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

MQ 問題の解決のための Hybrid approach の改良の検討
Development of hybrid approach for solving MQ problem

坂田 康亮 *
Kosuke Sakata

キーワード 耐量子計算機暗号/MQ 問題/Gröbner 基底/Hybrid approach

あらまし

公開鍵暗号は，現代の情報通信システムの安全性を支える重要な技術であり，RSA 暗号や楕円曲線暗号などが使用されている．しかし，実用的な量子コンピュータが開発されると，Shor のアルゴリズム [4] によって，現在使用されている公開鍵暗号の数学的な問題は多項式時間で解くことが可能であるため，公開鍵暗号の安全性が著しく低下することが問題となっている．そのため，量子コンピュータでも解読が困難な暗号である耐量子計算機暗号の研究が進められている．

米国立標準技術研究所 (NIST) は耐量子計算機暗号の標準化プロジェクトにおいて，次世代暗号の候補を公募し，検討を進めている．多変数多項式公開鍵暗号は現在，次世代暗号の最終候補として残っている暗号方式の一つである．連立二次多変数代数方程式の求解 (MQ 問題) は多変数多項式公開鍵暗号の安全性根拠となっており，その計算困難性を評価することは重要な研究課題である．MQ 問題を解く有力な方法の一つとして Gröbner 基底を求める方法があり，その場合には F4[2]，F5[3] などのアルゴリズムが用いられる．MQ 問題の変数の数 n が多項式の数 m と同じ，もしくは大きい場合には，hybrid approach[1] を用いることで効率的に解けることが知られている．Hybrid approach は有限体上の連立多変数代数方程式の解法の一つで，全探索法 (exhaustive search) と Gröbner 基底を計算する方法を合わせた方法である．まず，いくつかの変数に代入を行い，$n < m$ となった MQ 問題の Gröbner 基底を求める方法であり，$n \geq m$ となっている MQ 問題を解く場合に有効な方法である．

この発表では，Hybrid approach における代入計算を行う前に，あらかじめ Gröbner 基底計算を途中まで進めてから代入計算を行い，さらにその後に Gröbner 基底計算を進める手法について検討したので報告する．$n = m$ の MQ 問題を Hybrid approach を用いて解く場合，代入する変数の数を k，多項式環の係数体を K とすると，全ての解を計算するには K^k 回の Gröbner 基底計算が必要であるが，代入を行う前に Gröbner 基底計算をあらかじめ進めておくことが可能であれば，代入後の K^k 回行われる Gröbner 基底計算が緩和されることが想定される．

* 東京大学大学院 情報理工学系研究科 数理情報学専攻, 東京都文京区本郷 7-3-1, Department of Mathematical Informatics, The Graduate School of Information Science an Technology, The University of Tokyo, 7-3-1, Hongo, Bunkyo-ku, Tokyo, Japan

参考文献

[1] Bettale L., Faugère J.C. and Perret L., “Hybrid Approach for Solving Multivariate Systems over Finite Fields”, Journal of Mathematical Cryptology, vol. 2, pp. 1–22, 2008.

[2] Faugère J.C., “A New Efficient Algorithm for Computing Groebner Bases (F4)”, Journal of Pure and Applied Algebra, vol. 139, pp. 61–88, 1999.

[3] Faugère J.C., “A New Efficient Algorithm for Computing Groebner Bases (F5)”, In Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation, ISSAC 2002, pp. 75–83, 2002.

[4] Peter W. Shor. “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer”. SIAM Review, Vol. 41, No. 2, pp. 303–332, 1999.