Cryptology ePrint Archive: Report 2011/572

The ElGamal cryptosystem over circulant matrices

Ayan Mahalanobis

Abstract: Can one use the discrete logarithm problem in matrix groups, to build a better and secure cryptosystem? We argue, it is indeed the case. This makes the group of circulant matrices suitable and attractive for lightweight cryptography.

Category / Keywords: public-key cryptography /

Date: received 21 Oct 2011

Contact author: ayanm at iiserpune ac in