Cryptology ePrint Archive: Report 2013/041

Trace Expression of r-th Root over Finite Field

Gook Hwa Cho and Namhun Koo and Eunhye Ha and Soonhak Kwon

Abstract: Efficient computation of r-th root in $\mathbb F_q$ has many applications in computational number theory and many other related areas. We present a new r-th root formula which generalizes M\"{u}ller's result on square root, and which provides a possible improvement of the Cipolla-Lehmer algorithm for general case. More precisely, for given r-th power $c\in \mathbb F_q$, we show that there exists $\alpha \in \mathbb F_{q^r}$ such that $Tr\left(\alpha^\frac{(\sum_{i=0}^{r-1}q^i)-r}{r^2}\right)^r=c$ where $Tr(\alpha)=\alpha+\alpha^q+\alpha^{q^2}+\cdots +\alpha^{q^{r-1}}$ and α is a root of certain irreducible polynomial of degree r over $\mathbb F_q$.

Category / Keywords: applications / finite field, r-th root, linear recurrence relation, Tonelli-Shanks algorithm, Adleman-Manders-Miller algorithm, Cipolla-Lehmer algorithm

Date: received 26 Jan 2013, last revised 30 Jan 2013

Contact author: shkwon7 at gmail com