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	
氏　名： 平田典子（河野典子）	**機関名**： 日本大学

1. 研究の背景

暗号は安全な暮しを守るための重要な科学技術の一つですが、純粋数学の理論が本質的に用いられているという事実はあまり知られていないかもしれません。暗号は解読されにくいことが大切ですが、暗号理論そのものを支える基礎理論は、現在せいぜい数種類しかありません。次世代のクリプトシステム（暗号構造）に役立つような純粋数学の理論の創成が本研究の動機として背景にあります。

2. 研究の目標

ディオファントス近似と呼ばれる考え方を元に、ディオファントス方程式もしくは不等式があたえられたとき、解読にあたる整数解（整数格子の点）の求め方について考究し、整数論そのものおよび暗号理論の斬新な指導原理を創成することが、この研究の目標です。

3. 研究の特色

pを素数とします。高次元楕円p進ディオファントス近似という理論を構築します。これは今までの暗号を支えてきた数学の基礎理論とは根本的に異なります。純粋数学の深い理論の応用により、基幹構造の変換が容易な暗号を備えられる点が特色です。

4. 将来的に期待される効果や応用分野

情報科学の見地から俯瞰すれば、暗号が生活の質を高める効果を発揮することは予測できます。ダイレクトに純粋数学の理論を適用する研究により、世界中が安心できる平和な暮しを守るために貢献できればと願っています。

グリーンイノベーション推進への寄与
＝整数論の暗号で明るい暮し

独創性と期待される成果

本研究は、楕円曲線暗号を含む素因数分解暗号・組み合わせ論的暗号などとは異なる理論であるが、ディオファントス近似を暗号に用いる考え方はすでに世界に存在している。しかし肝心の高次元p進楕円対数のディオファントス近似理論が完成していない。

素数pは無限個ある。今までの暗号に使っていた素数を取りかえ、pに関する整数解の定義を変えられることは整数論では知られている。これが暗号の復号困難性の操作に直接応用される。