様式20

先端研究助成基金助成金（最先端・次世代研究開発支援プログラム）
実績報告書

本様式の内容は一般に公表されます

研究課題名	高次元 p 進ディオファントス近似と整数格子クリプトシステム
研究機関・部局・職名	日本大学・理工学部・教授
氏名	平田典子 （河野典子）

1. 研究実施期間　平成23年2月10日～平成26年3月31日

2. 収支の状況

（単位：円）

	交付決定額	交付を受けた額	利息等収入額	収入額合計	執行額	未執行額	既返還額
直接経費	15,000,000	15,000,000	0	15,000,000	14,945,100	54,900	0
間接経費	4,500,000	4,500,000	0	4,500,000	4,500,000	0	0
合計	19,500,000	19,500,000	0	19,500,000	19,445,100	54,900	0

3. 執行額内訳

（単位：円）

費目	平成22年度	平成23年度	平成24年度	平成25年度	合計
物品費	477,920	2,836,670	2,609,090	1,327,980	7,251,660
旅費	0	135,520	462,360	106,620	704,500
謝金・人件費等	80,080	1,946,350	1,893,500	2,765,400	6,685,330
その他	242,000	26,560	35,050	0	303,610
直接経費計	800,000	4,945,100	5,000,000	4,200,000	14,945,100
間接経費計	240,000	1,500,000	1,500,000	1,260,000	4,500,000
合計	1,040,000	6,445,100	6,500,000	5,460,000	19,445,100

4. 主な購入物品（1品又は1組若しくは1式の価格が50万円以上のもの）

物品名	仕様・型・性能等	数量	単価（単位：円）	金額（単位：円）	納入年月日	設置研究機関名
パーソナルコンピューター式	アップルジャパン	1	812,818	812,818	2011/6/22	日本大学
				0		
				0		

5. 研究成果の概要

(i) 本研究課題の主たる目的である新規のクリプトシステム構築に関しては，基礎的な数学の研究を元にして，A. Pethoとの共同研究を遂行し，査読付き論文を出版済みである．またその拡張を　A. Petho のみならずT. KovacsおよびA. Berczes, L. Hajdu との共同研究に発展させた．特に高次ディオファントス方程式の求解という新しい公開鍵に基づいた，新規クリプトシステムの提案の研究発表を実施して好評を得ている．具体例も構築した．

(ii) 関数の値が整数格子に近い場所に落ちる場合に起こり得る現象については解明を達成して，査読付き論文を出版済みである．整数格子にかかわる研究をさらに進めた研究内容も査読付き論文として掲載決定済みである．

(iii) 多重対数関数とそのp進版のディオファントス近似に関する研究も進め，研究発表などを行った．

(iv) p進楕円対数の任意個数の代数的係数一次形式のディオファントス近似不等式の下からの評価に対する計算を遂行した．この主張は，短期的な技術革新ではなく，極めて新規性に富む，絶対的な結果として将来にわたり長期間に使われ続けるような，国際的な数学の基礎的結果である．

様式21

課題番号	GR 087

先端研究助成基金助成金（最先端・次世代研究開発支援プログラム）
研究成果報告書

本様式の内容は一般に公表されます

研究課題名 （下段英語表記）	高次元p進ディオファントス近似と整数格子クリプトシステム
	High dimensional p-adic Diophantine approximations and a cryptosystem based on integer lattices
研究機関・部局・職名 （下段英語表記）	日本大学・理工学部・教授
	Nihon University, College of Science and Technology, Professor
氏名 （下段英語表記）	平田典子　（河野典子）
	Noriko HIRATA-Kohno

研究成果の概要

（和文）：本研究課題の高次元p進ディオファントス近似不等式とは、楕円曲線のS整数点の決定のために重要なp進楕円対数に関する不等式であり、長い間その成立が待たれていたものである。本研究においては当該不等式を証明し、楕円曲線のS整数解を決定する整数格子のアルゴリズム構成に応用した。この純粋数学の発想に負い、本研究課題の主たる目的であった、ディオファントス問題の応用に基づく公開鍵暗号の数理的な基礎原理を開拓し、安全な暗号を支える基盤の構築という社会的課題に資する、暗号構造（クリプトシステム）の独創的な指導原理を導いた。

（英文）：We established an inequality associated with Diophantine approximations for linear forms in elliptic logarithms in high dimensional p-adic case. Our result is important in determining the so-called S-integer solutions to a Diophantine equation. We constructed an algorithm to determine all the S-integral points on elliptic curves via this inequality. By means of our new mathematical concept, we created an original key exchange protocol in a cryptosystem based on Diophantine equations, as aimed. Our approach opens a new leading principle to control a secure system in the theory of cryptography.

様式21

1. 執行金額　　19,445,100 円
（うち、直接経費　　14,945,100 円、 間接経費　　4,500,000 円）

2. 研究実施期間　　平成23年2月10日～平成26年3月31日

3. 研究目的

高次元p進ディオファントス近似不等式を確立し、その発想に基づいた新しい暗号構造（クリプトシステム）を提唱すること、また解読にあたる整数格子決定のアルゴリズムの考究を行うことが主たる研究目的であった。特にこのディオファントス問題の数理的考察に負うた、斬新なクリプトシステムを担う、公開鍵暗号の新指導原理を創成することを目指していた。

(1) 高次元p進ディオファントス近似不等式の研究

① 高次元p進ディオファントス近似、つまりp進対数一次形式およびその拡張であるディオファントス近似不等式を確立する。

② 研究①において構築された手法および確率論的手法を組み合わせて、関数の値が整数格子に近い場所に落ちる際の現象を考察する。

③ 関連する手法を一般化して多重対数関数とそのp進版のディオファントス近似を記述し、これらの関数値の諸性質を解明する。

(2) 整数格子の決定アルゴリズムとクリプトシステムへの応用研究

① ディオファントス方程式のS整数解、即ち楕円曲線の整数格子決定アルゴリズムを構成して数値計算をする。

② (1)の①②③、(2)の①の研究により得られた知見を適用し、ディオファントス方程式の整数解を求める操作を基本鍵とするという斬新な発想に基づいた、クリプトシステムの新しい指導原理を提案する。

4. 研究計画・方法

(1) 高次元p進ディオファントス近似不等式の研究

① 高度な計算のできる比較的大型のパーソナルコンピュータ・周辺機器・ソフトウェア等を購入し数値計算を実施

② ディオファントス近似の専門的な知見を持つ国内外の研究協力者を招聘し、研究討議

③ ディオファントス近似の専門家を集め、研究討議の機会を提供するため研究集会を開催

④ ディオファントス近似の専門家に対する講演の実施および研究討議の実行

以上の活動により、求める高次元p進ディオファントス近似不等式を証明した。

(2) 整数格子の決定アルゴリズム構築とクリプトシステムへの応用研究

① 高度な計算の出来る研究支援者を雇用して、暗号計算実験を実施

② 公開鍵暗号に関する専門的な知見を持つ研究協力者を招聘し、研究討議

③ 暗号の専門家に対する講演の実施および研究討議の実行

以上の活動により、ディオファントス近似を応用した暗号の数理的な基礎原理を創成した。

5. 研究成果・波及効果

携帯電話によるメールや、インターネット上でのクレジットカードによる買い物等が日常化された現在では、様々な場面における情報の暗号化は、暮しを守るために重要なものである。暗号においては何よりも安全であることが最重要の課題であり、誰にでもすぐに解読されるものであってはならない。しかし実際には、暗号のからくりを担う基礎理論そのものは数種類しか存在しないため、常に同じ基盤に負うていると、その暗号はいつか破られかねない危険性を持っていた。従って、次世代の安全な暗号を支えるためには、「新しい基礎理論」を開発し続けることが肝要である。

本研究課題ではこの洞察に基づき、数理的な発想を応用した公開鍵を持つクリプトシステムの基礎理論を、下記のように提案した。またそのために必要な純粋数学の理論を発展させた。

1および自分自身以外に約数を持たない2以上の整数を素数という。2以上の正整数は素数の積に一意的に分解されることが知られているが、元の整数が大きい場合にはその計算に時間がかかる。現存するクリプトシステムは、このような素因数分解の計算困難性、あるいは巡回群の生成元というものを求める際の計算困難性等に基づくものが大部分である。本研究では、情報の交換に際して常に傍聴されている場合であっても、伝えたい肝心の情報に関しては簡単には他者に求められないという公開鍵暗号において、ディオファントス問題の求解の計算困難性と素因数分解の困難性の両方を組み合わせた、数理的発想による斬新なプロトコルを開発した。このクリプトシステムには素数pに対応する高次元p進ディオファントス近似が応用されている。これは従来の暗号を支えている数学の基礎理論とは根本的に異なる独創的な内容を持ち、上述の研究動機に応えるものである。

本研究による基礎理論および公開鍵を発表した媒体としては、口頭発表、査読付き論文で既に出版されたもの、査読無し報告文で出版されたもの、引き続き発展した内容をまとめたプレプリントが存在する。これらの公開鍵暗号の実用化を目指し、企業の研究者に対する研究成果の概要説明も、実施している。

様式21

6. 研究発表等

雑誌論文 計 9 件	（掲載済み－査読有り） 計 5 件 [1] Noriko Hirata-Kohno, Arithmetic properties of p-adic elliptic logarithmic functions, Series on Number Theory and its Applications, vol. 7, (eds. Y. Hamahata, T. Ichikawa, A. Murase and T. Sugano), World Scientific, (2011), 110--119. [2] Noriko Hirata-Kohno, Diophantus 近似, 日本数学会「数学」(岩波書店), 64巻 3号, (2012), 254--277. [3] Noriko Hirata-Kohno and Hironori Okada, A note on linear independence of polylogarithms over the rationals, Proceedings of the Japan Academy, series A, 88/9, (2012), 156--161. [4] Masaru Ito and Noriko Hirata-Kohno, Optimization for lattices and Diophantine approximations, Interdisciplinary Information Sciences, vol. 19, no. 2, (2013), 135--142. [5] Noriko Hirata-Kohno and Attila Petho, On a key exchange protocol based on Diophantine equations, Infocommunications Journal, ISSN 2061-2079, vol. 5, no. 3, (2013), 17--21. （掲載済み－査読無し） 計 3 件 [1] Noriko Hirata-Kohno, Arithmetic properties of p-adic elliptic polylogarithms and irrationality, Diophantische Approximationen, Oberwolfach Report vol. 9, issue 2, (eds. Y. Bugeaud and Yu. V. Nesterenko), European Math. Society, (2012), 1347--1351, (DOI: 10.4171/OWR/2012/22). [2] Noriko Hirata-Kohno and Tunde Kovacs, Computing S-integral points on elliptic curves of rank at least 3, RIMS Kokyuroku, Kyoto University, vol. 1898, (2014), 92--102. [3] Noriko Hirata-Kohno, Diophantine approximation related to polylogarithms, RIMS Kokyuroku, Kyoto University, vol. 1898, (2014), 194--206. （未掲載－査読有り） 計 1 件 [1] 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, in press, http://projecteuclid.org/euclid.rmjm/1374758594.

様式21

会議発表 計 19 件	専門家向け 計 18 件 [1] Noriko Hirata-Kohno, The abc conjecture and Diophantine problems, KWMS International Conference (June 21), KIAS, Seoul, Korea, June 21, 2011. [2] Noriko Hirata-Kohno, On Diophantine approximations, Sendai Symposium (August 1-26), Tohoku University, Sendai, August 25, 2011. [3] Noriko Hirata-Kohno, p-adic elliptic logarithms and polylogarithms, Sendai Symposium (August 1-26), Tohoku University, Sendai, August 25, 2011. [4] Kazuyoshi Kobayashi, p進楕円対数一次形式, 日本数学会秋季総合分科会 (September 28-October 1), Shinshu University, Matsumoto, October 1, 2011. [5] Noriko Hirata-Kohno, Arithmetic properties of p-adic elliptic polylogarithmic functions, Diophantine Analysis and Related Fields 2012 (January 9-10), Niigata University, Niigata, January 9, 2012. [6] Noriko Hirata-Kohno, Arithmetic properties of p-adic elliptic polylogarithmis and irrationality, Diophantische Approximationen (April 23-27), the Mathematisches Forschungsinstitut Oberwolfach Workshop, MFO, Oberwolfach,Germany, April 27, 2012. [7] Noriko Hirata-Kohno, Arithmetic properties of elliptic polylogarithms (May 14), Math. Colloq., Graduate School of Mathematics, Osaka University, Osaka, May 14, 2012. [8] Noriko Hirata-Kohno, Polylogarithms revisited from the viewpoint of the irrationality (July 21), Komaba monthly seminar, University of Tokyo, Komaba, July 21, 2012. [9] Noriko Hirata-Kohno, Padé approximations of polylogarithms, Math. Colloq., Graduate School of Mathematics (October 15), Tohoku University, Sendai, October 15, 2012. [10] Noriko Hirata-Kohno, Polylogarithms revisited from the viewpoint of the irrationality, Algebraic Number Theory 2012 (December 3-7), RIMS, Kyoto University, Kyoto, December 7, 2012. [11] Noriko Hirata-Kohno, Sur l'irrationalité de polylogarithmes, Séminaire de Théorie des Nombres (February 28), Université de Caen, Caen, France, February 28, 2013. [12] Noriko Hirata-Kohno, L'irrationalité de polylogarithmes p-adiques, Problèmes Diophantiens, Institut des mathématiques, Université de Paris 6 (March 7), Jussieu, France, March 7, 2013. [13] Noriko Hirata-Kohno, Sur l'irrationalité de polylogarithmes, Séminaire arithmétique et géométrie algébrique (March 8), Institut de Recherche Mathématique Avancée, Université de Strasbourg, Strasbourg, France, March 8, 2013. [14] Attila Petho, On a key exchange protocol based on Diophantine equations, Central European Conference on Cryptology 2013, Telc, Czech Republic (26-28 June), 28 June, 2013.

様式21

	[15] Noriko Hirata-Kohno, Diophantine approximations related to polylogarithms, Analytic Number Theory (November 5-7), RIMS, Kyoto University, Kyoto, 7 November, 2013. [16] Tunde Kovacs, Computing S-integral points on elliptic curves of rank at least 3, Analytic Number Theory (November 5-7), RIMS, Kyoto University, Kyoto, 6 November, 2013. [17] Noriko Hirata-Kohno, Polylogarithms from the viewpoint of Hermite-Padé approximation, East Asia Number Theory Conference (January 20-24), Kyushu University, Nishi-jin Plaza, 20 January, 2014. [18] Noriko Hirata-Kohno, A new cryptosystem based on Diophantine equations, 2014年 日本応用数理学会研究部会「数論アルゴリズムとその応用」 JANTセッション (March 20), Kyoto University, Kyoto, 20 March, 2014. 一般向け 計1件 [1] 平田典子(河野典子), 単位円上の有理数座標の点の幾何学的考察, (鷲尾勇介との共同研究, 2012年9月20日), 数学教育学会 秋季例会講演会(九州大学 伊都キャンパス, 9月18-20日), 数学教育学会誌臨時増刊号, 2012年秋季例会発表論文集, pp. 84--86.
図 書 計0件	
産業財産権 出願・取得状況 計0件	(取得済み) 計0件 (出願中) 計0件
Webページ (URL)	研究代表者の NEXT 研究紹介ウェブページ「NEXT Program 2010-2013」 http://trout.math.cst.nihon-u.ac.jp/~hirata/Next.html
国民との科学・技術対話の実施状況	[1] 平田典子(河野典子), 方眼紙を使った工作で確かめる整数格子の話, 日本大学理工学部駿河台入試フォーラム(対象 高校生), 参加者数 約70名, 2011年7月17日, (内容:整数格子に関する研究の紹介). [2] 平田典子(河野典子), 方眼紙で探る整数格子の不思議, 東京都立科学技術高等学校(対象 高校生), 参加者数 約20名, 2011年10月25日, (内容:整数格子に関する研究の紹介). [3] 平田典子(河野典子), ビー玉で遊ぶと現れる整数格子の最先端研究, 日本大学理工学部駿河台入試フォーラム(対象 高校生), 参加者数 約90名, 2012年7月15日, (内容:整数格子に関する研究の紹介).

	[4] 平田典子(河野典子), 方眼紙で考える分数のはなし, 藤岡市おもしろ数学教室(群馬県藤岡市教育委員会主催, 日本数学会後援), (対象 中学生), 参加者数 約150名, 2012年10月24日, (内容:整数格子に関する研究の紹介). [5] 平田典子(河野典子), 三角比と正多角形, 日本大学豊山女子高等学校 理数科講座 (対象 高校2年生), 参加者数 35名, 2012年12月14日, (内容:整数格子に関する研究の紹介). [6] 平田典子(河野典子), 星印と数列, 日本大学豊山女子高等学校 理数科講座 (対象 高校1年生), 参加者数 35名, 2013年7月17日, (内容:ディオファントス問題に関する研究の紹介). [7] 平田典子(河野典子), 数の不思議と格子点, 埼玉県立草加高等学校(対象 高校2年生), 参加者数 17名, 2013年7月19日, (内容:整数格子に関する研究の紹介). [8] 平田典子(河野典子), タイルばりの不思議, 日本大学理工学部船橋キャンパスウォッチング (対象 高校生), 参加者数 23名, 2013年11月2日, (内容:ディオファントス問題に関する研究の紹介). [9] 平田典子(河野典子), 数列の不思議, 千葉県立 船橋芝山高等学校(対象 高校2年生), 参加者数 41名, 2013年11月26日, (内容:ディオファントス問題に関する研究の紹介).
新聞・一般雑誌等掲載計3件	[1] 上毛新聞「数学って面白い」, 2012年10月27日掲載, 本誌 西北毛-紙面. [2] 雑誌「工学教育」『事例紹介』, 2013年5月号61巻, no. 3, 113--115 (鷲尾勇介と共同). [3] 雑誌「数学セミナー」『素朴で奥深い整数の世界』, 2013年7月号, 52巻, no. 7, (2013), 32--36.
その他	プレプリント (所在 URL http://trout.math.cst.nihon-u.ac.jp/~hirata/publications.html) [1] Attila Berczes, Lajos Hajdu, Noriko Hirata-Kohno, Tunde Kovacs and Attila Petho, A key exchange protocol based on Diophantine equations and S-integers. [2] Noriko Hirata-Kohno and Tunde Kovacs, S-integral points on elliptic curves via new approximation of p-adic elliptic logarithms. [3] Noriko Hirata-Kohno, Linear forms in p-adic elliptic logarithms.

7. その他特記事項

内閣府 FIRST シンポジウム「科学技術が拓く2030 年へのシナリオ」(ベルサール新宿, 平成 26 年 3 月 1 日開催) NEXT グリーンイノベーション ポスターセッション銀賞 受賞, 平成 26 年 3 月 1 日.