УДК 004.056.55

АНАЛИЗ СХЕМ РАЗДЕЛЕНИЯ СЕКРЕТА НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ

Кустов Е.Ф. (Университет ИТМО)
Научный руководитель – д.т.н, профессор Беззатеев С.В.
(Университет ИТМО)

Аннотация. Были рассмотрены современные схемы разделения секрета на эллиптических кривых. Кроме того, было проведена проверка схем на соответствие критериям Шамира.

Введение. Схемы разделения секрета применяются в случаях, когда существует значимая вероятность компрометации хранителей секрета, но вероятность недобросовестного сговора значительной части участников считается пренебрежимо малой. Однако большинство схем основаны на задаче факторизации и дискретного логарифмирования. После изобретения Питером Шором квантового алгоритма возник вопрос о создании новых систем устойчивых к атаке с использованием квантового компьютера. Одним из возможных решений описанной проблемы может являться схема, основанная на эллиптических кривых.

Основная часть. Был проведён сравнительный анализ схем разделения секрета на основе шести критериев Шамира: размер доли меньше или равен самому секрету, возможность повторного использования секрета, невозможность проанализировать секрет, возможность добавления нового участника, возможность обновить секрет и возможность изменения веса долей. Большинство современных схем, хоть и удовлетворяют поставленным критериям, однако не являются постквантовыми.

Возможным решением могут являться схемы на изогениях кривых. Исследований схем, основанных на изогениях, не так много. Основная суть данных схем заключается в использование модифицированного протокола SIDH. Схемы работают на жестких однородных пространствах (HHS), а эффективные квантово-безопасные реализации основаны на графах суперсингулярных изогений, используемых в CSIDH и CSI-FiSh. HHS был впервые использован для криптографии в CSIDH, и именно с помощью HHS можно добиться защиты от алгоритма Шора, внедрив схему разделения секрета в теорию изогении.

Однако постквантовые схемы разделения секрета не отвечают всем заданным критериям. Решением может являться объединение двух подходов, используемых в доквантовых и постквантовых схемах. Предлагается разработать систему на основе спаривания точек на изогении эллиптических кривых.

Выводы. В результате исследований был получен сравнительный анализ на основе критериев Шамира современных схем разделения секрета на эллиптических кривых. Исходя из анализа, ясно, что схемы, удовлетворяющие критериям Шамира, не являются постквантовыми, а постквантовые схемы не удовлетворяют критериям Шамира. Был предложен вариант теоретического объединения двух подходов.

Кустов Е.Ф. (автор) Подпись

Беззатеев С.В. (научный руководитель) Подпись