Cryptology ePrint Archive: Report 2011/318

Scalar Multiplication on Koblitz Curves using τ^2-NAF

Sujoy Sinha Roy and Chester Rebeiro and Debdeep Mukhopadhyay and Junko Takahashi and Toshinori Fukunaga

Abstract: The paper proposes a τ^2-NAF method for scalar multiplication on Koblitz curves, which requires asymptotically $0.215m$ point additions in $GF(2^m)$. For τ^2-NAF method, point quading operation $(a\rightarrow a^4)$ is performed instead of point squarings. The proposed method is faster than normal $\tau-$NAF method, which requires around $\frac{m}{3}$ point additions. However, like width w based $\tau-$NAF methods, there is an overhead of pre-computations in the τ^2-NAF method. For extended binary fields of small size, the τ^2-NAF based scalar multiplication requires almost same number of point additions as in width 4 $\tau-$NAF method. Though, complexity wise, τ^2-NAF based scalar multiplication and width $4-\tau-$NAF based scalar multiplication are similar, but the techniques are different.

Category / Keywords: implementation / Koblitz curve, elliptic curve, scalar multiplication, tau^2 NAF

Date: received 15 Jun 2011

Contact author: sujoyetc at cse iitkgp ernet in, chester@cse iitkgp ernet in, debdeep@cse iitkgp ernet in, takahashi junko@lab ntt co jp, toshi fukunaga@hco ntt co jp