論文審査の結果の要旨

氏名　　山川　高志

本博士論文は全五章からなる．第一章は序章で，第二章では必要な諸定義がなされている．第三章では補助情報付き自己双線形写像と呼ばれる新たな暗号要素技術が定義され，その構成と応用が述べられている．第四章では攻撃者依存損失落し戸関数と呼ばれる新たな暗号要素技術が定義され，その構成と応用が述べられている．第五章では，論文の総括と，いくつかの未解決問題の提起がなされている．

現代暗号理論においては暗号の安全性を客観的に保証するために安全性証明を行うことが必須であるとされている．安全性証明においては様々な仮定が用いられるが，その中でも素因数分解仮定は最も歴史が長く信頼性が高いものであると言える．したがって，素因数分解仮定に基づく安全性証明は非常に強い安全性の保証を与えると言える．一方，素因数分解仮定に基づく構成が知られていない暗号要素技術は数多く存在し，それらの構成を与えることは重要な問題である．本博士論文では新たな暗号要素技術を中間技術として用いることでこの問題を部分的に解決した．

第三章では補助情報付き自己双線形写像の構成と応用について述べる．群 G 上での写像 $e:G\times G\to G$ が自己双線形写像であるとは，任意の整数 a, b, X, $Y\in G$ に対して $e(X^a,Y^b)=e(X,Y)^{ab}$ を満たすことである．ある種の計算量仮定を満たす自己双線形写像は暗号学的に非常に有用であることが知られている一方，その存在には否定的な結果が知られている．そこで，本論文では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を導入した．これは，効率的な計算のために写像の入力に加えて補助情報が必要となるような自己双線形写像である．そして，素因数分解仮定と識別不可性難読化を用いて補助情報付き自己双線形写像の構成を与えた．また，その応用として，多者間非対話鍵共有，放送暗号，属性ベース暗号，準同型署名の新たな構成を与えた．特に，こうして得られた多者間非対話鍵共有および放送暗号方式はユーザ数の上限をあらかじめ指定しておく必要のない初めての方式である．また，同様のアイディアを用いることで，Φ 秘匿仮定と識別不可性難読化を用いて NC^1 回路が評価可能な準同型暗号方式を構成した．

第四章では攻撃者依存損失落し戸関数の定義，構成および応用について述べる．損失落し戸関数は 2008 年に Peikert と Waters により提案された暗号要素技術であり，様々な暗号要素技術の構成に応用できることが示されている．損失落し戸関数は様々な仮定から構成できることが知られている一方で，素因数分解仮定に基づく構成は知られていなかった．本論文では損失落し戸関数の定義を弱めた攻撃者依存損失落し戸関数を定義した．これは損失関数の生成アルゴリズムが識別攻撃者に依存することを許すような損失落し戸関数である．そして，セミスムーズ部分群 RSA 数と呼ばれる形式の合成数に関する素因数分解仮定のもとでその構成を与えた．また，攻撃者依存損失落し戸関数は多

くの応用において通常の損失落し戸関数と同様に用いることができることを示した．その結果，衝突困難ハッシュ関数，公開鍵暗号，決定的公開鍵暗号の素因数分解仮定に基づく新たな構成を与えた．特に，こうして得られた決定的公開鍵暗号方式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定義を満たす初めての方式である．また、同様のアイディアを用いることで，セミスムーズ部分群 RSA 数に対する素因数分解仮定に基づく暗号文の短い選択暗号文攻撃に対して安全な公開鍵暗号方式を与えた．この方式の暗号文長は同様の仮定に基づく構成の中で最短である．

本論文の第三章と第四章は山田翔太，花岡悟一郎，國廣昇との共同研究であるが，論文提出者が主体となり貢献を行っている．そのため，論文提出者の寄与が十分であり，博士（科学）の学位を授与できると認める．

以上１６１２字