論 文 の 内 容 の 要 旨

論文題目　　New Tools for Factoring-based Cryptography
（素因数分解に基づく暗号における新たな手法）

氏　名　　山川 高志

現代社会において，暗号は安全な情報通信のために不可欠な技術となっている．暗号の歴史は少なくとも数百年以上前に遡ることができるが，1976年にDiffieとHellmanにより提案された公開鍵暗号の概念により大きな転機を迎えた．公開鍵暗号においては，復号の権限は秘密の復号鍵を持っている受信者に限られているのに対し，暗号化は誰でも自由に行うことができるという特徴を持つ．これにより，インターネット上における不特定多数との暗号通信が可能となり，現在では日常的に用いられている．また，公開鍵暗号の構成に用いられた手法は，ディジタル署名，認証，コミットメント等のより幅広い応用を持つことがわかってきている．現代暗号理論ではこれらの技術を総称して暗号プリミティブと呼び，これら全般の研究を扱う．

暗号プリミティブの安全性を保証するために一般的に用いられる手法として安全性証明がある．安全性証明とは，もし暗号方式が脆弱であったとすると，ある数学的に困難であるとされている問題が容易に解けるということを証明することである．これにより，元となる数学的な問題が実際に困難である限りにおいては，その暗号方式が安全であるということが数学的に保証されるため，安全性証明は暗号方式の安全性の強い傍証と言える．一方で，もし元となる仮定が偽であった場合，すなわち難しいとされていた数学的問題が実は容易に解けてしまう場合，もはや暗号方式の安全性は一切保証されない．したがって，より高い安全性を保証するためには，より信頼できる仮定に基づいて安全性証明を行うことが重要である．

現在暗号理論においては，素因数分解仮定，離散対数問題仮定，格子最短ベクトル仮定など様々な仮定が用いられている．これらの中で，素因数分解仮定，すなわち大きな合成数の素因数分解は困難であるという仮定は最も歴史が古い．素因数分解の困難性に基づく暗号方式は 1978 年に Rivest, Shamir, Adleman によって初めて提案され，以降数多くの解析がなされてきている．それにも関わらず，現在まで素因数分解問題を解く多項式時間アルゴリズムは提案されていない．したがって，素因数分解仮定は暗号理論において用いられる仮定の中でも特に信頼性が高いもののひとつであると言える．したがって，素因数分解仮定に基づいて安全性証明がなされる暗号方式は高い安全性を有しており，

その研究は重要である. 本論文においては素因数分解問題の困難性に基づく暗号プリミティブの構成を研究する. 本論文は大きく分けて二つに分けられる.

前半では補助情報付き自己双線形写像(AI-SBM)と呼ぶ暗号プリミティブについて述べる. 自己双線形写像とは, 定義域と値域が同一の群であるような双線型写像である. 自己双線形写像を用いれば, これを繰り返し用いることで多重線形写像へ拡張できることが容易にわかる. 近年多重線形写像は双線形写像をはるかにしのぐ多くの応用を持つことがわかってきており, したがって自己双線形写像も非常に有用なプリミティブであるといえる. 一方, Cheon と Lee は自己双線形写像の存在性に対して否定的な結果を示した. すなわち, もし既知素数位数の群上での自己双線形写像が存在するならば, その群の上では計算 Diffie-Hellman(CDH)仮定が成り立たないことを示した. CDH 仮定は群上での暗号方式の構成における最低限の仮定のひとつであるので, 上記の結果は, 暗号学的に有用な自己双線形写像に対する強い否定的な結果であると考えられる. そこで, 本論文では上記の否定的結果を回避するために位数が未知であるような群を考え, さらに自己双線形写像の定義を弱めた補助情報付き自己双線形写像(AI-SBM)を考える. 通常の自己双線型写像においては, 写像は入力のみから効率的に計算可能であることを要求する. これに対して, AI-SBM においては, 入力に加えてその入力に関する「補助情報」が与えられた時に写像が計算できればよいと定義する. そして, 素因数分解仮定と識別不可性難読化(iO)の存在のもとで AI-SBM の具体的な構成を与えた. その応用として, 多者間非対話鍵共有, 分散放送暗号, 属性ベース暗号, 準同型署名を構成した. 特に, 多者間非対話鍵共有および分散放送暗号方式はあらかじめユーザ数の上限を定める必要のない初めての方式である.

後半では攻撃者依存損失落とし戸関数(ad-LTDF)と呼ぶ暗号プリミティブについて述べる. 損失落し戸関数(LTDF)は 2008 年に Peikert と Waters により提案された暗号プリミティブである. 既存研究により, LTDF を用いることで, 衝突困難ハッシュ関数, 公開鍵暗号, 決定的公開鍵暗号等を含む様々な暗号プリミティブが構成できることが知られている. また, 素因数分解の困難性に関連した LTDF の構成として, QR 仮定や DCR 仮定に基づくもの等がしられている. しかし, これらの仮定は素因数分解仮定自体よりも強い仮定であり, 素因数分解仮定のみを用いた LTDF の構成は知られていない. そこで, 本研究では LTDF の定義を弱めた攻撃者依存損失落し戸関数(ad-LTDF)と呼ぶ概念を提案した. ad-LTDF は LTDF よりも弱いプリミティブであるが, 多くの応用において LTDF と同様に用いることができることを示した. また, セミスムース部分群 RSA 数(SS 数)と呼ばれる特殊な構造を持った合成数に関する素因数分解仮定のもとで ad-LTDF を構成した. その結果, 既存の LTDF を用いた暗号プリミティブの構成において, 単に LTDF を ad-LTDF で置き換えることで, 衝突困難ハッシュ関数, 公開鍵暗号, 決定的公開鍵暗号の新たな構成を得た. 特に, こうして得られた決定的公開鍵暗号は素因数分解仮定のもとで Boldyreva らにより定義された安全性を満たす初の方式である. また, 類似の手法を用いることにより, 暗号文サイズの小さい選択暗号文攻撃に対して安全な公開鍵暗号方式を構成した. この方式の暗号文サイズは, 素因数分解仮定に基づく方式の中で最小である.