МАТЕМАТИЧЕСКИЕ ВОПРОСЫ КРИПТОГРАФИИ
2017 Т. 8 № 1 С. 7–12

УДК 519.719.2

Key agreement schemes based on linear groupoids [1]

A. V. Baryshnikov, S. Yu. Katyshev

Certification Research Center, LLC, Moscow

Получено 19.III.2016

Abstract. Authors present a study of the possibility to use special class of non-associative groupoids (called linear) for the implementation of a key exchange protocol based on a generalization of Diffie – Hellmann algorithm. The necessity to use the power commutation and effective power calculation properties is proved. A specific example of linear groupoid over the elliptic curve is described.

Keywords: key exchange protocol, Diffie – Hellmann algorithm, non-associative groupoids, linear quasigroups, elliptic curves

Схемы выработки общего ключа на основе линейных группоидов

А. В. Барышников, С. Ю. Катышев

ООО «Центр сертификационных исследований», Москва

Аннотация. Исследуется возможность использования одного класса неассоциативных группоидов (так называемых линейных группоидов) для реализации схемы выработки общего ключа, основанной на обобщении алгоритма Диффи – Хеллмана. Доказана необходимость использования коммутативности степеней и свойств эффективного вычисления степеней. Описан конкретный пример линейного группоида над группой точек эллиптической кривой.

Ключевые слова: протокол выработки общего ключа, алгоритм Диффи – Хеллмана, неассоциативные группоиды, линейные квазигруппы, эллиптические кривые.

Citation: *Mathematical Aspects of Cryptography*, 2017, v. 8, № 1, pp. 7–12 (Russian)

[1] The article was submitted by the Organizing Committee of the Symposium CTCrypt'2016.

Список литературы

[1] Katyshev S. Yu., Markov V. T., Nechaev A. A., “Application of non-associative groupoids to the realization of an open key distribution procedure”, *Дискретная математика*, **26**:3 (2014), 45–64 (in Russian); Engl. transl., *Discrete Math. Appl.*, **25**:1 (2015), 9–24.

[2] Belyavskaya G. B., Tabarov A. Kh., “Identities with permutations leading to linearity of quasigroups”, *Дискретная математика*, **21**:1 (2009), 36–51 (in Russian); Engl. transl., *Discrete Math. Appl.*, **19**:2 (2009), 173–190.

[3] Diffie W., Hellman M. E., “New directions in cryptography”, *IEEE Trans. Inf. Theory*, **22**:6 (1976), 644-654.

[4] Hellman M., “A cryptanalytic time-memory trade-off”, *IEEE Trans. Inf. Theory*, **26**:4 (1980), 401–406.

[5] Silverman J., *The Arithmetic of the Elliptic Curves*, Heidelberg etc.: Springer, 1986.