

審査の結果の要旨

氏 名 王 亜成

公開鍵暗号は、情報社会の安全性を支える要素技術として広く利用されている。現在普及している公開鍵暗号となるRSA暗号や楕円曲線暗号の安全性は素因数分解問題や離散対数問題の困難性を基にしているが、これらの問題はShorの量子アルゴリズムにより多項式時間で解くことが可能であることが知られている。そのため、従来とは異なる数学問題を利用することにより、量子アルゴリズムに耐性がある公開鍵暗号を構成する耐量子計算機暗号の研究は重要となる。本論文では、有限体上の多変数多項式求解問題の困難性に基づく多変数多項式暗号の安全性評価を主な目的としている。

本論文は「Security Evaluation of Multivariate Public-Key Cryptography via Algebraic Techniques」（代数的手法による多変数多項式暗号の安全性評価）と題し、8章からなる。

第1章「Introduction」（序論）では、暗号理論の基本的な事項を説明した後に、量子アルゴリズムに対して安全となる耐量子計算機暗号の主要な候補およびその数学問題の概要を解説している。特に、多変数多項式求解問題の困難性に基づく多変数多項式暗号を概説して、本研究の位置付けを示している。また、多変数多項式求解問題を効率的に解くグレブナー基底アルゴリズムに関して主要な手法および計算量の評価方法を説明している。

第2章「Multivariate public-key cryptography」（多変数多項式暗号）では、多変数多項式暗号の基本概念を説明し、主要な方式となるRainbow署名方式およびHFEv-署名方式に対してトラップドアの構成方法および安全性評価法に関して解説している。安全性評価法では、主要な攻撃手法となるグレブナー基底による直接攻撃、多項式系の構造を利用したRank攻撃などを説明している。更には、現在までに知られている多変数多項式暗号の構成による分類を概説している。

第3章「Algebraic techniques for solving polynomials」（多項式解法の代数的手法）では、可換環や代数幾何における基本的な数学定理を述べた後に、有限体上の多変数多項式システムの解を効率的に求めるグレブナー基底を用いたアルゴリズムを説明している。特に、Hilbert多項式を用いた正則次数によるF4アルゴリズムの計算量評価方法を解説している。

第4章「Evaluating the security of EFC using algebraic techniques」（代数的手法による暗号方式EFCの安全性評価）では、Extension Field Cancellation (EFC) と呼ば

れる多変数多項式を用いた公開鍵暗号方式の安全性を評価している。既存のEFCに対する安全性評価ではHFE方式に変形した正則次数による考察がなされていたが、本論文は変数の一部を総当たりするhybrid法による攻撃計算量の削減手法を考察している。Hybrid法のグレブナー基底の計算におけるstep次数を評価することにより、従来は83ビットの安全性を持つと評価されていたEFCの暗号パラメータ $(n, a) = (83, 10)$ が、67ビットの計算量で攻撃可能であることを示した。

第5章「On the algebraic aspects of solving the minrank problem」(minrank問題の代数的解法に関して)では、特別な代数構造を有する多変数多項式暗号に対する攻撃として有効な手法として知られるminrank問題の困難性を考察している。本論文は、Kipnis-Shamir法と余因子行列を用いる既存の二つの手法に対して、underdeterminedな多項式システムの線形従属性を考察した融合手法を提案している。これにより、minrank攻撃に対して従来では156ビットの安全性を持つと評価されていたRainbow署名のパラメータ $(q, v, o_1, o_2) = (16, 32, 32, 32)$ が、138ビットの計算量で攻撃可能であることを示した。

第6章「Algebraic cryptanalysis of multivariate encryption scheme PERN」(多変多項式暗号方式PERNの代数的攻撃手法)では、実数体上の多項式システムを用いた暗号化方式PERNの安全性を評価している。特に、グレブナー基底を用いたhybrid法により攻撃計算量の理論的評価と解読実験による正則次数の検証を考察し、128ビット安全性を有するPERNの暗号パラメータとして $(m, p, q) = (65, 7, 5)$ を提案した。

第7章「On the Weil descent attack against the MQ problem」(MQ問題に対するWeil降下攻撃法について)では、標数2の拡大体上の多変数多項式を素体上の多項式で表現するWeil降下攻撃法を考察している。本論文では、低次数の非自明なsyzygiesを考察し、Weil降下により得られる多項式システムの正則次数が、semi-regularシステムの次数より減少することを証明している。これにより、多変数多項式暗号で用いられる大きさの暗号パラメータに対して、数十ビット程度の計算量が低下する評価を得た。

最後に第8章「Conclusion and future work」(結論と今後の課題)では、本論文の成果を簡潔にまとめると共に、今後の研究課題を提示している。

以上を要するに、本論文は、量子計算機の時代にも安全となる多変数多項式暗号に関して、minrank問題による攻撃やWeil降下攻撃法などの詳細な計算量をグレブナー基底による代数的手法により評価し、幾つかの暗号方式(EFC, Rainbow, PERN)の実用的なパラメータに対して理論的な安全性評価を与えたものである。これらの成果は数理情報学分野の発展に寄与するところが多い。

よって本論文は博士(情報理工学)の学位請求論文として合格と認められる。