様式19 別紙1

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)
実施状況報告書(平成 25 年度)

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. 当該年度の研究目的

当該年度の研究目的は以下である.

(1) 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推し進めて, 全ての定数項を完全に決定する.
(2) 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を, 解析的および確率論的手法を用いて考察する. また整数格子にかかわるディオファントス方程式の解を考察する.
(3) 多重対数関数とそのp進版のディオファントス近似を応用して, これらの関数値の数論的な性質を解明する.
(4) 上記の結果を応用し, 高次ディオファントス方程式の整数解を求める操作がその基本鍵となるような新しい公開鍵の構造を持つクリプトシステムを構築する. A. Petho らとの共同研究に基づき, 新規の暗号の提供に不可欠な数学の基礎的命題を証明する.

2. 研究の実施状況

(i) 本研究課題の主たる目的である(4)に関しては, 目的(1)(2)(3)のための研究を元にして, A. Petho との共同研究を平成 25 年度に遂行し, 査読付き論文を出版済みである(雑誌論文リスト 1). またその拡張を A. Petho のみならず T. Kovacs および平成 25 年度の招聘研究者 A. Berczes, L. Hajdu との共同研究に発展させた. 中間報告として, 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(会議発表リスト 5). 具体例も構築した.

(ii) 目的(2)を達成して, 査読付き論文を1本出版済みである(雑誌論文リスト 2), この整数格子にかかわる研究をさらに進めた研究内容をまとめて投稿し, 査読付き論文として掲載決定済みである(雑誌論文リスト 5).

(iii) 目的(3)を達成して研究発表(会議発表リスト 3・4). 報告論文も出版された(雑誌論文リスト 4).

(iv) 目的(1)を達成して研究発表をおこなった(会議発表リスト2). 結果の一部を報告する論文も出版された(雑誌論文リスト3). 該当する結果は短期的な技術革新ではなく, 絶対的なものとして将来にわたり長期間に使われ続けるような基礎的な数学の結果である.

(v) 以上に関して, 査読付き雑誌に掲載決定済みもしくは投稿中などの状況にあるプレプリントは http://trout.math.cst.nihon-u.ac.jp/~hirata/publications.html に掲載中.

様式19 別紙1

3. 研究発表等

雑誌論文 計 5 件	（掲載済み－査読有り） 計 2 件 (1) Noriko Hirata-Kohno and Attila Petho, On a key exchange protocol based on Diophantine equations, Infocommunications Journal, ISSN 2061-2079, Vol. 5, (2013), No. 3, 17--21. (2) Masaru Ito and Noriko Hirata-Kohno, Optimization for lattices and Diophantine approximations, Interdisciplinary Information Sciences, Vol. 19, No. 2, (2013), 135--142. （掲載済み－査読無し） 計 2 件 (3) 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. (4) Noriko Hirata-Kohno, Diophantine approximation related to polylogarithms, RIMS Kokyuroku, Kyoto University, Vol. 1898, (2014), 194--206. （未掲載） 計 1 件（査読有り） (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, Accepted for Publication.
会議発表 計 5 件	専門家向け 計 5 件 (1) A. Petho, On a key exchange protocol based on Diophantine equations (joint work with Noriko Hirata-Kohno), Central European Conference on Cryptology 2013, Telc, Czech Republic, 26-28 June, 2013. (2) T. Kovacs, Computing *S*-integral points on elliptic curves of rank at least 3 (joint work with Noriko Hirata-Kohno), Analytic Number Theory (November 5-7), RIMS, Kyoto University, 6 November, 2013. (3) Noriko Hirata-Kohno, Diophantine approximations related to polylogarithms, Analytic Number Theory (November 5-7), RIMS, Kyoto University, 7 November, 2013. (4) Noriko Hirata-Kohno, Polylogarithms from the viewpoint of Hermite-Pade approximation, East Asia Number Theory Conference (January 20-24), Nishi-jin Plaza, Kyushu University, 20 January, 2014. (5) Noriko Hirata-Kohno, A new cryptosystem based on Diophantine equations (joint work with T. Kovacs), 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, 20 March, 2014. 一般向け 計 0 件
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

様式19 別紙1

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)「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）． (2)「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）． (3)「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 2 件	(1) 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）． (2) 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, 32--36.
その他	内閣府による最先端研究開発支援プログラム（FIRST）「科学技術が拓く2030 年へのシナリオ」FIRST シンポジウムにおける最先端・次世代研究開発支援プログラム研究展示ポスターにおいて ポスター銀賞を受賞(平成 26 年 3 月 1 日)．

4. その他特記事項

様式19 別紙2

課題番号	GR087

実施状況報告書(平成25年度) 助成金の執行状況

本様式の内容は一般に公表されます

1. 助成金の受領状況(累計) (単位:円)

	①交付決定額	②既受領額(前年度迄の累計)	③当該年度受領額	④(=①−②−③)未受領額	既返還額(前年度迄の累計)
直接経費	15,000,000	10,800,000	4,200,000	0	0
間接経費	4,500,000	3,240,000	1,260,000	0	0
合計	19,500,000	14,040,000	5,460,000	0	0

2. 当該年度の収支状況 (単位:円)

	①前年度未執行額	②当該年度受領額	③当該年度受取利息等額(未収利息を除く)	④(=①+②+③)当該年度合計収入	⑤当該年度執行額	⑥(=④−⑤)当該年度未執行額	当該年度返還額
直接経費	54,900	4,200,000	0	4,254,900	4,200,000	54,900	0
間接経費	0	1,260,000	0	1,260,000	1,260,000	0	0
合計	54,900	5,460,000	0	5,514,900	5,460,000	54,900	0

3. 当該年度の執行額内訳 (単位:円)

	金額	備考
物品費	1,327,980	計算用パーソナルコンピュータ、数学資料等
旅費	106,620	研究集会参加・講演旅費(京都大学)等
謝金・人件費等	2,765,400	PD人件費、臨時職員人件費、専門的知識提供に対する謝金
その他	0	
直接経費計	4,200,000	
間接経費計	1,260,000	
合計	5,460,000	

4. 当該年度の主な購入物品(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
				0		
				0		
				0		