課題番号	GR087

最先端・次世代研究開発支援プログラム
事後評価書

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（河野）典子

【研究目的】

安全な暗号とは、単射写像のうち与えられた像に対し有限回の操作により逆像を求められる解読アルゴリズムを持つが、その実行時間が大きいなど、計算困難性を持つ理論に負うものと捉えることができる。一般的には数学の問題のうち論理的には解決されているが、解答を求める計算が困難であるものを応用して作られることが殆どである。暗号の基礎原理では、技術革新により簡単な解読法が見つかってしまえば、その暗号が使えなくなるという危険性が常にある。したがって、新しい暗号の基礎原理を絶え間なく探求し続けることが必須である。

本研究課題ではこのような暗号の新しい技術の創成に資する、高次元ｐ進ディオファントス近似不等式の確立、その応用による新しい暗号構造（クリプトシステム）の提唱、そして暗号の解読にあたる整数格子決定のアルゴリズムを考究することを目的としている。いわばディオファントス問題の数理科学的考察に応じた高度なクリプトシステムを支える新指導原理を創成することを目指している。

【総合評価】

	特に優れた成果が得られている
	優れた成果が得られている
○	一定の成果が得られている
	十分な成果が得られていない

【所見】

①　総合所見

数学的基盤研究において所期の目的を十分に達成したが、それを活かして応用面の目的を達成するには、更に努力が必要である。そのためには、多くの応用面の研究者の関心を引き付けることから開始すべきであろう。

応用面、特に工学関係の日本人研究者の反応が今一つであるのは、「高次元ｐ進ディオファントス近似」という数学的に深いトピックに対する十分な理解力を持つ研究者が少数で、しかも、何とか理解できる研究者はおおむね忙しい、という現状による部分が大きい。したがって、応用面研究者（特に若手）への一層の普及を通じて暗号構造に関心を持つ研究者の数を増やすことが重要であると判断する。

研究代表者が、海外研究者と共著で、応用面の論文を工学的な側面の強い雑誌に投稿しているのは、具体策の一つとして評価したい。しかしながら、代表者の目的に対する優れた研究成果が浸透するのは、数学者の間でも時間がかかると予想されるので、目的に挙げられた、工学面との連携が必要な応用面に対する成果は不十分ではあるが、工学サイドに伝わるまでにはさらに時間がかかるのはある程度仕方ないことと考える。

本研究においては、主目的であると考えられる原理面の目的における研究は順調に進展して、所期の期待を超える著しい成果が既に得られている点は十分評価する。

②　目的の達成状況

・所期の目的が

（□全て達成された　・　■一部達成された　・　□達成されなかった）

当初の研究目的は、

①　高次元ｐ進ディオファントス近似の確立

②　①を応用した新しい暗号構造の提唱

③　②で提唱された暗号の解読に関するアルゴリズムの研究である。

原理面での目的である①に関しては、ｐ進楕円対数の一般個数の一次結合に関するディオファントス近似不等式を得ており、当初の目標は達成されたと考えられる。

一方、応用面の目的②に関しては、スローガン的な提唱を行った段階にとどまり、応用面の関係者の強い関心をひいているとは言え、応用の現場との接触にまでは到っていない。

総合すると、最も重要である数学的基盤研究において目的①を達成したが、それを活かして応用面の目的②、③に関しては十分に達成されたとは、判断できない。具体的な暗号構造の構築、それを支える目的③に関する成果の充実が課題と考える。

③　研究の成果

・これまでの研究成果により判明した事実や開発した技術等に先進性・優位性が

（■ある　・　□ない）

・ブレークスルーと呼べるような特筆すべき研究成果が

（□創出された　・　■創出されなかった）

・当初の目的の他に得られた成果が（□ある　・　■ない）

ｐ進楕円対数の一般個数の一次結合に関する厳密なディオファントス近似不等式が初めて証明された。

日本数学会の編集する邦文雑誌「数学」に代表者の論説が掲載されることが決定しているが、論説の掲載には、当該分野（代数学、特に整数論）の複数人の権威による推薦が必要である点を考慮すれば、この成果の重要性が広く認識されていることに間違いはない。

一方、数学における重要な新成果が得られたのは間違いないが、極端に新規性に

富む成果ではない。また、応用面に関しては、まだ十分な成果が得られているとは言い難い。これらを勘案すると、特筆すべき成果が創出されたとまでは言えない。

④　研究成果の効果

・研究成果は、関連する研究分野への波及効果が
（■見込まれる　・　□見込まれない）

・社会的・経済的な課題の解決への波及効果が
（□見込まれる　・　■見込まれない）

ｐ進楕円対数の一般個数の一次結合に関する厳密なディオファントス近似不等式の確立は、研究目的を達成するものであり、「高さ」関数の意義、ディオファントス方程式の具体的な整数解決定、楕円関数のＳ整数格子点の具体的な配置など、関連する多くのトピックへの更なる探究を促すだけでなく、その証明の分析を通じて、今後の整数論や代数幾何学などの分野を中心とした数学研究への寄与が見込まれる。

原理的には重要な成果が既に確立されているので、応用面での具体的成果は現時点ではまだ少ないものの、長期的視野に立てば、情報産業を中心とした人間社会における社会的・経済的課題の解決に関し、この研究成果の貢献が見込まれるのは疑いない。しかし、現状では工学面での良いパートナーと巡り合えておらず、研究開発の方向が見当違いの方向になっているという危険性も捨てきれず、短期的にはグリーン・イノベーションへの貢献への見込みは薄いと判断する。

⑤　研究実施マネジメントの状況

・適切なマネジメントが（□行われた　・　■行われなかった）

毎年の執行状況から、非常に着実な研究のマネジメントが行われているという印象を持つ。代表者が、理論面における自身の深遠な結果の証明とその取りまとめに忙しく、応用面では熟練の暗号学専門家からの援助が受けにくい現状の中で、才能ある臨時職員を雇って計算に当たらせているのは妥当な処置であろう。ただし、応用に向けたマネジメントという観点では、知的財産権の取得は無く、もう一歩の努力が必要であったという印象を受ける。

研究成果の公表は、会議発表数が５件以上の発表があり、これは数学者（特に整数論の研究者）としては多い方であり、この点から、研究成果の積極的な発表が行われていると判断する。

国民との科学・技術対話については、件数をみると、理論的な数学者としては飛びぬけた数の一般向け公演を行っている。半分程度は高校生向けであり、国民に向けて、研究内容に繋がる数学を伝えようとする研究代表者の情熱を感じる。数学しかも整数論という高度に抽象的な研究に携わる者としては非常に柔軟な姿勢である点は高く評価できる。