氏名	村上恭通（むらかみやすゆき）
学位(専攻分野)	博士（工学）
学位記番号	博乙第103号
学位授与の日付	平成13年3月26日
学位授与の要件	学位規則第4条第2項該当
学位論文題目	Studies on Public-Key Type Cryptosystems
審査委員	（主査） 教授 若杉耕一郎 教授 柴山 潔　教授 三木博雄　大阪学院大学教授 笠原正雄

論文内容の要旨

本論文は高安全性が保証された情報記録・情報通信システムの構築に資するための手法について研究したものである。論文は以下に示す10章から構成されている。

第1章序論は本論文で遂行した研究内容に関する研究分野およびその背景を示している。

第2章では、有力な素因数分解法であるP-1法およびP+1法に対して高い耐性を有する素数を提案し、考察している。さらに、P-1法およびP+1法のいずれに対しても強い素数を効率的に生成する手法を新たに提案している。

第3章では、試行割算法を用いることなく、効率的に素数を生成する新たな手法を提案するとともに、P-1法およびP+1法に対して高い耐性を有する素数が生成可能となるように提案手法を改良している。

第4章では、合成数を法とする離散対数問題に基づいた結託攻撃に対して安全なID情報に基づく予備通信不要な鍵共有方式（ID-NIKS）を提案している。

第5章では、一般的なべき積型ID-NIKSに対する結託攻撃法を提案し、べき積型ID-NIKSは安全ではないことを明らかにしている。

第6章では、安全なID-NIKSに必要な条件を提示するとともに、積和型ID-NIKSに対して非線形な演算を導入することにより、結託攻撃に対して非常に高い耐性を有するID-NIKSを新たに提案し、その安全性について検討を行っている。

第7章では、従来知られていた森井・笠原暗号をもとに平文の重みを制限することにより、高いレートを実現する公開鍵暗号を提案するとともに、高速に暗号化処理が可能な改良方式を二つ提案している。

第8章では、基数を退化させるという手法を用いて高い密度を実現した新たなクラスの積和型暗号を提案している。

第9章では、まず、基本方式として多進基数に基づく積和型暗号を提案し、さらに、この提案暗号方式を用いて、暗号化に使用された公開鍵を特定できないことを安全性の根拠とする新たなクラスの公開鍵暗号方式（HP暗号）を提案している。

最後に、第10章は結論であって、情報記録・通信システムの安全性のために、本論文が寄与しうる事項を総括して述べている。

論文審査の結果の要旨

マルチメディア社会の進展とともに、安全性が保証された情報記録・情報通信システムを構築することが重要なテーマになっている。本論文は、暗号理論を基盤にして、高安全性を確保する手法について研究

したものである。すなわち、本論文は、暗号化の鍵を公開することを可能にした画期的な方式として、近年多くの注目を集めている公開鍵暗号方式について、主として、

（Ⅰ）公開鍵暗号使用の際に必要となる素数に関して詳細に考察し、安全な素数を効率的に生成する手法

（Ⅱ）公開鍵暗号のクラスのうち、一般に高速復号が可能な積和型公開鍵暗号に注目し、その安全性を（ⅰ）乗算型ナップザック法、（ⅱ）退化手法、（ⅲ）多進基数応用法により高める手法を提案し研究を進めている。

さらに、共通鍵暗号における秘密鍵共有プロセスの煩雑さを解決する手法として注目されているID情報に基づく予備通信不用の鍵共有方式（ID-NIKS）について（ⅰ）攻撃性、（ⅱ）合成数を法とする手法、（ⅲ）非線形変換手法を提案し、研究を進めている。

主な成果は次の通りである。

(1) P-1法およびP+1法の両者に対して強い1000ビットの大きさの素数を、従来法に比べ約6倍高速に求める手法を明らかにしている。

(2) 合成数を法とするID-NIKS法を提案し、本手法が計算量較差に基づく安全な手法であることを示している。

(3) べき積型ID-NIKSに対し、強力な攻撃法を提案するとともに新しいID-NIKSを提案し、この方式が提案結託攻撃に対し安全であることを示している。

(4) 従来の乗算型ナップザック暗号を改良した方式を提案しレートを大幅に改善している。

(5) 退化基数を用いることにより密度の高い積和型暗号を提案し、LLL攻撃に対し安全であることを明らかにしている。

(6) 暗号化鍵を自由に選択できる新しいクラスの公開鍵暗号について、多進基数を用いた手法を提案しLLL攻撃に対し安全であることを示している。

以上のように、本論文は情報記録・情報通信システムの高安全性を実現するための手法について研究し、それぞれについて新しい手法を提案するとともに厳密な解析を行っている。

本論文の主要な内容はレフェリーシステムある学術雑誌に掲載されたもの8編（うち本学紀要の論文1編）に基づいている。この掲載論文において、2編は申請者が筆頭著者であり、残る6編は2番目の著者である。

本学位論文作成の基礎となる学術論文は以下の通りである。

1．Yoshizo Sato, Yasuyuki Murakami and Masao Kasahara, "New Methods of Generating Primes Secure against Both P-1 and P+1 Methods," 電子情報通信学会英文論文誌 EA Vol. E82-A, No.10, pp.2161-2166 (1999年10月).

2．佐藤義三、村上恭通、笠原正雄、"素数の効率的生成法に関する考察," 電子情報通信学会論文誌 A Vol. J83-A, No.1, pp.125-128 (2000年1月).

3．村上恭通、笠原正雄、"合成数を法とする離散対数問題," 電子情報通信学会論文誌 A Vol. J76-A, No.4, pp.649-655 (1993年4月).

4．藤川篤則、村上恭通、笠原正雄、"べき積型ID-NIKSに対する攻撃法," 電子情報通信学会論文誌 A Vol. J80-A, No.2, pp.406-409 (1997年2月).

5．Yasuyuki Murakami, Ryuichi Sakai and Masao Kasahara, "A New Probabilistic ID-Based Non-interactive Key Sharing Scheme," 電子情報通信学会英文論文誌 EA Vol. E83-A, No.1, pp.2-9 (2000年1月).

6．Shinya Kiuchi, Yasuyuki Murakami and Masao Kasahara, "New Multiplicative Knapsack-Type Public Key Cryptosystems," 電子情報通信学会英文論文誌 EA Vol. E84-A, No.1, pp.188-196 (2001年1月).

7．Daishuke Suzuki, Yasuyuki Murakami and Masao Kasahara, "A New Product-Sum Type Public Key Cryptosystem Based on Reduced Bases," 電子情報通信学会英文論文誌 EA Vol. E84-A, No.1, pp.326-

330 (2001年1月).

8．Masao Kasahara and Yasuyuki Murakami, "New Public-key Cryptosystems Based on Arithmetic in Integer Ring," 京都工芸繊維大学工芸学部研究報告，第48巻　理工・欧文，pp.43-57 (2000年2月).