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 do $2^w - 1$
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: $V \leftarrow P, f \leftarrow 1$

提案手法の計算量 Miller Algorithm, Window Miller Algorithm, BKLS Algorithm, 提案したアルゴリズムの計算量を比較する。

Miller のアルゴリズムにおける演算部分のステップを加算 (TADD), 減算 (TSUB), 2 倍算 (TDBL) に分ける.