УДК 004.056.55

РАЗРАБОТКА СХЕМЫ ПОРОГОВОЙ ПОДПИСИ НА ОСНОВЕ АЛГОРИТМА RAINBOW

Иогансон И. Д. (Университет ИТМО), **Голованов А. А.** (Университет ИТМО), **Дакуо Ж.-М. Н.** (Университет ИТМО)

Научный руководитель – доцент, д. т. н. Беззатеев С. В.

(Университет ИТМО)

В данной работе приведена схема разделения секрета, разработанная на основе схемы Шамира, использующая в качестве секрета многомерные полиномы. Представленная схема позволяет реализовать такие протоколы пороговой подписи как: генерация открытого ключа и теней закрытого ключа, подпись сообщения с помощью теней закрытого ключа и проверка подписи.

Введение. На сегодняшний день стало ясно, что появление первых квантовых компьютеров с большим количеством кубит всего лишь вопрос времени. Поэтому важно уже сейчас готовиться к этому и изучать постквантовые криптографические схемы. Одной из таких схем является схема электронной подписи на основе многомерных уравнений Rainbow. Данная схема входит в тройку финалистов третьего раунда конкурса NIST на звание стандарта электронной подписи, что говорит о высоком уровне доверия к данной схеме.

Схемы пороговой подписи нужны для того, чтобы любая коалиция из уполномоченных пользователей, количеством не менее порогового значения, могла сформировать электронную подпись от лица всех уполномоченных пользователей. Подобные схемы имеют широкое распространение в децентрализованных системах, таких как, например, криптовалюты. Однако, на сегодняшний день не существует полноценных постквантовых схем пороговой подписи.

Таким образом, целью данной работы является разработка схемы пороговой подписи на основе алгоритма Rainbow.

Основная часть. В данной работе представлена схема разделения секрета на основе схемы Шамира, которая пригодна для использования в постквантовых алгоритмах на основе многомерных уравнений. Представленная схема позволяет производить вычисления над тенями, не раскрывая секрета, к примеру, складывать, умножать и производить композицию секретов. Также, как и в оригинальной схеме разделения секрета Шамира, приведенная в данной работе схема позволяет из имеющихся теней генерировать тени для новых пользователей, что упрощает масштабирование системы.

Использование подобной схемы позволяет реализовать такие протоколы пороговой подписи как: генерация открытого ключа и теней закрытого ключа, подпись сообщения с помощью теней закрытого ключа и проверка подписи.

Выводы. Постквантовая схема пороговой подписи в будущем может быть использована в различных децентрализованных системах, таких как, например, криптовалюты.

Иогансон И. Д. (автор) Подпись

Беззатеев С. В. (научный руководитель) Подпись