

BLS12 曲線上のペアリングにおける $\mathbb{G}_2$ 上の有理点生成の高速化

Fast Generating Rational Points on $\mathbb{G}_2$ for Pairing on BLS12

飯田 智宏* 服部 大地* 松村 陸矢* 南條 由紀* 小寺 雄太*
Tomohiro Iida Daichi Hattori Rikuya Matsumura Yuki Nanjo Yuta Kodera
日下 卓也* 野上 保之*
Takuya Kusaka Yasuyuki Nogami

キーワード ペアリング暗号, BLS 曲線, 混合座標系

近年, ペアリング暗号は様々な高機能暗号を実現できると注目されている. ペアリング暗号には, 楕円曲線上の有理点群 $\mathbb{G}_1$, $\mathbb{G}_2$ と拡大体における乗法群 $\mathbb{G}_3$ に対して, $e: \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_3$ で定義されるペアリング写像が用いられる. ペアリング写像のもつ双線型性により ID ベース暗号などの高機能暗号を実現することができる. ID ベース暗号を用いると, 識別情報である ID 情報を公開鍵として使用することが可能であり, 鍵管理を簡単に行うことが可能となる. ペアリング暗号を利用した ID ベース暗号では, ID 情報を $\mathbb{G}_1$ もしくは $\mathbb{G}_2$ 上の有理点にハッシュする必要がある. $\mathbb{G}_1$, $\mathbb{G}_2$ 上の有理点の生成は, 楕円曲線上のランダムな点 P に対してある整数 c によるスカラー倍算 $[c]P$ を計算することにより実現できる. 中でも, $\mathbb{G}_2$ 上の有理点を生成するためのスカラー倍算の計算量は大きいため, 高速に計算するための手法が必要である.

楕円曲線が曲線族により与えられている場合においては, スカラー倍算の計算量を削減する手法 [1], [2] が提案されている. これらの手法では, c がある整数 x による多項式により表現できることを利用している. c の多項式を適切に分解すると, Skew Frobenius 写像と呼ばれる計算コストの低い写像を利用することができ, $[c]P$ を効率的に計算することができる. BLS12 曲線に対して手法 [3] を適用した場合, $\mathbb{G}_2$ 上の有理点生成のためのスカラー倍算は, 有理点に対する 2 回の x のスカラー倍算, 5 回の加算, 1 回の二倍算, 3 回の Skew Frobenius 写像により実行することができる.

$\mathbb{G}_2$ 上の有理点をより高速に生成するために, 本研究では 2 回の x のスカラー倍算に対して, Jacobian 座標系と Affine 座標系を組み合わせた混合座標系を用いる実装を提案する. 具体的に, 2 回の x のスカラー倍算の計算に対して, (a) すべて Jacobian 座標系を用いる場合, (b) 1 回目に混合座標系, 2 回目に Jacobian 座標系を用いる場合, (c) すべて混合座標系を用いる場合における $\mathbb{F}_p$ 上の計算コストを検証する. その結果, 本研究の実験環境においては, (a), (b), (c) の場合における加算を 1 としたときの計算コストは, それぞれ 46220, 45884, 45891 であることが確認できた. よって, 高速に $\mathbb{G}_2$ 上の有理点を生成するためには, (b) 1 回目に混合座標系, 2 回目に Jacobian 座標系を用いることが推奨されると結論づけた.

参考文献

- [1] Michael Scott et al. "Fast hashing to $\mathbb{G}_2$ on pairing friendly curves". In: International Conference on Pairing-Based Cryptography. Springer. 2009, pp. 102-113.
- [2] Laura Fuentes-Castañeda, Edward Knapp, and Francisco Rodríguez-Henríquez. "Faster Hashing to $\mathbb{G}_2$ ". In: International workshop on selected areas in cryptography. Springer. 2011, pp. 412-430.
- [3] Alessandro Budroni and Federico Pintore. "Efficient hash maps $\mathbb{G}_2$ on BLS curves". In: Applicable Algebra in Engineering, Communication and Computing (2020), pp. 1-21.

* 岡山大学大学院自然科学研究科, 岡山県岡山市北区津島中 1 丁目 1 番 1 号, Graduate School of Natural Science and Technology, Okayama University, 1-1-1, Tsushimanaka, Okayama, Okayama, Japan