УДК 004.056.6

ОБЗОР СУЩЕСТВУЮЩИХ ПОДХОДОВ К РАЗДЕЛЕНИЮ СЕКРЕТА В РАМКАХ ПОРОГОВЫХ ПОДПИСЕЙ

Волков А. Г. («ИТМО»),
Научный руководитель – кандидат технических наук, доцент Таранов С. В. (ИТМО)

Аннотация. С ростом важности безопасности и конфиденциальности в цифровой среде вопросы разделения секрета становятся все более актуальными. В рамках данной работы проводится обзор существующих методов разделения секрета, сосредотачиваясь на их применении в пороговых подписях. Анализируются различные подходы к разделению секрета, их преимущества и ограничения.

Введение. Пороговые подписи набирают актуальность с каждым годом, помимо использования в рамках блокчейн-сетей, появляется всё больше и больше работ предлагающих использование пороговых подписей в новых сферах человеческой деятельности, тем самым более надёжно обеспечивая требования к существующим моделям, где необходимо взаимодействие множества членов группы. Методы разделения секрета играют важную роль в протоколах пороговых подписей, настолько, что некоторые из них накладывают ограничения или предлагают свойства для всей криптосистемы, которая её использует.

Основная часть. В рамках данной работы предлагается обзор существующих решений разделения секрета, за счёт которых достигается устойчивость криптосистемы к компрометации хранителя секрета, тем самым повышая общую стойкость криптосистемы.

Были рассмотрены такие схемы разделения секрета как схема Шамира, схема Блэкли, схемы, основанные на китайской теореме об остатках, схемы, основанные на решении систем уравнений.

Таким образом, обзор существующих основных методов разделения секретов позволил обратить более пристальное внимание на данные механизмы разделения секретов, обозначить области и криптосистемы, в рамках которых, данные механизмы разделения секрета демонстрируют себя оптимально. Помимо этого, в рамках обзора существующих решений стало возможным провести сравнительный анализ данных решений, что в последствии может быть использовано для дальнейшей работы в данном направлении.

Выводы. Рассматриваемые в данном докладе схемы разделения секрета, затрагивают основополагающие вопросы проблематики прикладной области, для решения которых и были предложены схемы пороговых подписей и схемы разделения секрета. Изучение данных вопросов и их анализ позволит сформировать базис для дальнейших работ в рамках диссертационной работы аспиранта.

Список использованных источников:

1. Давыдов В. В., Хуцаева А. Ф., Иогансон И. Д., Дакуо Ж.-М. Н., Беззатеев С. В. УСОВЕРШЕНСТВОВАННАЯ СХЕМА ПОРОГОВОЙ ПОДПИСИ CSI-FISH СО СВОЙСТВОМ БЫСТРОЙ СБОРКИ СЕКРЕТА // Вестник СибГУТИ. 2023. №1. URL: https://cyberleninka.ru/article/n/usovershenstvovannaya-shema-porogovoy-podpisi-csi-fish-so-svoystvom-bystroy-sborki-sekreta (дата обращения: 01.02.2024).
2. Парватов Николай Георгиевич Совершенные схемы разделения секрета // ПДМ. 2008. №2 (2). URL: https://cyberleninka.ru/article/n/sovershennye-shemy-razdeleniya-sekreta (дата обращения: 01.02.2024).
3. Н.Ф. Богаченко СХЕМА РАЗДЕЛЕНИЯ СЕКРЕТА МЕЖДУ ИЕРАРХИЧЕСКИ СВЯЗАННЫМИ УЧАСТНИКАМИ // МСиМ. 2022. №4 (64). URL:

https://cyberleninka.ru/article/n/shema-razdeleniya-sekreta-mezhdu-ierarhicheski-svyazannymi-uchastnikami (дата обращения: 07.02.2024).

Автор _____ Волков А. Г.

Научный руководитель _____ Таранов С. В.