審査結果の要旨

論文提出者　國廣 昇

本論文は，「Security and Efficiency Analyses of Public Key Cryptosystems（公開鍵暗号の安全性解析と高速化手法）」と題し，8章から構成されている．情報化社会を支える不可欠な技術として暗号技術があり，その中でも公開鍵暗号は，電子商取引や電子現金などを始めとするさまざまな情報・通信システムのセキュリティを支える基礎技術となっており，その安全性や処理の高速化が重要な研究テーマになっている．本論文では，安全性に関して，(1) 素因数分解の高速化，(2) RSA型楕円曲線暗号の安全性評価，(3) ElGamal型楕円曲線暗号の安全性評価，(4) RSA暗号の改良法の提案とその安全性評価を行っており，また高速化に関しては，(5) べき乗計算の高速化を行い，こられに対して新しい知見を与えている．

第1章「Introduction」は，序論であり，研究の背景と目的を述べるとともに，従来の公開鍵暗号研究に対する本論文の位置付けを与えている．また，本論文の構成を示している．

第2章「Preliminaries」では，公開鍵暗号の基礎となる整数論および楕円曲線理論を要約すると共に，重要な公開鍵暗号方式の暗号化・復号化アルゴリズムとその安全性などの特徴を紹介している．

第3章は，「Speeding up elliptic curve factoring method（素因数分解の高速化）」と題し，従来よりもより短い時間で素因数分解可能な方法を提案している．具体的には，素因数分解の一方式である楕円曲線法の改良として，「剰余環上で定義された楕円曲線の点の個数が，与えられた素数で割り切れるかどうかを判定する多項式時間アルゴリズム」の存在を仮定すれば，従来の楕円曲線法を適用する前に良い性質の楕円曲線を選び出すことができ，それにより，素因数が10^{30}～10^{50}の時，従来の楕円曲線法よりも，3～4倍高速化できることを理論的に明らかにしている．

第4章は，「Difficulty of counting the number of points on elliptic curve over the ring Z/nZ（剰余環Z/nZ上の楕円曲線の点の個数を求める困難さ）」と題し，RSA型楕円曲線暗号の一つであるKMOV暗号の安全性を評価している．KMOV暗号は，「素因数分解の困難さ」に安全性の根拠を置いているとともに，「剰余環上の楕円曲線の点の個数を求める問題」の困難さにも安全性の根拠を置いているが，本章では，この二つの問題が，確率的多項式時間の意味で計算量的に等価であることを，理論的に証明している．

第5章は，「Discrete log problem for super-anomalous elliptic curve（超アノマラス楕

円曲線に対する離散対数問題）」と題し，ElGamal型の楕円曲線暗号の安全性評価を行っている．この暗号は，楕円曲線として，特殊な曲線（anomalous curve や supersingular elliptic curve）を選んでしまうと簡単に解読されてしまうことが解っているが，本章では，それら以外にも解読が可能な曲線があることを明らかにしている．具体的には，まず超アノマラス楕円曲線を定義し，この曲線上の離散対数問題を確定的多項式時間で解くアルゴリズムを２つ提案している．その結果，この超アノマラス楕円曲線を用いたElGamal型の楕円曲線暗号が安全でないことを明らかにしている．

第６章は，「Multi-variate RSA cryptosystems and their security analyses（多変数RSA暗号方式とその安全性）」と題し，RSA暗号の改良型を提案すると共に，その処理速度と安全性の評価を行っている．提案方式は，Koyama暗号方式の一般化を行って多変数化したRSA暗号であるが，送りたい長いメッセージをいくつかのブロックに分割し，そのブロックを多変数有理関数を用いて処理し，処理後のブロック一つだけに対して，べき乗演算を行う方式であるため，通常のRSA暗号よりも高速である．ただし，盗聴者がブロック間の関係を知ったとき，メッセージは全て解読されてしまうため，安全性が少し低下するが，使用条件に注意すれば，十分に安全で高速な暗号方式とみなすことできる特徴を有している．

第７章は，「How to generate shot addition chains（短い加算連鎖作成法）」と題し，公開鍵暗号で使用される「べき乗計算 $C=M^e \bmod n$」の高速化，特に，べき乗計算におけるかけ算回数を減らす方法を明らかにしている．べき乗計算は，それをかけ算に分解して計算するために，addition chainを利用して計算されるが，短いaddition chainを作成るための２つの効率的なアルゴリズム（Run-length法とHybrid法）を提案し，その性能を理論的に解析すると共に，数値実験によりその性能を確認している．これらの手法は，データ圧縮の理論を導入したユニークな方法であり，従来のWindow methodなどに比べて，効率的であることが示されている．

第８章「Conclutions」は，結論であり，本論文の内容がまとめられていると共に，今後の研究課題が示されている．

以上を要するに，公開鍵暗号の重要な方式であるRSA暗号，RSA型楕円暗号，ElGamal型楕円暗号の安全性に関して新しい知見を与えており，これらの成果を利用することにより，それらの暗号のより厳密な安全性評価が可能となっている．これらの成果は，今後新たに提案される多くの暗号に対する設計指針を与えたことにもなっている．また，高速なべき乗計算法を用いれば，公開鍵暗号の暗号化復号化処理をより高速に行うことができ快適な使用が可能になる．したがって，本論文は暗号理論の研究に大きく貢献するとともに，数理工学の進歩に対して寄与するところが大であり，博士（工学）の学位請求論文として合格と認められる．