Cryptology ePrint Archive: Report 2011/073

Cryptanalysis of three matrix-based key establishment protocols

Simon R. Blackburn, Carlos Cid and Ciaran Mullan

Abstract: We cryptanalyse a matrix-based key transport protocol due to Baumslag, Camps, Fine, Rosenberger and Xu from 2006. We also cryptanalyse two recently proposed matrix-based key agreement protocols, due to Habeeb, Kahrobaei and Shpilrain, and due to Romanczuk and Ustimenko.

Category / Keywords: public-key cryptography /

Date: received 11 Feb 2011

Contact author: s blackburn at rhul ac uk