Subgroup membership testing on elliptic curves via the Tate pairing

Journal of Cryptographic Engineering (2022)

This note explains how to guarantee the membership of a point in the prime-order subgroup of an elliptic curve (over a finite field) satisfying some moderate conditions. For this purpose, we apply the Tate pairing on the curve; however, it is not required to be pairing-friendly. Whenever the cofactor is small, the new subgroup test is much more efficient than other known ones, because it needs to compute at most two n

-th power residue symbols (with small n

) in the basic field. More precisely, the running time of the test is (sub-)quadratic in the bit length of the field size, which is comparable with the Decaf-style technique. The test is relevant, e.g., for the zk-SNARK friendly curves Bandersnatch and Jubjub proposed by the Ethereum and Zcash research teams, respectively.