論文審査の結果の要旨

氏名　吉野　雅之

本博士論文は九章から構成されている．第一章では，研究全体の位置づけとして，格子問題および隠れ部分群問題に基づく暗号化技術の研究が，今後の計算機環境においては非常に重要であり，かつどちらか一方の研究だけでは不十分であることが述べられている．基本的な暗号化／復号機能に加え，格子問題に基づく暗号化技術は暗号文同士の演算が実行可能な準同型暗号に関係し，また隠れ部分群問題に基づく暗号化技術は暗号化したまま条件判定を可能とする述語暗号に関係する．暗号化技術では，情報の秘匿性を数学的に保証する為に安全性証明技法が広く使われているが，本研究では特に安全性の根拠となる格子問題と隠れ部分群問題の計算量的困難性に着目し，それらの数論仮定を十分に検証した上で，各暗号化技術の安全性を数学的に証明している．第二章から第五章は隠れ部分群に基づく述語暗号の安全性と効率性について述べられている．述語暗号とは，情報を暗号化したまま，論理和（OR）や論理積（AND）などを用いた条件判定を第三者に委託可能な暗号化技術である．これまでの暗号化技術では対応できなかった，クラウドコンピューティング等の複数の組織に渡る計算機環境でも，情報漏洩を防止可能な技術として実利用が有望視されている．以降では，簡便のため，暗号化した情報を暗号文とし，暗号化した条件判定を暗号化トークンと呼ぶ．本研究の目的は，十分に計算量的困難性が保証された数論仮定の下で，暗号文と暗号化トークンが最高レベルの安全性（多項式時間で構成された任意の攻撃者に対し，暗号文と暗号化トークンから元の情報が 1 ビットも漏洩しない）を有する述語暗号の設計にある．これまでに提案された述語暗号のほとんどは，暗号文の安全性のみに着目し，暗号化トークンの安全性は不十分であった．例えば，近年（2000 年以降）盛んに研究されている述語暗号は，総じて，暗号化トークンが頻度分析を行う攻撃者に対して脆弱である．また，暗号化トークンの安全性を証明した述語暗号も存在はするものの，肝心の数論仮定が特殊な隠れ部分群問題に帰着しているため，その計算量的困難性が不十分であり，解読される危険性が高い．本博士論文では，これらの研究動向を鑑み，まず取り扱う数論仮定の計算量的困難性を証明した上で，その数論仮定に基づく述語暗号を新たに設計し，暗号文と暗号化トークン双方の安全性を数学的に証明している．また，設計した述語暗号を別の数論仮定に帰着させた場合，IC チップ等の計算能力に乏しい小型機器でも軽快に動作できるまで計算量を削減できることも示している．第六章と第七章は，暗号文同士の演算が実行可能な準同型暗号の数論仮定において，代表的な格子問題である最短近似ベクトル問題の計算量的困難性を高速に検証可能な解読アルゴリズムについて述べられている．最短ベクトル問題は，複数本の線形独立なベクトルが与えられた時に，線形結合により，ゼロベク

トルを除いた最も短いベクトルを発見する問題である．ただし，線形結合するベクトルの係数は整数とし，ベクトルの長さをユークリッドノルムで評価する．最短ベクトル問題は NP 困難性が証明されている一方，その近似解（以降，最短近似ベクトル問題と呼ぶ）は近似度合によっては多項式時間で解読可能なことが知られている．本博士論文では，安全性証明における数論仮定に最短近似ベクトル問題を利用できるよう，その計算量的困難性を評価する検証アルゴリズムを設計している．具体的には，従来研究で報告された検証アルゴリズムの中でも計算効率の高さで優位性があるランダムサンプリング法に事前計算を適用し，より高速なアルゴリズムを設計できることを証明している．その結果，最短近似ベクトル問題の線形独立なベクトルの本数の自乗に比例していた計算量が，利用者が設定可能なパラメータのその対数の積の自乗に抑えられており，大幅に計算量が改善されている．第八章は，安全性の根拠とする数論仮定に最短近似ベクトル問題を用い，暗号文の加減算と乗算を第三者に委託可能な準同型暗号について述べられている．本博士論文では，検証アルゴリズムによって安全性が保証された最短ベクトル問題を数論仮定とし，暗号文の安全性が保証された準同型暗号を設計している．具体的には，数論仮定に用いた最短近似ベクトル問題が従来の検証アルゴリズムでは解読不可能であることを示した上で，その最短近似ベクトル問題に安全性が帰着可能な準同型暗号を新たに設計している．

本論文第二章から第五章は，佐藤尚宜，長沼健，國廣昇との共同研究，第六章から第八章は，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おり，論文提出者の寄与が十分であると判断する．したがって，博士（科学）の学位を授与できると認める．

以上１９６５文字