審査の結果の要旨

氏名　　勝又　秀一

本博士論文は全七章からなる．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．近年，クラウド技術や計算機技術の発展に伴い，公開鍵暗号や電子署名のような従来の暗号方式と比べ，より高機能な暗号方式が求められるようになってきた．一般的な傾向として，機能性と安全性はトレードオフの関係にあり，暗号方式がより高機能になるに従い，安全性が低下する．しかし，現実利用の観点から見た場合，安全，かつ，高機能な暗号方式が社会的に求められる．本博論に収録されているいずれの結果も，特定の高機能な高機能暗号方式の安全性強化手法に関するものである．

各章の詳細に入る前に，強い安全性の概念について記す．安全性には大きく分けて三つある．一つは，仮定する数学的問題が計算問題か判定問題かである．二つ目は，問題が静的であるか動的であるかである．最後は，問題が耐量子性を備えているかどうかである．このとき，仮定する問題が計算問題で，静的で，かつ，耐量子性を備えている場合の方がそうでない場合と比べ安全性が高い．以下，この安全性の指標の元，各章の内容の詳細について簡潔に説明する．

第三章と第四章では，ID ベース暗号（IBE）に関する成果を扱う．IBE とは，代表的な高機能暗号の一種で，e-mail アドレスなどのような ID（個人の識別子）を公開鍵として利用できる暗号技術である．第三章では，現在もっとも効率的な耐量子性を備えた IBE 方式に従来とは異なるテクニックを用いることで，より緊密な安全性証明を与えた．安全性証明が緊密であることにより，大幅なパラメータ改善を図ることができ，効率性を高めることに成功している．第四章では，分割関数と呼ばれる IBE の構成に用いられる道具の普遍的特徴を抽出し，非線形多項式によって分割関数を表現する一般的手法を確立した．この手法を用いることにより，代数的性質が大きく異なる格子とペアリングの二つの道具から，統一的なアプローチで IBE を構成した．特に，ペアリングを基にした構成は，計算問題を仮定した IBE の構成の中で最も効率的，かつ，安全な方式である．

第五章では，格子に基づく述語暗号とペアリングに基づく検証可能擬似乱数関数に関する成果を扱う．述語暗号とは，暗号文の緻密なアクセス制御を可能にする暗号方式で，検証可能擬似乱数関数とは，誰かが乱数を生成したときに，その乱数を正しく生成したことを第三者が検証できる暗号方式である．一見両者は接点のない暗号方式に見えるが，どちらの構成も部分集合述語と呼ばれる特殊な関数を利用しているという共通点を持つ．本成果は，従来の部分集合述語の計算方法（論理回路や分岐プログラム）を算術回路に置き換え，さらに，述語の関数として取りうる値を変更することにより，部分集合述語の高速かつ効率的な計算方法を提案したことである．このアイデアは，ある特定の高機能暗号方式に特化した手法ではなく，部分集合述語を構成に用いる多くの高機能暗号方式に適応可能である．

第六章では，非ゼロ内積暗号（NIPE）に関する成果を扱う．NIPE は，上述の述語暗

号の一種で，アクセス制御が特殊な線形関数で記述できる場合に利用でき，執行機能付きの IBE などへの応用がある．この章では，NIPE の構成方法を新しく二つ提案する．一つ目は，格子暗号に特化した構成になっており，多次元格子における離散ガウス分布を重ね合わせたときの理論解析を駆使することで，従来よりも効率的な NIPE の構成を与えた．離散ガウス分布は連続ガウス分布と比べ，未解明な性質が多く，この結果は離散ガウス分布の暗号理論への応用の幅を広げると期待される．二つ目は，内積値を計算する関数型暗号（LinFE）からの NIPE の一般的構成手法の提案である．LinFE は近年活発に研究が行われている暗号方式であるため，LinFE の最新の構成を用いることにより，効率的，かつ，安全性が高い NIPE を構成できる．

第七章は，格子に基づく属性ベース署名（ABS）の構成である．ABS とは，一般の電子署名にアクセス機構を付与し，アクセス権限を与えられている文書にのみユーザが署名生成ができるという暗号方式である．この章では，まず，格子に基づく特定の言語に対するゼロ知識証明（NIZK）を提案し，その提案した NIZK を基に耐量子性を備える初めての ABS を構成した．格子に基づく NIZK は様々な暗号方式に利用される基礎技術の一つであるため，この結果はこの章で新しく構成した属性ベース署名以外にも数多くの暗号方式に影響を与える．

本論文には，山田翔太，山川高志，Ali El Kaafarani との共同研究も含まれているが，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 1907 字