УДК 004.056.55

РАЗРАБОТКА ПРОТОКОЛА ДОКАЗАТЕЛЬСТВА С НУЛЕВЫМ РАЗГЛАШЕНИЕМ ДЛЯ ГОМОМОРФНЫХ СИСТЕМ

Чапасов П. К. (Университет ИТМО)
Научный руководитель - Голованов А. А.
(Университет ИТМО)

Введение. Доказательство с нулевым разглашением (Zero-knowledge proof) - это криптографический протокол, позволяющий одной стороне протокола (доказывающему) доказать другой стороне (проверяющему), истинность определенного утверждения, не раскрывая никакой информации, кроме достоверности утверждения [1]. Не существует универсального протокола доказательства с нулевым разглашением, поэтому для каждой проблемы необходим свой уникальный протокол [2]. Так, не существует эффективного протокола для доказательства эквивалентности расшифрованного текста и шифротекста без раскрытия закрытого ключа асимметричной гомоморфной системы шифрования.

Основная часть. Данная работа состоит в разработке протокола обмена данными между двумя участниками [3], один из которых владеет закрытым ключом криптосистемы, а второй – шифротекстом, содержание которого он не знает. Цель протокола – доказательство с нулевым разглашением эквивалентности расшифрованного одной из сторон текста и шифротекста без раскрытия закрытого ключа ассиметричной гомоморфной системы шифрования. Доказательство строится на свойстве гомоморфности, позволяющем производить определенные математические операции с зашифрованным текстом и получать зашифрованный результат, который соответствует результату операций, выполненных с открытым текстом.

Выводы. Разработан протокол доказательства с нулевым разглашением для рассмотренной проблемы. Результаты работы предполагается использовать в дальнейших разработках.

Список использованных источников:

1. Goldwasser S., Micali S., Rackoff C. The knowledge complexity of interactive proof systems // SIAM Journal on Computing / M. Sudan - SIAM, 1989. - Vol. 18, Iss. 1. - P. 186-208. - ISSN 0097-5397; 1095-7111 - doi:10.1137/0218012;
2. Brassard G., Chaum D., Crépeau C. Minimum disclosure proofs of knowledge //Journal of computer and system sciences. - 1988. - Т. 37. - №. 2. - С. 156-189;
3. A. Fiat, A. Shamir. How to prove yourself: Practical solutions to identification and signature problems (1986) // Advances in Cryptology: Proc. Crypto’86, Lecture Notes in Computer Science 263, pp. 186 - 194.

Автор _____ Чапасов П. К.

Научный руководитель _____ Голованов А. А.