ОТЗЫВ

на автореферат диссертации Кондратёнка Н.В. «Свойства теоретико-числовых и криптографических алгоритмов в дедекиндовых кольцах», представленной на соискание ученой степени кандидата физико-математических наук 01.01.06 – математическая логика, алгебра и теория чисел при Государственном научном учреждении «Институт математики Национальной академии наук Беларуси»

В настоящее время интенсивно развивается алгоритмическая теория чисел, что объясняется значительными успехами в криптографии с открытым ключом и появлением высокопроизводительных компьютеров. Работа посвящена исследованию свойств теоретико-числовых и криптографических алгоритмов в дедекиндовых кольцах. В частности, получены следующие результаты.

Предложено несколько алгоритмов для определения простоты идеала и оценки эффективности этих алгоритмов. Доказаны экстремальные свойства алгоритма Евклида в факториальных кольцах. Здесь возникает естественная проблема, принадлежит ли данное кольцо к указанному классу. В работе найдены эффективные алгоритмы решения этой проблемы.

Приведены необходимые условия для параметров криптосистемы RSA, обеспечивающие ее криптостойкость. Показана корректность полученной криптосистемы и представлены ограничения на дедекиндово кольцо для ее эффективного применения. Исследована криптосистема RSA в дедекиндовых кольцах с конечным полем остатков. Здесь целью является доказательство теорем, связанных с криптостойкостью системы. Например, теоремы Винера, теоремы об эквивалентности факторизации и взлома криптосистемы, а также проводится изучение методов взлома криптосистемы.

Считаю, что диссертация Кондратёнка Н.В. выполнена на высоком научном уровне, и ее результаты вносят значительный вклад в алгоритмическую теорию чисел и соответствуют требованиям, предъявляемым ВАК к кандидатским диссертациям, а их автор заслуживает присуждения степени кандидата физико-математических наук по специальности 01.01.06 – математическая логика, алгебра и теория чисел.

ПОДПИСЬ УДОСТОВЕРЯЮ
Начальник управления
организационной работы и
документационного обеспечения
Л.Б. Черкасская
04 2023

Ведущий научный сотрудник
НИЛ физики электронных материалов
кафедры физики полупроводников
и наноэлектроники физического
факультета Белорусского государственного
университета
кандидат физ.-мат. наук, доцент А. Т. Власов