АКЦИОНЕРНОЕ ОБЩЕСТВО
“НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ИНСТИТУТ
“Р У Б И Н”

Кантемировская ул., дом. 5, Санкт-Петербург, 194100, тел.: (812)670-89-89, факс: (812)596-35-81, e-mail: inforubin@rubin-spb.ru
ИНН/КПП 7802776390/780201001, ОГРН 1127847043720, ОКПО 07542394

РЕЦЕНЗИЯ

на выпускную квалификационную работу
«Отзыв со связыванием в схеме кольцевой подписи на решетках»,
выполненную обучающимся гр. 3651004/40101
Санкт-Петербургского политехнического университета Петра Великого
Рехвиашвили Ириной Шотовной

Актуальность работы

В настоящее время электронные подписи являются одним из важнейших криптографических механизмов защиты информации от нарушения целостности, подделки авторства, отказа от авторства. Сама возможность широкого применения электронных подписей в различных приложениях для решения задач аутентификации данных и их источника, стала причиной появления таких новых разновидностей электронных подписей, как разовая подпись, подпись вслепую, групповая подпись и др. Особый интерес в последние годы вызывает применение для решения названных задач, так называемой, кольцевой подписи, предоставляющей автору, подписавшему документ, возможность сохранять полную анонимность в пределах заданной группы авторов, и нашедшей широкое применение в решении таких прикладных задач, как организация не отслеживаемых транзакций в системах электронной валюты, реализация принципа тайного голосования в системах электронного голосования и др. При этом, для подобных систем должна быть обеспечена возможность динамического изменения состава участников группы путем организации отзыва права подписи.

Вместе с тем, появление квантовых алгоритмов, позволяющих за полиномиальное время решать многие задачи, лежащие в основе безопасности большинства схем подписи, потребовало наличия стойких к атакам квантового компьютера криптосистем, основанных на новых вычислительно трудных задачах, в частности на основе задач теории решеток и механизмов организации отзыва в схемах кольцевой подписи на решетках.

Поэтому тема выпускной квалификационной работы И.Ш. Рехвиашвили, посвященной исследованию механизмов отзыва права подписи у участников схем кольцевой подписи на решетках, с целью повышения эффективности процедур отзыва, является чрезвычайно актуальной.

Характеристика работы

Дипломная работа Рехвиашвили И.Ш. содержит: введение, три главы; заключение и список использованных источников.

Во введении указаны объект и предмет исследования, сформулирована цель исследования и поставленные задачи.

Первая глава работы посвящена анализу основных свойств схем кольцевых подписей, обоснованию и выбору решеток в качестве математического аппарата кольцевой подписи, описанию вычислительно трудных задач, основанных на решетках, а также протокола кольцевой подписи на решетках.

Во второй главе осуществлено сравнение механизмов отзыва, предложены варианты применения выбранного механизма. В результате разработана схема кольцевой подписи на решетках с отзывом со связыванием, использующая шифрование с открытым ключом с тестами на равенство для реализации свойств связываемости.

В третьей главе осуществлена программная реализация разработанной схемы кольцевой подписи на решетках с отзывом со связыванием, произведена оценка влияния выбранного механизма отзыва на эффективность системы путем замера времени выполнения алгоритмов реализованной системы.

Замечания по работе

Несмотря на то, что материал дипломной работы логически структурирован и написан научным стилем, проведенные исследования в целом соответствуют поставленным в работе задачам, работа имеет ряд недостатков:

1 при оценивании эффективности предложенной системы по времени выполнения алгоритмов не указан механизм измерения (текущее случайное значение, среднее значение, ошибка измерения) времени;

2 не приведена оценка допустимого числа членов группы, чтобы время работы алгоритмов не превышало допустимого;

3 оценивание параметров схемы только по влиянию параметров механизма отзыва не в полной мере позволяет оценить безопасность системы.

Вместе с тем, отмеченные недостатки не снижают общего положительного впечатления от работы.

Заключение

Выпускная квалификационная работа Рехвиашвили Ирины Шотовны по теме «Отзыв со связыванием в схеме кольцевой подписи на решетках» соответствует требованиям, предъявляемым к выпускным квалификационным работам, и заслуживает оценки *«отлично»*.

Рецензент
Ведущий научный сотрудник
НИО АО «НИИ «Рубин»
д.т.н., доцент _____ А.Н. Буренин

«22» января 2020 г.

С рецензией согласен.
Генеральный директор
АО «НИИ «Рубин» _____ С.С. Степанов

«22» января 2020 г.