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

F_4-style アルゴリズムの MQ 問題に対する多項式選択方法
Polynomial selections on an F_4-style algorithm for solving the MQ problem

伊藤 琢真 *† 黒川 貴司 * 篠原 直行 * 内山 成憲 †
Takuma Ito Takashi Kurokawa Naoyuki Shinohara Shigenori Uchiyama

キーワード 多変数多項式, 多変数公開鍵暗号, Gröbner 基底, MQ 問題, F_4 アルゴリズム

あらまし

連立二次多変数代数方程式の解を見つける問題は MQ 問題と呼ばれており, MQ 問題は耐量子計算機暗号の候補である多変数公開鍵暗号 (MPKC) の安全性の根拠として利用されており, MPKC の安全性評価の研究において重要な課題として扱われている.

MQ 問題を効率よく解く方法として Gröbner 基底を計算するアルゴリズムが挙げられ，その代表的なアルゴリズムとして F_4-style アルゴリズム [1] が知られている. F_4-style アルゴリズム による計算では有限体係数の多項式環における多項式の剰余算 (reduction) が多用され，reduction に使用する多項式の選択はその計算の効率性に大きな影響を与える. 例えば Gröbner 基底の計算に必要な S 多項式を計算するとき, S 多項式の全次数が小さくなるように多項式を選択していくと計算の効率が良くなることが知られているが, 一方でこの選択方法よりも効率的な手法や事例が見つかっている.

本稿の貢献: 本稿では，様々な多項式選択法を F_4-style アルゴリズムに導入し，MQ 問題を解いた場合に最も効率の良い多項式選択法を提案する. 結果としては [2] にて用いられている second monomial を指標とした方法を基にした選び方が最も効果があるということが数値実験により得られた.

* 国立研究開発法人情報通信研究機構, 〒 184-8795 東京都小金井市貫井北町 4-2-1, NICT, 4-2-1, Nukui-Kitamachi, Koganei, Tokyo 184-8795, Japan
† 東京都立大学, 〒 192-0397 東京都八王子市南大沢 1-1, Tokyo Metropolitan University, 1-1 Minami-Osawa, Hachioji-shi, Tokyo, 192-0397, Japan

参考文献

[1] Jean-Charles Faugère. A new efficient algorithm for computing gröbner bases (F_4). *Journal of Pure and Applied Algebra*, Vol. 139, No. 1-3, pp. 61–88, 1999.

[2] Takuma Ito, Atsushi Nitta, Yuta Hoshi, Naoyuki Shinohara, and Shigenori Uchiyama. Polynomial selection for computing grobner bases. *JSIAM Letters*, Vol. 13, pp. 72–75, 2021.