学位論文要旨（博士（理学））

論文著者名　伊藤 琢真

論文題名： An Efficient Algorithm for Computing Gröbner Bases to Solve the MQ Problem
（邦題）：MQ 問題を解くための効率的なグレブナ基底計算アルゴリズム(英文)

本論文では Gröbner 基底の計算を利用した MQ 問題の求解方法について論じる．そこで MQ 問題の求解の必要性と Gröbner 基底の関連性について述べる．
近年，量子コンピュータの開発が活発になっており，実用的な量子コンピュータの実現は暗号の分野にとって大きな影響を与える．現在使用されている公開鍵暗号として有名な RSA 暗号と楕円曲線暗号はそれぞれ巨大整数の素因数分解問題と離散対数問題を安全性として利用しているが，これらの問題は量子コンピュータにより効率よく解かれてしまうことが知られているため，これらの暗号の安全性が低下してしまうことが危惧されている．そのため量子コンピュータでも解読が困難な暗号(PQC)の研究が行われるようになった．

PQC の候補の中に多変数多項式を利用した暗号である多変数公開鍵暗号(MPKC)がある．ここで有限体上の連立多変数代数方程式の解を見つける問題は MP 問題と呼ばれており，特に多項式の全次数が 2 に限るものは MQ 問題と呼ばれる．Rainbow [1]や GeMSS [2]などの多くの MPKC の安全性は MQ 問題を解くことの困難性を利用している．MQ 問題の困難性を調査するために Fukuoka MQ Challenge [3] という国際コンテストが 2015 年から開かれており，そこでは MPKC の安全性に関連する MQ 問題が用意されている．例えば $\mathbb{F}_{256}$ 上の n 変数 m 多項式 $(m = 2n)$ から成る MQ 問題が n の大きさ毎に用意されている．このように MQ Challenge の問題を解くことを含め，MQ 問題を効率よく解くことは MPKC において重要な研究課題となっている．

MQ 問題を解く手法として Gröbner 基底の計算が挙げられる．Gröbner 基底という考え方は 1965 年に Buchberger により提唱されたものである．Gröbner 基底を計算する代表的なアルゴリズムには Faugère が 1999 年に提案したF_4 [4], Makarim らが 2017 年に提案した M4GB [5] などがある．これらのアルゴリズムは MQ Challenge の問題を解くことにも成功しており，計算効率の良いアルゴリズムであることが知られている．一方で Gröbner 基底の計算では計算の際にどの多項式から剰余算(reduction)をしていくのかといった部分が計算効率に影響を与えるが，計算効率が良くなるような多項式の選び方などについては改善の余地があることも知られている．

本稿の貢献:

本稿では Gröbner 基底を計算するアルゴリズムであるF_4-style アルゴリズムを基に，次の手法を導入する．

- Gröbner 基底の計算の途中で n 個の線形独立な多項式を得られたら計算を止める．

- zero-reduction されてしまう可能性の高いペアを省く.
- S 多項式を生成するためのペアの選び方で新しい方法を導入する.

MQ 問題を解くことにおいて, これらの方法を取り入れたアルゴリズムと M4GB を比較した結果, 計算に必要な時間(CPU 時間)とメモリの最大使用量の両方の面において M4GB よりも改善されているという実験結果が得られた. また Fukuoka MQ Challenge の Type II に分類される問題($\mathbb{F}_{256}$ 上のn 変数 $2n$ 多項式で構成される MQ 問題)で, 37 変数のときの問題を解くことに成功し, この結果は 2022 年 1 月 28 日現在も世界記録として残されている.

参考文献

[1] Jintai Ding and Dieter Schmidt. Rainbow, a New Multivariable Polynomial Signature Scheme. In Applied Cryptography and Network Security, Third International Conference, ACNS 2005, New York, NY, USA, June 7-10, 2005, Proceedings, pages 164–175, 2005.

[2] A. Casanova, Jean-Charles Faug`ere, G. Macario-Rat, J. Patarin,L. Perret, and J. Ryckeghem. GeMSS: A Great Multivariate Short Signature. https://www-polsys.lip6.fr/Links/NIST/GeMSS_specification.pdf.

[3] Takanori Yasuda, Xavier Dahan, Yun-Ju Huang, Tsuyoshi Takagi, and Kouichi Sakurai. MQ challenge: Hardness Evaluation of Solving Multivariate Quadratic Problems. IACR Cryptology ePrint Archive, 2015:275, 2015.

[4] Jean-Charles Faugère. A New Efficient Algorithm for Computing Gröbner Bases (F_4). Journal of Pure and Applied Algebra, 139(1-3):61–88, 1999.

[5] Rusydi H. Makarim and Marc Stevens. M4GB: An Efficient Gröbner-Basis Algorithm. In Proceedings of the 2017 ACM on International Symposium on Symbolic and Algebraic Computation, ISSAC 2017, Kaiserslautern, Germany, July 25-28, 2017, pages 293–300, 2017.