Cryptology ePrint Archive: Report 2011/275

Inverting Square systems algebraically is exponential

Jintai Ding

Abstract: In this paper, we prove that the degree of regularity of the family of Square systems, an HFE type of systems, over a prime finite field of odd characteristics q is exactly q, and therefore prove that \vskip .1in \begin{itemize} \item inverting Square systems algebraically is exponential, when $q=O(n)$, where n is the number of variables of the system. \end{itemize}

Category / Keywords: foundations / Square, HFE, degree of regularity

Date: received 28 May 2011

Contact author: jintai ding at gmail com

Available formats: PDF | BibTeX Citation

Version: 20110528:182125 (All versions of this report)

Discussion forum: Show discussion | Start new discussion