Distorsion Map の n-進展開を用いた Miller Algorithm の高速化に関する研究

Fast Computation of Miller Algorithm with n-adic expansion of Distortion maps

15D8101012B　増渕 佳輝
中央大学理工学部情報工学科 趙研究室
2019 年 3 月

要約　本研究ではペアリング暗号の演算で使用する Miller Algorithm に distortion map を用いた BKLS Algorihtm と Window 法を組み合わせることで, 高速化を行った.

キーワード　ペアリング暗号, Tate ペアリング, Miller Algorithm, BKLS Algorithm,

1　序論

楕円曲線暗号とは有限体上の楕円曲線を用いた暗号で, これに対する攻撃方法としてペアリングが用いられた． その後, ペアリングを用いた暗号である ID ベース暗号への応用などに使われ, 近年では，ペアリングを用いたプロトコルが数多く提案されている．楕円曲線上のペアリングとして, Weil ペアリングや Tate ペアリングがあるが, 通常の楕円演算に比べて演算量が多く, ペアリング計算の高速化が課題となっている.

本研究ではペアリング暗号の演算で使用する Miller Algorithm に distortion map を用いることで改良した BKLS Algorihtm に,Window 法を適用し Tate ペアリングの高速化を行い, 計算コストと計算時間の比較を行った.

2　楕円曲線の定義

楕円曲線とは, 一般的に

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

で与えられる．素数 p, 有限体 F_q $(q = p^m)$ 上の楕円曲線とは, この方程式を満たす有理点 (x, y) に無限遠点 $\mathcal{O}$ を加えた集合のことであり, $E(\mathbb{F}_q)$ と表す． また, 定義体 $\mathbb{F}_q$ の標数が 3 より大きい場合は変数変換により, $y^2 = x^3 + ax + b$ と一般化できる.

3　ペアリング

3.1　ペアリングの定義

n を整数とする．G_1, G_2 を単位元 0 の加法アーベル群とする．G_1, G_2 は位数 n を持つ．G_3 は単位元 1 の乗法に関する位数 n の巡回群とする．ペアリングというのは以下の関数である.

$$e : G_1 \times G_2 \longrightarrow G_3$$

ペアリングは以下の 2 つの性質を満たす。ことが知られている。

- 双線形性
  全ての $P, P' \in G_1$ と $Q, Q' \in G_2$ に対して,
  $$e(P + P', Q) = e(P, Q) + e(P', Q)$$
  $$e(P, Q + Q') = e(P, Q) + e(P, Q')$$
  が成り立つ.
- 非退縮性
  全ての $P \in G_1$ $(P \neq 0)$ に対して $e(P, Q) \neq 1$ となるような $Q \in G_2$ が存在する.
  全ての $Q \in G_2$ $(P \neq 0)$ に対して $e(P, Q) \neq 1$ となるような $P \in G_1$ が存在する.

3.2　Tate ペアリング

有限体 $\mathbb{F}_q$ 上の楕円曲線を $y^2 = x^3 + ax + b$ とし, 素数 n, 埋め込み次数 k を $n|q^k - 1$ を満たす最小の整数とする． 楕円曲線上の点 P, Q を $P \in E(\mathbb{F}_q)[n]$, $Q \in E(\mathbb{F}_{q^k})$ と定め, Tate ペアリングを次に定義する.

$$E(\mathbb{F}_q)[n] \times E(\mathbb{F}_{q^k})/nE(\mathbb{F}_{q^k}) \to \mathbb{F}^*_{q^k}/(\mathbb{F}^*_{q^k})^n$$

$$(P, Q) \mapsto \langle P, Q\rangle_n = f_{n,P}(D)$$

3.3　Reduced Tate ペアリング

Tate ペアリングの値は剰余類全体の集合 $\mathbb{F}^*_{q^k}/(\mathbb{F}^*_{q^k})^n$ に属しており,Tate ペアリングの値に $(q^k - 1)/n$ 乗することで, 一意な値を得られる． Reduced Tate ペアリングを次に定義する.

$$P \in E(\mathbb{F}_q)[n],\ Q \in E(\mathbb{F}_{q^k}),\ \mu_n = \left\{x \in \mathbb{F}^*_{q^k} | x^n = 1\right\}$$

$$\tau\langle P, Q\rangle = \langle P, Q\rangle_n^{(q^k-1)/n} = f_{n,P}(Q)^{(q^k-1)/n} \in \mu_n$$

3.4　Miller Algorithm

ペアリングの計算手法として Miller Algorithm がある． $\mathbb{F}_q$ 上の楕円曲線の Reduced Tate ペアリングにおける Miller Algorithm を次に示す． 点 U, $V \in E(\mathbb{F}_{q^k})$ を通る直線の方程式を $g_{U,V}$ とする。$U = V$ の場合 V を通る E の接線を表す。 Miller Algoritm は $f_{i+j} = \left(f_i f_j \frac{g_{iP,jP}}{g_{\mathcal{O},(i+j)P}}\right)$ で表される再帰公式を利用する.

Input: $n,\ l = \log n,\ P \in E(\mathbb{F}_q)[n],\ Q \in E(\mathbb{F}_{q^k})$
Output: $f \in \mathbb{F}_{q^k}$

1: $V \leftarrow P,\ f \leftarrow 1,\ n = \sum_{i=0}^{l-1} n_i 2^i,\ n_i \in \{0,1\}$
2: for $j \leftarrow l-1$ down to 0 do
3: $\quad f \leftarrow f^2 \cdot \frac{g_{V,V}(Q)}{g_{\mathcal{O},2V}(Q)}.\ V \leftarrow 2V$
4: if $n_j = 1$ then
5: $\quad f \leftarrow f \cdot \frac{g_{V,P}(Q)}{g_{V+P}(Q)},\ V \leftarrow V + P$
6: return f

3.5 BKLS Algorithm

supersingular curve の distortion map ψ を利用して分母消去の手法を適用した BKLS Algorithm [1] を次に示す. 体 K をある拡大体 $\mathbb{F}_{q^k}$ とする。ordinary curve の場合, $Q' \in E'(K)$ として, distortion map ではなく twist の同型写像 ψ_d を用いる.

Input: $P,\ Q \in E(\mathbb{F}_q)[n]$
Output: $f \in \mathbb{F}_{q^k}$

1: $f \leftarrow 1,\ V \leftarrow P$
2: $n = \sum_{l-1}^{i=0} n_i 2^i,\ n_i \in \{0,1\}$
3: for $j \leftarrow l-1$ down to 0 do
4: $\quad f \leftarrow f^2 \cdot g_{V,\ V}(\psi(Q))$
5: $\quad V \leftarrow 2V$
6: if $n_j = 1$ then
7: $\quad f \leftarrow f \cdot g_{V,\ P}(\psi(Q))$
8: $\quad V \leftarrow V + P$
9: return f

3.6 Window Miller Algorithm

Window Miller アルゴリズムは、オンライン事前演算 を用いる方法である。このアルゴリズムでは、n/w 回行うことになるため、適切な w を用いれば、楕円加算および直線 $g_{P,-P_i}$, 垂線 $g_{\mathcal{O},P_i}$ の計算を削減することができる。

Input: $n,\ P \in E(\mathbb{F}_q)[n],\ Q \in E(\mathbb{F}_{q^k})$
Output: $f \in \mathbb{F}_{q^k}$

(online computation)
1: $P_1 = P, f'_1 = 1$
2: for $i \leftarrow i$ up to do $2^w - 1$
3: $\quad P_i \leftarrow iP_i$
4: $\quad f \leftarrow f \cdot \frac{g_{P,-P_i}(S) g_{\mathcal{O},P_i}(Q+S)}{g_{P,-P_i}(S) g_{\mathcal{O},P_i}(Q+S)}$
(main computation)
5: $T \leftarrow P_i, f \leftarrow 1$
6: $n = \sum_{i=0}^{l-1} n_i 2^i,\ n_i \in \{0,1\}$
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: $\quad T \leftarrow 2T$
8-2: $\quad f \leftarrow f^2 \cdot \frac{g_{T,-2T}(Q+S) g_{\mathcal{O},2T}(S)}{g_{T,-2T}(Q+S) g_{\mathcal{O},2T}(S)}$
9: $n' \leftarrow = \sum_i^{j=i-w+1} n_j 2^{j-i+w-1}$
10: if $n' \neq 0$ then
10-1: $\quad T \leftarrow T + P_{n'}$
10-2: $\quad f \leftarrow f^2 \cdot \frac{g_{T,-2T}(Q+S) g_{\mathcal{O},2T}(S)}{g_{T,-2T}(Q+S g_{\mathcal{O},2T}(S)}$
11: return f

4 提案手法

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。

Input: $n,\ P, Q \in E(\mathbb{F}_q)[n]$
Output: $f \in \mathbb{F}_{q^k}$

(online computation)
1: $P_1 = P, f'_1 = 1$
2: for $i \leftarrow 2$ up to $2^w - 1$ do
3: $\quad P_i \leftarrow P + P_{i-1}$
4: $\quad f'_i \leftarrow f'_{i-1} \cdot g_{P_i,\ P}(\psi(Q))$
(main computation)
5: $V \leftarrow P, f \leftarrow 1$
6: $n = \sum_{i=0}^{l-1} n_i 2^i,\ n_i \in \{0,1\}$
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: $\quad V \leftarrow 2V$
8-2: $\quad f \leftarrow f^2 \cdot g_{V,\ V}(\psi(Q))$
9: $n' \leftarrow = \sum_i^{j=i-w+1} n_j 2^{j-i+w-1}$
10: if $n' \neq 0$ then
10-1: $\quad f \leftarrow f f'_m \cdot g_{V,\ P_m}(\psi(Q))$
10-2: $\quad V \leftarrow V + P_{n'}$
11: return f

5 評価

ペアリングで使用する 2 つの点の位数 n のビット列 l が長いほど高速化できる割合は大きくなった。例として、l が 80 より 160 の場合に 9.7% 高速化することができた。また, 埋め込み次数 k が大きいほど高速化できる割合は小さくなることが分かった。例として以下に、$k = 6, l = \log_2(n) = 160,\ w = 4$ の場合の計算量を示す。M を乗算の演算量とする。

$k = 6, l = 160,\ w = 4$	計算コスト
Miller Algorihtm	$58080M$
Window Miller Algorithm	$53036M$
BKLS Algorithm	$21840M$
提案手法	$20098M$

6 今後の課題

今後の課題としては, 既存の Signed Miller Algorithm や, 3 倍算の計算コストが乗算よりも小さいことを利用した標数 3 の有限体における Miller Algorithm に distortion map を適用した手法に今回の提案に使用した Window Miller Algorithm を組み合わせるなどが考えられる。また、今回の手法を適用するのに適した楕円曲線を探すなどが挙げられる。

謝辞

本研究において, あらゆる面でご指導していただいた趙晋輝教授並びに諸先輩方, 趙研究室の皆様にも深く感謝いたします.

参考文献

[1] P. S. L. M. Barreto, H. Y. Kim, B. Lynn, and M. Scott: *Efficient implementation of pairing-based cryptosystem*, Journal of Cryptology, 17(4):321-334, 2004.

[2] 小林 鉄太郎, 斉藤 泰一, 今井 秀樹: "Pairing 演算の高速化 Fast Computation of Pairing" The 2004 Symposium on Cryptography and Information Security Sendai, Japan, Jan. 27-30, 2004

[3] 大川一樹 :Double-Base Chains を用いたペアリング 暗号における Tate ペアリングの高速化に関する考察