Cryptology ePrint Archive: Report 2011/378

A generalization of the Lucas addition chains

Amadou TALL

Abstract: In this paper, we give a generalization of Lucas addition chains, where subtraction is allowed. We call them "Lucas addition-subtraction chain". We also show that this new method gives minimal addition-subtraction chains for infinitely many integers. This new method will also be used to prove that Lucas addition chains are optimal for many integers. Moreover, we show that Lucas addition chains give minimal addition chains for all integers of Hamming weight 3, like the \emph{binary method}. Finally, we give a theorem to get short (and many times minimal) Lucas addition-subtraction chains.

Category / Keywords: public-key cryptography / addition chain; addition-subtraction chain; Lucas chains;

Publication Info: Addition chains, exponentiation

Date: received 11 Jul 2011, last revised 24 Jul 2011

Contact author: tallamad at hotmail com