課題番号：GR087
助成額：20百万円

グリーン・イノベーション

理工系

平成23年2月10日
～平成26年3月31日

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

平田 典子（河野典子） 日本大学理工学部 教授
Noriko Hirata-Kohno

専門分野
数論と暗号の基本原理

キーワード
数論／数論幾何学／群論／暗号系／アルゴリズム理論／ディオファントス近似／格子

WEBページ
http://trout.math.cst.nihon-u.ac.jp/~hirata/Next.html

研究背景

暗号の基礎原理は，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．しかし技術革新により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．従って，新しい暗号の基礎原理を絶え間なく提案し続けることが肝要であった．

研究目的の特色

本研究において，新しいクリプトシステムの指導原理創成のための整数論の基礎的な命題を構築し，それを応用した公開鍵暗号を考案した．高次元 p 進ディオファントス近似不等式という長く未解決であった不等式を証明し，それに基づきディオファントス問題の求解の計算困難性に負う新しい鍵交換プロトコルを提案した．

実績

代表論文：Infocommunications Journal, ISSN 2061-2079, Vol. 5, no. 3, 17-21, (2013)
受賞：FIRSTシンポジウム「科学技術が拓く2030年へのシナリオ」NEXTポスターセッション銀賞(2014年3月)
一般雑誌：
「工学教育」61巻，3号，113-115, (2013年5月)
「数学セミナー」52巻，7号，32-36, (2013年7月号)

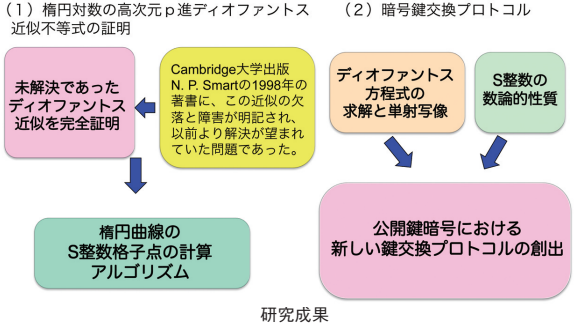
研究成果

高次元p進ディオファントス近似不等式の研究

高次元p進ディオファントス近似不等式という不等式を証明した．これは整数論において未解決であったものであり，1998年出版London Mathematical Society Student Texts, 41巻，N. P. Smart著の本（Cambridge大学出版）の207-210ページにこの不等式の欠落による障害が明記され，解決が望まれていた問題であった．当該研究によってその解決がなされた．

クリプトシステムへの応用

通信における情報交換の場では，他者に傍聴されていても，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性質を持つ公開鍵暗号と呼ばれる暗号構造が知られている．本研究では，前述のディオファントス近似不等式の考え方を応用し，公開鍵暗号におけるディオファントス問題の求解の計算困難性に負う，新しい鍵交換プロトコルを提案した．



研究成果

整数格子の決定アルゴリズム考察

前述で構築された不等式を応用して，楕円曲線の整数格子決定アルゴリズムを考察し，S整数の計算例を求めた．

2030年の応用展開

今までの暗号原理とは異なる斬新な基本原理の提唱は，安全な暗号の根幹を支えることに他ならない．本研究によって考案された，既存の暗号とは別の発想に基づく暗号プロトコルであるが，複数の攻撃者に対する場合の防御法解析などを続け，普遍的なクリプトシステムとしての確立を目指す．また基礎となる数学の研究も進める．