様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　３０　年　　５　月　２８　日現在

機関番号：　３２６６５
研究種目：　基盤研究(C)（特設分野研究）
研究期間：　2014～2017
課題番号：　２６５２０２０８

研究課題名（和文）ディオファントス方程式の変換とクリプトシステム原理の新展開

研究課題名（英文）New principle of cryptosystem via translation of Diophantine equations

研究代表者

平田　典子（河野典子）（HIRATA-KOHNO, Noriko）

日本大学・理工学部・教授

研究者番号：９０２１５１９５

交付決定額（研究期間全体）：（直接経費）　　3,800,000円

研究成果の概要（和文）：多項式暗号とディオファントス方程式をむすびつけた新しい暗号方式の新規提案をおこなった．主要結果は東芝研究開発センターの秋山浩一郎氏および日本大学伊藤勝氏，中村周平氏との共同研究として，多項式写像の求解困難性に安全性の根拠をおく耐量子鍵共有方式を論文にまとめて投稿したが，この内容は暗号方式をHonestな参加者の下で実現されたプロトコルに関し送信データを観測できる敵が共有鍵を復元できないという意味で安全証明可能である．その証明も論文の中に記述した．研究集会での講演の際に聴衆であった多項式写像暗号の専門家からは新規性があると認められている．関連するディオファントス近似の諸結果についても出版した．

研究成果の概要（英文）：We propose a new key exchange protocol using polynomial maps, whose security relies on the hardness in finding the solutions to certain polynomial equations. In particular, it concerns polynomial Diophantine equations combined with several translations. Under the assumption that protocol is established honestly, we prove with K. Akiyama, S. Nakamura and M. Ito that our protocol is secure in the sense of the hardness of recovering the common key from the observed data. Form the viewpoint of Diophantine problem in number theory, by means of the method above, we also obtain new results related to the irrationality of polylogarithms and values of special functions of form of Dirichlet series with periodic coefficients.

研究分野：　数論・ディオファントス問題・暗号原理

キーワード：　公開鍵暗号　多項式写像　鍵共有方式　暗号方式　安全証明　可逆写像　ディオファントス方程式　ディオファントス近似

１．研究開始当初の背景

(1) 多項式から構成されるディオファントス方程式を考え，その多項式に対する或る変数変換に基づいた単射写像を考える．ディオファントス方程式と，多項式を単射写像でうつした後の方程式の整数解の情報を公開鍵として与えるとき，それに基づく鍵交換プロトコルの原型は，研究代表者とA．Pethō氏により2010年から2013年にかけての研究によって得られたクリプトシステムであった．これはもともと H．Yosh 氏の論文（The key exchange cryptosystem used with higher order Diophantine equations，International Journal of Network Security & Its Applications，3，(2011)，43--50）において発表されていた方式であり，我々はYosh 方式と呼んでいた．

(2) 上記のYosh 方式の考え方をもとにしたより安全な，新しい代数的クリプトシステムの創成を主目的として研究を開始した．

２．研究の目的

(1) 本研究課題では，研究代表者とPethō氏により上記の論文において数理科学の視点から提案された発想をふまえ，実際の暗号技術として使われるために欠かせない発展的理論の整備を行うことを目的としていた．ディオファントス方程式が有限個の整数解を持つ場合，それら全てを求める作業はたとえ可能であっても計算量が多く困難な場合に，暗号を復号する困難性，即ち暗号の安全性を負わせるような暗号基本原理の新規考察を目的としたのである．

(2) さらにこのクリプトシステムの安全性証明および具体的な実装の可能性に向けた議論も目的の一つであった．先行研究のクリプトシステムとの比較をするための実験も実施したいと考えていた．

３．研究の方法

(1) 国内外の研究者との意見交換，国内外で開催された研究集会における討議などを経由して，多くの共同研究および論文執筆をおこなうことができた．特に南アフリカ，フランスの数学者との共同研究や，フランス，カナダにおける研究討議，日本での国際研究集会への参加および討議が大きな果実を生むものになった．

(2) 研究協力者である東芝の秋山浩一郎氏に実用面の視点からの考察と，検証の面からの協力を依頼したことが実りある成果獲得につながった．とりわけ暗号の基本原理の安全性を保証し得るという証明が可能になった．またプログラミング作成のできる計算支援員の雇用による実装および実験も進んだ．

４．研究成果

(1) 研究は極めて大きく進展し，当初に立てていた目的は達成されたと言って良い．研究代表者は A．Pethō 氏と得た鍵交換プロトコルによる Yosh 方式クリプトシステムの発展形から，新たなクリプトシステムの構築を可能とするような一つの基本構想をもともと得ていた．その改良として，ディオファントス方程式の解を求める困難さに暗号の根拠をおくもの，およびさらに軽量化されたクリプトシステムとして多項式の連立方程式の解を求める計算量の大きさに依存するものをこの研究期間に確立した．研究協力者の秋山浩一郎氏に加え，伊藤勝氏（日本大学理工学部助手），中村周平氏（日本大学生産工学部助手）らとの共同研究による部分を主たる内容として含む．

(2) 関連研究としてはディオファントス方程式とその整数解という数学的対象を抽象化し，ディオファントス方程式の変形のもととなる多変数多項式環の間の全射および単

射写像を特徴づける Jacobian 予想と，その関連分野における研究成果を適用させることも考察した．そして多変数多項式環の上の適切な全単射写像の新しい構成方法と，それに基づく具体的な暗号方式を模索した．基本構想については暗号の専門家を聴衆とする研究集会で講演及び研究討議を実施し，講演の場で得られた実りある意見を加えて精査し，最終年度に向けての論文執筆および投稿もおこなった（最終的な暗号方式提案の論文については投稿は終えたが，まだ査読結果が返ってきていない）．

(3) 同じ手法に基づく別の論文としては，整数で整数に近い値をとる整関数についてディオファントス近似に負う方法を適用させた結果を示した古津博俊氏（日本大学理工学部准教授）との共同研究が出版された．またディオファントス近似の手法を別の数学的対象である多重対数関数に適用させた，複数の関数値の代数体上の一次独立性に関する伊藤勝氏および鷲尾勇介氏との共著論文も出版された．

(4) さらに精度の高いディオファントス近似を用いて，周期的な係数をもつ級数の値の無理数性に対する今までに類似のない新しい結果を証明し，カナダの Banff センター BIRS 数学研究所における国際研究集会“Diophantine Approximation and Algebraic Curves”, BIRS, Banff, Alberta, Canada (No. 17w5045) においての招待講演者として基調講演をおこなった．加えて F. Luca との共著論文を出版して線形回帰数列によって表されたディオファントス方程式の整数解の決定問題にも寄与することができた．T. Kovacs 氏，宮崎隆史氏との共同研究から，別のディオファントス方程式の S 整数解および整数解の決定問題に関する結果も発表した．

(5) 川島誠氏との共同研究によって対数一次形式におけるディオファントス近似の定数値を改良することができた．このさらなる発展的手法に関する構想も得ている．

５．主な発表論文等

〔雑誌論文〕（計 8 件）

① Noriko Hirata-Kohno,
“Diophantine Approximation”, Sugaku Exposition, American Mathematical Society, 査読有り, in press.

② Noriko Hirata-Kohno, Masaru Ito and Yusuke Washio,
“A criterion for the linear independence of polylogarithms over a number field”, Bessatsu, RIMS Kokyuroku, The RIMS, Kyoto University, B. 64, (2017), 3-18, 査読有り．

③ Noriko Hirata-Kohno, Tunde Kovacs-Coskun and Takafumi Miyazaki,
“On the Nagell-Ljunggren equation”, RIMS Kokyuroku, The RIMS, Kyoto University, vol. 2013, (2017), 60-67, 査読なし, DOI: http://www.kurims.kyoto-u.ac.jp/~kyodo/kokyuroku/contents/pdf/2013-08.pdf

④ H. Furutsu and Noriko Hirata-Kohno,
“Conditions of an Analytic Function to be a Polynomial via Diophantine Approximations”,
J. Research Institute of Science and Technology, Nihon University, vol. 136, (2016), 12-16, 査読有り, DOI: https://doi.org/10.11346/cstj.2016.136_12

⑤ Noriko Hirata-Kohno and Florian Luca, “On the Diophantine equation F_n^x + F_{n+1}^x = F_m^y”, Rocky Mountain Journal of Mathematics, vol. 45/ 2, (2015), 509-538, 査読有り, DOI:https://projecteuclid.org/euclid.rmjm/1434208485

⑥ Attila Berczes, Lajos Hajdu, Noriko Hirata-Kohno, Tunde Kovacs and Attila Pethő, “A key exchange protocol based on Diophantine equations and S-integers”, JSIAM Letters, vol. 6, (2014), 85-88, 査読有り, DOI: https://doi.org/10.14495/jsiaml.6.85

⑦ Noriko Hirata-Kohno, “Diophantine approximation related to polylogarithms”, RIMS Kokyuroku, The RIMS, Kyoto University, vol. 1898, (2014), 194-206, 査読なし, DOI:http://www.kurims.kyoto-u.ac.jp/~kyodo/kokyuroku/contents/pdf/1898-17.pdf

⑧ Noriko Hirata-Kohno and Tunde Kovacs, “Computing S-integral points on elliptic curves of rank at least 3”, RIMS Kokyuroku, The RIMS, Kyoto University, vol. 1898, (2014), 92-102, 査読なし, DOI:http://www.kurims.kyoto-u.ac.jp/~kyodo/kokyuroku/contents/pdf/1898-09.pdf

〔学会発表〕(計 11 件)

① Makoto Kawashima and Noriko Hirata-Kohno, “Linear independence of special values of logarithms revisited”, Diophantine Analysis and Related Fields 2018, 2018, http://www.math.keio.ac.jp/~takaaki/DARF2018/DARF2018prog_j.html

② Shuhei Nakamura, Masaru Ito, Koichiro Akiyama and Noriko Hirata-Kohno, “A wild polynomial automorphism in positive characteristic and a key exchange protocol”, 日本応用数理学会年会 研究部会オーガナイズドセッション, 数論アルゴリズムとその応用, 2017, http://annual2017.jsiam.org/program

③ Y. Washio, Noriko Hirata-Kohno, Y. Ishii, Y. Kurimoto, K. Suzuki and M. Zenyoji, “The Irrationality via Diophantine Approximation and Mathematica”, RIMS Workshop, The RIMS of Kyoto University, 2017, https://www.dropbox.com/s/cxpw8mfs7rlvmh2/program2017_v8.pdf?dl=0

④ Noriko Hirata-Kohno, “New Pade approximation related to a series with periodic coefficients”, Diophantine Approximation and Algebraic Curves, BIRS, Banff, Alberta, No. 17w5045, 2017, https://www.birs.ca/events/2017/5-day-workshops/17w5045/schedule

⑤ Masaru Ito, Shuhei Nakamura, Koichiro Akiyama and Noriko Hirata-Kohno, “A key exchange protocol via polynomial automorphisms related to Jacobian conjecture”, 日本応用数理学会連合発表会, 2017, http://union2017.jsiam.org/program#879

⑥ Koichiro Akiyama and Noriko Hirata-Kohno, “A Key Exchange Protocol using Polynomial Map (多項式写像を用いた鍵共有方式)”,

2017 Symposium on Cryptography and Information Security, 2017,
http://www.iwsec.org/scis/2017/program.html

⑦ Noriko Hirata-Kohno,
“Pade approximation and the irrationality of polylogarithms”,
Leuca 2016 conference (celebrating Professor Michel Waldschmidt's 70th birthday) in Leuca, 2016,
http://www.rnta.eu/mw70/speakers.html

⑧ Noriko Hirata-Kohno,
“多重対数関数:ディオファントス近似の視点から”,中央大学理工学部数学科談話会19回, 2014,
http://www.math.chuo-u.ac.jp/danwakai.htm

⑨ Noriko Hirata-Kohno,
“New Diophantine criterion of polylogarithms over an algebraic number field”, RIMS Workshop, Algebraic Number Theory and Related Topics, The RIMS, Kyoto University,
2014,
http://www.ms.u-tokyo.ac.jp/~t-tsuji/ANTRIMS2014/Program2014.pdf

⑩ Noriko Hirata-Kohno,
“Linear independence criterion for polylogarithms in the complex and in the p-adic cases”,
Approximations Diophantiennes et Nombres Transcendants, CIRM, Luminy,
2014,
http://irma.math.unistra.fr/~bugeaud/travaux/ExpoCIRM2014web.pdf

⑪ Noriko Hirata-Kohno and Masaru Ito,
“Diophantine method in determining problem of lattice points”, JANT, JSIAM, 数論アルゴリズムとその応用(2),
2014,
http://jsiam2014.jsiam.org/program#1239

〔その他〕
ホームページ等
(1)http://trout.math.cst.nihon-u.ac.jp/~hirata/index.html

(2)http://kenkyu-web.cin.nihon-u.ac.jp/Profiles/40/0003941/profile.html

６．研究組織
(1)研究代表者
平田典子(河野典子)(HIRATA-KOHNO, Noriko)
日本大学・理工学部・教授
研究者番号：90215195

(2)研究協力者
秋山 浩一郎 (AKIYAMA, Koichiro)