Efficient Optimal Ate Pairing at 128-bit Security Level

Loubna Ghammam,
Greyc Université de Caen Normandie

Abstract :

Following the emergence of Kim and Barbulescu's new number field sieve (exTNFS) algorithm at CRYPTO'16 for solving discrete logarithm problem (DLP) over the finite field; pairing-based cryptography researchers are intrigued to find new parameters that confirm standard security levels against exTNFS.
Recently, Barbulescu and Duquesne have suggested new parameters for well-studied pairing-friendly curves i.e., Barreto-Naehrig (BN), Barreto-Lynn-Scott (BLS-12) and Kachisa-Schaefer-Scott (KSS-16) curves at 128-bit security level (twist and sub-group attack secure). They have also concluded that in the context of Optimal-Ate pairing with their suggested parameters, BLS-12 and KSS-16 curves are more efficient choices than BN curves.
Therefore, this paper selects the atypical and less studied pairing-friendly curve in literature, i.e., KSS-16 which offers quartic twist, while BN and BLS-12 curves have sextic twist.

In this work, we optimize Miller's algorithm of Optimal-Ate pairing for the KSS-16 curve by deriving efficient sparse multiplication and implement them.
The result shows that Miller's algorithm time with the derived pseudo 8-sparse multiplication is the most efficient for KSS-16 than other two curves.