Copyright ©2022 The Institute of Electronics,
Information and Communication Engineers

SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

ペアリング高速計算に適した楕円曲線における群所属判定
A Note on Group Membership Check in Elliptic Curves for Pairings

安田 貴徳 * 石井 将大 † 照屋 唯紀 ‡
Takanori Yasuda Masahiro Ishii Tadanori Teruya

キーワード ペアリング，楕円曲線，群所属判定問題，自己準同型環

あらまし

ペアリングに基づく多くの暗号プロトコルは，位数が十分に大きい素数の有理点部分群における離散対数問題の計算困難性に基づき，暗号学的な安全性が証明される暗号技術である．このような暗号技術の実装は，その処理で取り扱う群の値が実際にその有理点部分群に所属する単位元以外の非自明な値であることを保証しなければならない．これが保証されない場合，その暗号学的な安全性は成立せず，何らかの攻撃法が適用可能となる恐れがある．この保証を行う一般的な方法として，群所属判定や cofactor clearing などがある．本稿では群所属判定に注目し，その背景理論を整理する．そして，pairing-friendly 曲線などペアリング高速計算に適した楕円曲線について，ペアリングの入出力群の自己準同型環，特に自己同型写像と Frobenius 写像を利用し，適切な部分群に所属していることを判定できる，効率的に計算可能な群所属判定方法を提案する．

* 岡山理科大学, 岡山県岡山市北区理大町 1-1, Okayama University of Science, 1-1 Ridai-cho, Kita-ku, Okayama city, Okayama pref.
† 東京工業大学, 東京都目黒区大岡山 2-12-1, Tokyo Institute of Technology, 2-12-1 Ookayama, Meguro-ku, Tokyo
‡ 産業技術総合研究所, 東京都江東区青海 2-3-26, National Institute of Advanced Industrial Science and Technology, 2-3-26 Aomi, Koto-ku, Tokyo