Cryptology ePrint Archive: Report 2013/117

On r-th Root Extraction Algorithm in F_q For q=lr^s+1 (mod r^(s+1)) with 0 < l < r and Small s

Namhun Koo and Gook Hwa Cho and Soonhak Kwon

Abstract: We present an r-th root extraction algorithm over a finite field F_q. Our algorithm precomputes a primitive r^s-th root of unity where s is the largest positive integer satisfying r^s| q-1, and is applicable for the cases when s is small. The proposed algorithm requires one exponentiation for the r-th root computation and is favorably compared to the existing algorithms.

Category / Keywords: applications / r-th root algorithm, finite field, Adleman-Manders-Miller algorithm, Cipolla-Lehmer algorithm

Date: received 25 Feb 2013

Contact author: shkwon7 at gmail com

Available formats: PDF | BibTeX Citation

Version: 20130227:180513 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]