Cryptology ePrint Archive: Report 2013/024

New Cube Root Algorithm Based on Third Order Linear Recurrence Relation in Finite Field

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

Abstract: In this paper, we present a new cube root algorithm in finite field $\mathbb{F}_{q}$ with q a power of prime, which extends the Cipolla-Lehmer type algorithms \cite{Cip,Leh}. Our cube root method is inspired by the work of M\"{u}ller \cite{Muller} on quadratic case. For given cubic residue $c \in \mathbb{F}_{q}$ with $q \equiv 1 \pmod{9}$, we show that there is an irreducible polynomial $f(x)=x^{3}-ax^{2}+bx-1$ with root $\alpha \in \mathbb{F}_{q^{3}}$ such that $Tr(\alpha^{\frac{q^{2}+q-2}{9}})$ is a cube root of c. Consequently we find an efficient cube root algorithm based on third order linear recurrence sequence arising from $f(x)$. Complexity estimation shows that our algorithm is better than previously proposed Cipolla-Lehmer type algorithms.

Category / Keywords: applications / cube root algorithm, Cipolla-Lehmer algorithm

Date: received 16 Jan 2013

Contact author: shkwon at skku edu

Available formats: PDF | BibTeX Citation

Version: 20130124:195739 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]