zbMATH Open
THE FIRST RESOURCE FOR MATHEMATICS

Kotov, Matvei; **Ushakov, Alexander**

Analysis of a key exchange protocol based on tropical matrix algebra. (English)

Zbl 1397.94082
J. Math. Cryptol. 12, No. 3, 137-141 (2018).

Summary: In this paper, we consider a two party key-exchange protocol proposed in [*D. Grigoriev* and *V. Shpilrain*, Commun. Algebra 42, No. 6, 2624–2632 (2014; Zbl 1301.94114), Section 2], which uses tropical matrix algebra as the platform. Our analysis shows that the scheme is not secure.

MSC:

94A60 Cryptography
68W30 Symbolic computation and algebraic computation
15A80 Max-plus and related algebras

Cited in **2** Reviews
Cited in **2** Documents

Keywords:

tropical algebra; cryptography; key-exchange; min-plus systems

Software:

GAP

Full Text: DOI

References:

[1] P. Butkovič, Max-linear Systems: Theory and Algorithms, Springer Monogr. Math., Springer, London, 2010. · Zbl 1202.15032

[2] T. H. Cormen, C. E. Leiserson, R. L. Rivest and C. Stein, Introduction to Algorithms, 3rd ed., MIT Press, Cambridge, MA, 2009. · Zbl 1187.68679

[3] D. Grigoriev and V. Shpilrain, Tropical cryptography, Comm. Algebra 42 (2014), no. 6, 2624-2632. · Zbl 1301.94114

[4] M. Kotov and A. Ushakov, Implementation of FBA, available at .

[5] C. Mullan, Cryptanalysing variants of Stickel's key agreement scheme, J. Math. Cryptol. 4 (2011), no. 4, 365-373. · Zbl 1211.94033

[6] A. Myasnikov, V. Shpilrain And A. Ushakov, Non-Commutative Cryptography and Complexity of Group-Theoretic Problems, Math. Surveys Monogr. 177, American Mathematical Society, Providence, 2011, · Zbl 1248.94006

[7] V. Shpilrain, Cryptanalysis of Stickel's key exchange scheme, Computer Science in Russia - CSR 2008, Lecture Notes in Comput. Sci. 5010, Springer, Berlin (2008), 283-288. · Zbl 1142.94360

[8] The GAP Group, \textit{GAP - Groups, Algorithms, and Programming, Version 4.7.7}, 2015, .

This reference list is based on information provided by the publisher or from digital mathematics libraries. Its items are heuristically matched to zbMATH identifiers and may contain data conversion errors. It attempts to reflect the references listed in the original paper as accurately as possible without claiming the completeness or perfect precision of the matching.

© 2021 FIZ Karlsruhe GmbH