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

近似イデアルGCD問題に基づく不定方程式暗号のバリエーションについて
A variant of the indeterminate equation cryptosystems based on the approximate ideal GCD problem

秋山 浩一郎 *　　池松 泰彦 †
Koichiro Akiyama　　Yasuhiko Ikematsu

キーワード　耐量子計算機暗号、近似 GCD 計算、不定方程式、代数曲面暗号

あらまし

不定方程式暗号は不定方程式の求解問題の計算困難性をベースとする耐量子計算機暗号である。特に、非線形不定方程式の求解問題は（その係数環の取り方によっては）一般的な解法アルゴリズムがないことが証明できる極めて計算困難性の高い問題（非可解問題）となっている。本論文で述べる近似イデアルＧＣＤ問題に基づく不定方程式暗号もそのような非可解問題に基づく耐量子計算機暗号で、文献 [1] において提案され、鍵長が RSA 暗号の約 1/2 となることが主張されている。

本論文では、この近似イデアルＧＣＤ問題に基づく不定方程式暗号において、暗復号処理を簡素化できる 1 つのバリエーションを提案する。提案するバリエーションはこの簡素化によって復号演算の高速化が可能となる。しかしその一方で、文献 [2] において指摘されている部分イデアル分解攻撃が適用可能となり、その耐性評価が必要となる。本論文では文献 [1] において提案されているオリジナルアルゴリズムを復習し、そのバリエーションを提示するとともに部分イデアル分解攻撃への耐性を計算機実験に基づいて評価する。また、その結果に基づくパラメータを提案し、鍵長や暗号文長を見積もる。

参考文献

[1] 秋山 浩一郎, 池松 泰彦, 小貫 啓史, 縫田 光司, 高木 剛,“近似イデアル GCD 問題に基づく不定方程式暗号 “, SCIS2021, 3A4-1 (2021).

[2] 池松 泰彦, 秋山 浩一郎,“近似イデアル GCD 問題に基づく不定方程式暗号に対するイデアル分解攻撃の考察 “, SCIS2021, 3A4-2 (2021).

* 株式会社東芝　研究開発センター, 〒 212-8582 神奈川県川崎市幸区小向東芝町 1, Toshiba Corporation Corporate R&D Center, 1,Komukai-Toshiba-cho, Saiwai-ku, Kawasaki 212-8582, Japan, koichiro.akiyama@toshiba.co.jp
† 九州大学 マス・フォア・インダストリ研究所, 〒 819-0395 福岡市西区元岡 744 番地 Institute of Mathematics for Industry, Kyushu University, 744 Motooka, Nishi-ku, Fukuoka 819-0395, ikematsu@imi.kyushu-u.ac.jp