# Public key cryptosystems based on diophantine equations

奥村, 伸也

https://doi.org/10.15017/1500515

（様式３）

氏　　名　：奥村　伸也

論 文 名　：Public key cryptosystems based on diophantine equations
（ディオファントス方程式に基づいた公開鍵暗号）

区　　分　：甲

## 論　文　内　容　の　要　旨

本論文では、代数曲面暗号の安全性の根拠となっている「求セクション問題」についての研究と、数論の最も古典的な問題の一つである整数係数ディオファントス方程式の整数解・有理数解を求めることの困難性に基づいた公開鍵暗号の提案を行っている。前半では代数曲線暗号について復習した後、安全な代数曲面暗号を設計するために求セクション問題の困難性評価のための下準備となる研究を行った。後半では、ディオファントス方程式の求解困難性を利用した 4 つの公開鍵暗号を提案した。ディオファントス方程式の整数解・有理数解を求める問題は、量子計算機を用いたとしても効率よく解くアルゴリズムは知られていないため、耐量子暗号として期待できる。各章の概要は次の通りである。

第 1 章では、求セクション問題と代数曲面暗号及び現在までに知られている代数曲面暗号に対する攻撃法の概要について説明している。求セクション問題とは、与えられた多項式$X(x,y,t) \in \mathbb{F}_p[x,y,t]$に対して、$X\big(u_x(t),u_y(t),t\big)=0$を満たす多項式$u_x(t),u_y(t) \in \mathbb{F}_p[t]$を見つける問題であり、関数体上のディオファントス問題と見ることができる。量子計算機を用いたとしてもこの問題を効率よく解くアルゴリズムは未だに知られていないため、代数曲面暗号は耐量子暗号の一つとして研究されている。代数曲面暗号の最新版は 2009 年に秋山・後藤・三宅氏の３名により提案されているが、Faugère と Spaenlehauer により提案された「イデアル分解攻撃」によりその一方向性は破られている。この攻撃では、あるイデアルの分解を利用して終結式を用いることにより平文多項式を含むイデアルを構成し、そのイデアルには平文多項式と同じ形式の多項式があまり含まれていないことを利用している。

第 2 章では、求セクション問題の困難性を評価するための研究について述べている。求セクション問題を解くことは公開鍵の多項式とその多項式が定義する曲面のセクションに依存した、ある多次多変数連立方程式（セクション方程式と呼ぶ）を解く問題に帰着することができる。その連立方程式をグレブナー基底を用いて解く場合の計算量を評価するのに重要な「semi-regular」という概念とその性質について説明する。多項式列が semi-regular であるための必要十分条件を導き、セクション方程式に出てくる多項式の semi-regularity についての実験結果とその考察、今後の課題について述べる。なお、この章は東芝（株）研究開発センターの秋山 浩一郎氏との共同研究である。

第 3 章は、第 4 章で提案する暗号の安全性の根拠となるディオファントス問題についてのサーベイである。とくに、Faltings の定理（Mordell 予想）や Vojta 予想と Lang 予想など代数多様体上の有理点に関する定理や予想、ディオファントス近似とその応用、ある種の 2 変数ディオファントス方程式に対する Baker の理論による整数解の有限性ついて説明する。

第 4 章では､ディオファントス方程式の求解困難性に基づいた 4 つの公開鍵暗号を提案している。提案方式はどれも代数曲面暗号と同様で、平文である多項式を別の多項式に紛れ込ませることで暗

号化を行っている。

まず初めに、第一章で述べた代数曲面暗号と本質的に同じ暗号を提案した。秘密鍵は $n$ 個の整数の組 $(a_1, \dots, a_n) \in \mathbb{Z}^n$ であり、公開鍵は整数係数の多次多変数多項式 $X(x_1, \dots, x_n) \in \mathbb{Z}[x_1, \dots, x_n]$ で $X(a_1, \dots, a_n) = 0$ を満たすものとする。このような $X$ は秘密鍵 $(a_1, \dots, a_n)$ から容易に構成することができる。暗号化では平文多項式 $m(x_1, \dots, x_n) \in \mathbb{Z}[x_1, \dots, x_n]$ を次のように

$$F_i = m + s_i f + r_i X \ (i = 1,2)$$

別の多項式に紛れ込ませている。復号では秘密鍵により $X$ を消して $m(a_1, \dots, a_n)$ を隠しているものを少なくし、いくつかの操作ののちに $m(a_1, \dots, a_n)$ を手に入れ、それから $m(x_1, \dots, x_n)$ を復元している。ただし、途中で整数の因数分解を行う必要があるためあまり効率的な暗号とは言えない。また平文多項式に秘密鍵を代入した $m(a_1, \dots, a_n)$ を用いて元の多項式 $m(x_1, \dots, x_n)$ を一意的に復元する必要があるため、$\mathbb{Z}[x_1, \dots, x_n]$ の部分集合 $S \neq \mathbb{Z}$ で写像 $S \ni g \mapsto g(a_1, \dots, a_n) \in \mathbb{Z}$ が単射になるものを見つける問題、及び $g(a_1, \dots, a_n)$ から $g$ を復元する方法についても考察を行った。このことに関して、いくつかの部分集合とそれぞれの部分集合に対する復元方法を与えることができた。さらに、この暗号についてもイデアル分解攻撃の類似を適用でき、$n = 2,3$ の時その一方向性を効率よく破ることができることを実験により確かめた。それ以外（$n \geq 4$）の時は、さらなる実験が必要である。

2 番目と 3 番目の暗号では、イデアル分解攻撃を避けるために公開鍵をそのまま用いずに、平文の送り手に公開鍵と平文多項式を変換してもらう方式をとっている。変換は送り手が選んだ整数 $\ell$ を用いて行われ、秘密鍵を知っていれば整数 $\ell$ を手に入れて容易に平文多項式を得ることができる方式を提案した。しかし、どちらの暗号も秘密鍵を知ることなく整数 $\ell$ を手に入れる方法が存在するため、これらの暗号の一方向性も破られてしまうことがわかった。

4 番目の暗号では、秘密鍵は今まで通りで公開鍵として $X\left(\frac{a_1}{d}, \dots, \frac{a_n}{d}\right) = 0$ を満たす多項式 $X$ と整数 $d$ と $e$ を選ぶ。ただし、$\gcd\left(\prod_i a_i, d\right) = 1$ と仮定し、$X$ を著者が``degree increasing type”（次数上昇型）と呼んでいる特殊なものを用いるとする。$X$ と同じ形式の多項式 $f, m_c, s_i, r_i$ を用いて

$$F_i = m_c + s_i f + r_i X \ (i = 1,2,3)$$

を構成する。そして 4 つ組（$F_1, F_2, F_3, N$）を暗号文として送る。復合では、秘密鍵を用いて $X$ を消し GCD 計算やモジュラー計算などを用いて $m_c\left(\frac{a_1}{d}, \dots, \frac{a_n}{d}\right)$ を手に入れてから、その値を元に $m(x_1, \dots, x_n)$ を復元する。その際 $m_c$ が次数上昇型の多項式であることが大事であり、モジュラー計算と（RSA 暗号のように）オイラーの定理も利用している。今回提案した方式ではイデアル分解攻撃を避けるため、$m_c$ を含むイデアルが構成できたとしても、そのイデアルは $m_c$ と同じ形式で同じように係数の大きい多項式を多く含むため $m_c$ を特定することが難しくなるようにしている（$f$ と $m_c$ が $X$ と同じ形式であることも大事であり、これが次数上昇型の多項式を公開鍵としている理由である）。また、代数曲面暗号に対するイデアル分解攻撃以外の攻撃の類似についても検討し、現状ではどれもこの暗号の一方向性を破る有効な攻撃ではないと結論付けた。