Mohamed, Mohamed Saied Emam; Ding, Jintai; Buchmann, Johannes; Werner, Fabian

**Algebraic attack on the MQQ public key cryptosystem.** (English) [Zbl 1287.94087]


Summary: In this paper, we present an efficient attack on the multivariate Quadratic Quasigroups (MQQ) public key cryptosystem. Our cryptanalysis breaks the MQQ cryptosystem by solving a system of multivariate quadratic polynomial equations using both the MutantXL algorithm and the $F_4$ algorithm. We present the experimental results that show that MQQ systems is broken up to size $n$ equal to 300. Based on these results we show also that MutantXL solves MQQ systems with much less memory than the $F_4$ algorithm implemented in Magma.

For the entire collection see [Zbl 1176.94003].

**MSC:**

- 94A60 Cryptography

**Keywords:**

- Algebraic Cryptanalysis; MQQ public key cryptosystem; MutantXL algorithm; $F_4$ algorithm

**Software:**

- Magma

**Full Text:** DOI

Cited in 1 Review
Cited in 1 Document

© 2021 FIZ Karlsruhe GmbH