論文の内容の要旨

論文題目　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）

氏名　　國廣　昇

1976年のDiffie and Hellmanによる公開鍵暗号系の提案以後，数多くの研究がなされている．その研究の成果は，現在の情報社会の基礎となっており，電子商取引，電子現金等が現実のものとなりつつある．しかし，依然，安全性を不安視する意見もあり，問題が全て解決されているわけではない．例えば，完全に安全性が証明され，なおかつ，実用に耐えうる暗号は未だ提案されていない．それゆえ，新たな暗号の提案が今も活発に行われている．新たに提案された暗号が，広く世の中に浸透するかどうかは次の二つの問い：「その暗号は十分安全であるか?」，「その暗号は実用上十分な速度を持っているか?」にどう答えるかにかかっている．その観点から，我々は，公開鍵暗号の安全性に関する研究，及び高速化に関する研究を行った．その研究の成果として，安全性に関する成果4件，高速化に関する成果1件を得た．安全性に関する研究については，(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 暗号の改良法の安全性評価，を行った．高速化に関しては，(5) べき乗計算の高速化を行っている．

(1) 素因数分解の高速化について

いくつかの公開鍵暗号，特に RSA 暗号の安全性は素因数分解の困難さに根拠をおいている．我々は，素因数分解を効率的に行うアルゴリズムを提案した．具体的には，有効な素因数分解法である楕円曲線法に改良を加え，ある仮定の下で，従来よりもより短い時間で，素因数分解に成功する方法を提案した．さらに，その有効性を理論的考察により示した．その方法は，「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を判定する多項式時間アルゴリズム」の存在を仮定し，このアルゴリズムを有効に利用することにより，事前に良い性質の楕円曲線の選別を行うという特徴を持っている．ここで，「良い性質の楕円曲線」とは，その点の個数が小さな素数の積を因数に持つ楕円曲線を指す．この選別により生成された良い性質の楕円曲線に対してのみ，楕円曲線法を適用することにより，高速化を実現している．その結果，見つけたい素因数 p が 10^{30} から 10^{50} 程度の時，提案方式は従来の楕円曲線法よりも，3 から 4 倍高速化されている．また，漸近的には，$(\log p)^{0.318}$ 倍高速化されることを，理論的解析により明らかにした．

(2) RSA 型楕円曲線暗号の安全性評価について

ついで，公開鍵暗号の一つである RSA 型の楕円曲線暗号の安全性解析を行っている．このタイプの代表例である 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．我々は，この二つの問題が，実は，計算量的に等価であることを示した．前者の問題を解くオラクルを用いれば，後者の問題が簡単に解けることは自明であるので，その逆，後者の問題を解くオラクルを用いれば，前者の問題が解けることを示した．具体的には，楕円曲線の点の個数を求めるオラクルを用いて，確率的多項式時間で素因数分解を行うアルゴリズムを提案した．このアルゴリズムは，ある合成数 n と Euler の ϕ 関数 $\phi(n)$ が与えられ時に，n の素因数分解を行う Miller のアルゴリズムを基にしている．さらにこの結果を利用して，前述の「点の個

数を求める問題」よりも直感的には易しいと考えられる問題：「剰余環上の楕円曲線上の点の個数を，与えられた素数で割った余りを求める問題」も素因数分解問題と計算量的に等価であることを示した．さらに，「剰余環上での楕円離散対数問題」を解くオラクルを用いれば，素因数分解が確率的多項式時間で可能であることを示した．

(3) ElGamal 型楕円曲線暗号の安全性評価

ついで，公開鍵暗号の一つである ElGamal 型の楕円曲線暗号の解析を行っている．このタイプの暗号は，暗号として用いる曲線として，特殊な曲線 (anomalous 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． anomalous elliptic curve に関しては， Rück, Semaev, Smart, Satoh-Araki らがほぼ同時にその攻撃法を提案している．我々は，まずこの anomalous elliptic curve の概念を拡張した super-anomalous elliptic curve を定義し，ついで，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 つ提案した．我々の提案したアルゴリズムは， Rück が提案したアルゴリズムと Satoh-Araki が提案したアルゴリズムをそれぞれ拡張した形になっている．さらに，提案したアルゴリズムにより解読されてしまう暗号に関しても考察を行っている．

(4) RSA 暗号の改良法の安全性評価

RSA 暗号の提案以後，いくつかの改良版が提案されている．我々は，そのうちの一つ， Koyama 暗号方式の一般化を行い，その一般化された暗号方式（以後，多変数 RSA 暗号方式）の暗号化，復号の速度評価及び安全性解析を行った．多変数 RSA 暗号方式は， (1) 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， (2) そのブロックを多変数有理関数を用いて処理し， (3) 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．この暗号の速度に関しては，通常の RSA 暗号よりも高速であることを理論的考察により明らかにした．また，安全性解析の結果としては， (1) 盗聴者にブロックの一つが厳密にわかったとき，メッセージは全て解読されてしまう， (2) 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， (3) メッセージを 2 回送り，なおかつ，そのメッセージ中に，関連のブロックが含まれていた時，メッセージは 2 つとも全て解読されてしまう，ことを示した．

以上の考察により，多変数RSA暗号方式の総合的な評価は，次のようになる．従来の方式と比較して十分高速であるが，その反面，若干の安全性の低下を招いている．しかし，安全性が低下する使用条件に注意すれば，十分安全で高速な暗号方式とみなすことができる．

(5) べき乗計算の高速化

公開鍵暗号の高速化に関しては，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目的で，より短い Addition chain の構成法に関する研究を行った．我々は，二つの効率的なアルゴリズム，(1) Run-length 法，(2) Hybrid 法を提案し，理論的解析，及び数値実験による解析を行った．その結果，この二つの方法は，e の2進系列中の1の個数 w が大きい時に，従来の方法（例えば，Window method）よりも効率的であることを示した．より具体的には，e の2進系列の長さを L とすると，

- $0.8 \leq w/L \leq 1$ の時，Run-length 法が，
- $0.6 \leq w/L \leq 0.8$ の時，Hybrid 法が，
- $0 \leq w/L \leq 0.6$ の時，Window 法が，

最適であることを明らかにした．また，$w/L = 0.95$ の時，Run-length 法は，Window 法より，8% 短い Addition chain を構成することを示した．

この研究を通して，公開鍵暗号の安全性に関して，ある一定の新たな寄与をすることができた．これらの成果を利用することにより，従来提案されている暗号のより厳密な安全性評価が可能となった．さらに，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なる．また，高速な暗号化手法を与え，より快適な公開鍵暗号の使用を可能とした．