Cryptology ePrint Archive: Report 2011/570

Degree of regularity for HFE-

Jintai Ding and Thorsten Kleinjung

Abstract: In this paper, we prove a closed formula for the degree of regularity of the family of HFE- (HFE Minus) multivariate public key cryptosystems over a finite field of size q. The degree of regularity of the polynomial system derived from an HFE- system is less than or equal to

\begin{eqnarray*} \frac{(q-1)(\lfloor \log_q(D-1)\rfloor +a)}2 +2 & & \text{if q is even and $r+a$ is odd,} \\ \frac{(q-1)(\lfloor \log_q(D-1)\rfloor+a+1)}2 +2 & & \text{otherwise.} \end{eqnarray*}

Here q is the base field size, D the degree of the HFE polynomial, $r=\lfloor \log_q(D-1)\rfloor +1$ and a is the number of removed equations (Minus number).

This allows us to present an estimate of the complexity of breaking the HFE

Challenge 2: \vskip .1in \begin{itemize} \item the complexity to break the HFE Challenge 2 directly using algebraic solvers is about 2^{96}. \end{itemize}

Category / Keywords: public-key cryptography / multivariate, degree of regularity

Date: received 21 Oct 2011

Contact author: jintai ding at gmail com