

既
 存研究と提案手法提案手法のアルゴリズム
 BKLS
 Algorithm,
 Window
 Miller
 Algorithm
 を組み合わせること
 で新しい高速化手法を提案する。以下にそのアルゴリズムを示す。

[htbp]

Input: $n, P, Q \in E(F_q)[n]$
 Output: $f \in F_{q^k}$
 (online computation)
 1: $P_1 = P, f'_1 = 1$
 2: for $i \leftarrow 2$ up to $2^w - 1$
 3: $P_i \leftarrow P + P_{i-1}$
 4: $f'_i \leftarrow f'_{i-1} \cdot g_{P_i, P}(\psi(Q))$
 (main computation)
 5: $V \leftarrow P, f \leftarrow 1$