УДК 004.056.2

Анализ алгоритмов подписи, обладающих свойством доказательства факта подделки

Голованов А. А.[1]
Научный руководитель – д.т.н., профессор Беззатеев С. В.[1]
[1]Университет ИТМО
aagolovanov@itmo.ru

Работа выполнена в рамках государственного задания (проект FSER-2025-0003)

Введение

Подпись со свойством доказательства факта подделки (FS-подпись, от англ. Fail-Stop Signature) – криптографический примитив, аналог цифровой подписи, позволяющий владельцу ключа предоставить третьей стороне (честному судье) доказательство, что подпись взломана [1, 2, 3]. Безопасность любой схемы цифровой подписи основана на сложности решения некоторой вычислительной задачи. Модель FS-подписи обоснована тем, что невозможно доказать сложность задачи, если не найден эффективный алгоритм её решения. Так, модель предполагает злоумышленника, который обладает знанием о таком алгоритме. Предполагая такого злоумышленника, подделка классической цифровой подписи неотличима от легитимной подписи, а в рамках модели FS-подписи с преобладающей вероятностью они отличаются и становится возможным предоставить доказательство факта подделки.

Основная часть

Работа состоит в анализе модели FS-подписи и механизмов, лежащих в основе конкретных схем. Обосновывается, что модель FS-подписи не состоятельна в действительности – предлагается пример сценария атаки на FS-подпись.

Предложены новые криптографические примитивы и протоколы, использующие механизмы, разработанные для реализации FS-подписи. Рассматриваются такие механизмы, как:

— связывающий гомоморфизм (англ. bundling homomorphism);
— порождающий элемент, устойчивый к коллизиям (англ. collision resistant group generator);
— настраиваемая хэш-функция (англ. compressing tweakable hash functions).

Рассмотрены новые криптографические примитивы и протоколы:

— доказательство возможности;
— групповая подпись на основе перечисленных механизмов;
— коалиционная подпись с заданным порогом вхождения в коалицию.

Выводы

Проведён сравнительный анализ существующих решений FS-подписей. Предложены новые схемы на основе механизмов FS-подписей. Результаты работы предполагается использовать в дальнейших разработках.

Литература

1. Boschini C. и др. That’s Not My Signature! Fail-Stop Signatures for a Post-quantum World // Advances in Cryptology – CRYPTO 2024 / под ред. Reyzin L., Stebila D. Cham: Springer Nature Switzerland, 2024. Т. 14920. С. 107–140.

2. Van Heyst E., Pedersen T. P. How to Make Efficient Fail-stop Signatures // Advances in Cryptology — EUROCRYPT’ 92 / под ред. Rueppel R. A. Berlin, Heidelberg: Springer Berlin Heidelberg, 1993. Т. 658. С. 366–377.
3. Mashatan A., Ouafi K. Efficient Fail-Stop Signatures from the Factoring Assumption // Information Security / под ред. Lai X., Zhou J., Li H. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011. Т. 7001. С. 372–385.