УДК 004.056.55

РАЗРАБОТКА СХЕМ ПОДПИСИ ID-BASED КРИПТОГРАФИИ С ИСПОЛЬЗОВАНИЕМ ФУНКЦИЙ СПАРИВАНИЯ НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ

Дакуо Ж. -М. Н. (федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»),

Научный руководитель – **Давыдов В. В.** (федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»)

Данная работа посвящена рассмотрению различных ID-Based схем подписи с использованием функций спаривания на эллиптических кривых. В ходе работы были построены новые схемы с использованием 3 и 4 типов спаривания, а также проведен сравнительный анализ полученных схем.

Введение. В наше время ID-Based схемы подписи, созданные на спариваниях Вейля и Тейта, получили новый виток в развитии благодаря тому, что криптография на эллиптических кривых сделала большой шаг вперед. И также ID-Based криптосистемы подходят для внутреннего использования в компаниях, где уже имеется общий доверенный сервер, и данные схемы могут использоваться в рамках государства, где на их основе можно создать новый тип удостоверения личности, с которым можно легко будет легко и удобно подписывать электронные чеки, квитанции, юридические документы и тому подобное.

Основная часть. Были рассмотрены три ID-Based схемы подписи: схема Лаи и Аватаси, схема Патерсона и схема Гесса. Все эти схемы основаны на спариваниях первого типа. Последние исследования показали, что использование спариваний второго и третьего типов позволяет ускорить вычисления и не потерять в защищенности систем. Но для некоторых систем данный переход невозможен ввиду их внутреннего устройства. В своей кандидатской работе Шачам вывел и описал четвёртый тип спариваний, который является более универсальным, что позволяет попытаться сократить время, необходимое для проведения вычислений в ID-Based схемах подписи. В данной работе рассматриваются схемы с измененными типами спаривания и проводится их сравнение с оригиналами и друг с другом.

Выводы. В ходе работы были рассмотрены ID-Based схемы подписи. На их основе были разработаны новые схемы с использованием новых типов спариваний на эллиптических кривых. Проведен сравнительный анализ между оригинальными схемами подписи и полученными.

Дакуо Ж.-М. Н. (автор)

Давыдов В. В. (научный руководитель)