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: $V \leftarrow P, f \leftarrow 1$
6: $n = \sum_{i=0}^{l-1} n_i 2^i,\ n_i \in \{0, 1\},\ n_0 = 1$
7: for $n - 1 \leftarrow i$ down to 0 step w
8: step 8-1 から 8-2 を w 回繰り返す
8-1: $V \leftarrow 2V$
8-2: $f \leftarrow f^2 \cdot g_{V,\ V}(\psi(Q))$

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

Miller Algorithm における演算部分のステップを加算 (TADD), 2 倍算 (TDBL), BKLS Algoritm における