1092-94-127

jintai ding* (jintai.ding@gmail.com) and **Chengdong Tao** (chengdongtao2010@gmail.com).

Simple Matrix Scheme for Encryption.

There are many attempts to build asymmetric pubic key encryption schemes based on multivariate polynomials of degree two over a finite field. However, most of them are insecure. The common defect comes from the fact that certain quadratic forms associated with their central maps have low rank, which makes them vulnerable to the MinRank attack. We propose a new simple and efficient multivariate pubic key encryption scheme based on matrix multiplication, which does not have such a low rank property. The new scheme will be called Simple Matrix Scheme or ABC in short. We also propose some parameters for practical and secure implementation. (Received August 06, 2013)