Отзыв научного руководителя

на выпускную квалификационную работу на степень бакалавра студента 4-го курса

Федерального государственного автономного образовательного учреждения высшего образования "Южный федеральный университет"

Института математики, механики и компьютерных наук им. И.И. Воровича

Денисова Илии Игоревича

на тему "Модификация примитива современного криптографического агрегата"

Целью работы И.Денисова является построение модификации не интерактивного протокола доказательства знания с нулевым разглашением "ZK-SNARK" путём расширения полиномиальной базы его квадратичной арифметической программы и анализ параметров модифицированного протокола. Основными задачами являются: модификация протокола ZK-SNARK, анализ параметров модифицированного протокола и построение примеров реализации изначальной и модифицированной версий ZK-SNARK.

Задача построения, изучения и модификации не интерактивных протоколов доказательства знания с нулевым разглашением является актуальной. Это также подтверждается, во-первых, теоретическими исследованиями, публикуемыми в известных рецензируемых изданиях, такими учеными как Э.Гэбисон, Ц.Джентри, Дж.Гроус, Б.Фиш, Б.Банц, а во-вторых, широкой применимостью различных решений этой задачи, в том числе в различных имплементациях технологии блокчейн.

При проведении исследования И.Денисовым получена модификация не интерактивного протокола доказательства знания с нулевым разглашением "ZK-SNARK" путём расширения полиномиальной базы его квадратичной арифметической программы и анализ параметров модифицированного протокола, показывающий наличие его преимущества   
в длине нагружающей канал общей ссылочной строки величиной примерно в 5%, а также заложены направления для дальнейших исследований в сторону обобщения полученного способа улучшающей модификации.

Над темой диплома И.Денисова работал активно и усердно. После доработки результат может быть опубликован в научном издании. Степень оригинальности выпускной квалификационной работы соответствует требованиям, предъявляемым к выпускным квалификационным работам данного уровня образования. Диплом, имеет теоретический и практический интерес, удовлетворяет требованиям, предъявляемым к работам по направлению «Прикладная математика и информатика» и заслуживает оценки «Отлично».

|  |  |  |
| --- | --- | --- |
| Научный руководитель  к.т.н., доц. кафедры АДМ  Института математики, механики и компьютерных наук  им. И. И. Воровича ЮФУ |  | В. В. Мкртичян |