомненно, проведена интересная и полезная работа по исследованию указанного типа схем разделения секрета.

Есть три незначительных замечания.
1) На протяжении текста присутствует ряд некорректно оформленных переносов.
2) В последней строке Введения вместо «участников» стоит слово «частников».

3) Автор использует понятия «совершенной системы» и «идеальной системы», не указывая, что под этим подразумевает, поскольку приписывает системе то или иное качество без всякой аргументации «почему». Из контекста ясно, что в его трактовке этих понятий следует, что совершенная система может быть дополнительно ещё и идеальной, т.е. класс идеальных является подклассом совершенных или эти классы имеют непустое пересечение. Хотя по исходному определению идеальной и совершенной системы, что идёт от Шеннона, всякая совершенная система является идеальной, но не всякая идеальная является совершенной, т.е. совершенная является подклассом идеальной. Здесь либо следует просто пояснить, какими именно критериями пользуется автор для их определения, либо как-то согласовать их с известной традицией.

Научная статья Рацеева С. М. «Конструкции некоторых схем разделения секрета на основе линейных кодов» соответствует всем требованиям, предъявляемым к работам такого вида. При учёте указанных замечаний данная статья может быть рекомендована к публикации.

Рецензент: доцент кафедры теоретических основ компьютерной безопасности и криптографии,
кандидат физ-мат. наук _____ НОВИКОВ В.Е.

подпись, дата