Public key cryptosystems based on diophantine equations

奥村, 伸也

https://doi.org/10.15017/1500515

（様式６ - ２）

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）
論文調査委員	主　査　九州大学　　准教授　田口　雄一郎 副　査　九州大学　　教授　髙木　剛 副　査　九州大学　客員教授/(株)東芝研究開発センター 秋山　浩一郎 副　査　日本大学　　教授　平田　典子

論　文　審　査　の　結　果　の　要　旨

本論文に於いて奥村氏は、ディオファントス問題の求解困難性を根拠とする暗号系について、二つの重要な研究を行っている。一つ目は、代数曲面暗号に現れるセクション方程式系の semi-regularity に関する実験的考察であり、二つ目は、代数曲面暗号の代数体版である新しい暗号系の構築びその安全性の検証である。

現在広く使われているＲＳＡ暗号は、将来量子コンピュータが実用化されれば容易に破られてしまう事が証明されている。代数曲面暗号は量子コンピュータによる攻撃にも耐えるであろう次世代の暗号系として秋山-後藤-三宅により提案された。代数曲面暗号の安全性は「求セクション問題」の困難性に基づいている。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、$X(u_x(t),u_y(t),t) = 0$ 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、函数体上のディオファントス問題と見る事が出来る。量子コンピュータ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注目されている。一方、代数曲面暗号に対する攻撃法もまた幾つか提案されている。特に、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、或るイデアルの準素イデアル分解を利用して終結式を用いる事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事を利用している。この様な状況の中、代数曲面暗号を実装する際にその安全性の根拠となる求セクション問題の困難性を評価する事は重要な課題である。本論文の第一の成果は、これを評価するための基礎となる優れた研究である。求セクション問題を解く事は公開鍵である多項式 $X(x,y,t)$ 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事が出来る。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際に重要な「semi-regular」という概念があるが、奥村氏は（株）東芝研究開発センターの秋山浩一郎氏との共同研究により、多項式列が semi-regular であるための必要十分条件を導き、セクション方程式として現れる多項式列の semi-regularity がどれくらいの頻度で成り立つのかについての実験的考察を行い、多くのデータを得た。その結果、多くの場合 semi-regularity は成り立たない事が判明した。この結果は、今後の研究に指針を与えると言う意味で重要なものである。

本論文の第二の成果であるディオファントス方程式に基づく新しい暗号系は、整数論に於いて古

くから知られている「代数体と函数体の類似」という指導原理に導かれてオリジナルの代数曲面暗号を有限体上の一変数代数函数体上の代数曲線の有理点を用いた暗号と解釈し、その代数体版を構築したものであり、奥村氏は４つの新しい公開鍵暗号を提案している。これらの暗号系はどれも形式的にはオリジナルの代数曲面暗号と似たものであり、平文である多項式を別の多項式に紛れ込ませる事で暗号化を行っているが、細かい所では代数体特有の事情により色々と異なっている。奥村氏独自の工夫としては、平文多項式を復元する際に鍵となる概念として「次数上昇型多項式」という概念を定義して用いている事、秘密鍵として整数点のみならず有理点も使用する事で安全性の向上を狙った事、整数環に於ける素因数分解が多項式環に於ける既約多項式分解よりも手間がかかる事を考慮して暗号文となる多項式を（代数曲面暗号の場合の二つから）三つに増やした事、安全性と将来性を考慮して多変数版も考察している事、平文多項式の係数を「捻る」事により安全性の向上を図っている事、等が挙げられる。今回奥村氏が提案している４つの暗号系の中では最後のものが最も有望であり、奥村氏は本論文の最終章でこれについて安全性を検討している。その結果、代数曲面暗号に対して考案されている既存の攻撃法はどれもこの暗号の一方向性を破るほど有効ではないと結論されている。なお、公開鍵となる多項式に課されている現在の諸条件を緩和することにより、安全性の根拠となるディオファントス方程式をより求解困難とし、これにより暗号の安全性を向上させるという今後の大きな研究課題も暗示され、奥村氏の研究の発展性が示唆されている。この様に、奥村氏の提案する新しい公開鍵暗号は、量子コンピュータに耐性を持つ代数曲面暗号をディオファントス方程式に拡張する事により新たな可能性がある事を示唆するものであり、非常に有意義な研究成果である。

以上の結果は、暗号理論に於ける重要な貢献であり、数論の分野において価値ある業績と認められる。

よって、本研究者は博士（数理学）の学位を受ける資格があるものと認める。