БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Факультет прикладной математики и информатики

Кафедра дискретной математики и алгоритмики

Аннотация к магистерской диссертации

«Тайное многостороннее вычисление цифровой подписи на эллиптических кривых»

Дядюк Алексей Юрьевич

Научный руководитель – кандидат физико-математических наук
Васильков Д.М.

Минск, 2020

Реферат

Магистерская диссертация, 40 страниц, 6 рисунков, 10 источников.

ТАЙНОЕ МНОГОСТОРОННЕЕ ВЫЧИСЛЕНИЕ, ЦИФРОВАЯ ПОДПИСЬ, ЭЛЛИПТИЧЕСКИЕ КРИВЫЕ, ГОМОМОРФНОЕ ШИФРОВАНИЕ, ECDSA, EdDSA, КРИПТОГРАФИЯ.

Объект исследования – алгоритмы цифровой подписи на эллиптических кривых основанных на тайном многостороннем вычислении.

Цель работы – изучить доступные алгоритмы цифровой подписи и их проблемы, изучить возможности оптимизации, реализовать их. Рассмотреть алгоритмы длинной арифметики.

Методы проведения работы – анализ, эксперимент, тестирование, сравнение.

Результаты – Изучены и реализованы алгоритмы для длинной арифметики. Изучены и реализованы алгоритмы для оптимальной генерации параметров. Изучен и реализован подход гомоморфного шифрования на основе криптосистемы Пэйе. Изучен и реализованы алгоритм ECDSA для схемы 2 из 2. Изучен и реализованы алгоритм EdDSA для схемы n из n. Рассмотрена модификация алгоритма EdDSA для схемы n из m.

Область применения – блокчейн, любые криптосистемы в которых необходимо производить цифровую подпись с использованием нескольких ключей.

Abstract

Master thesis, 40 pages, 6 figures, 10 references.

SECURE MULTI-PARTY COMPUTATION, DIGITAL SIGNATURE, ELLIPTIC CURVES, HOMOMORPHIC ENCRYPTION, ECDSA, EdDSA, CRYPTOGRAPHY.

Object of research – digital signature algorithms on elliptic curves based on secret multi-sided computing.

Objective – study the available digital signature algorithms and their problems, to study optimization possibilities, to implement them. Consider algorithms for long arithmetic.

Methods – analysis, experiment, testing, comparison.

*Result*s – studied and implemented algorithms for long arithmetic. Algorithms for optimal parameter generation are studied and implemented. The homomorphic encryption approach based on the Paillier cryptosystem was studied and implemented. The ECDSA algorithm for schemes 2 of 2 was studied and implemented. The EdDSA algorithm for n of n schemes was studied and implemented. A modification of the EdDSA algorithm for a circuit n of m is considered.

Application area – blockchain, any cryptosystems in which it is necessary to digitally sign using several keys.