審査の結果の要旨

氏名　イン　ホェイ　ミン　ジェイソン

本博士論文では，暗号プリミティブにおける様々な状況下での計算困難性を議論している．暗号技術を安全に利用するためには，その暗号の安全性だけでなく，安全性を保証する基礎的問題の困難さも，徹底的に検証されなくてはならない．本博士論文では，いくつかの基礎的問題に対して，その問題を解く計算量に関する研究を行い，その結果を踏まえて，実際の暗号方式の安全性評価を与えている．

本博士論文は全五章からなる．第一章は序章である．第二章では，複数離散対数問題の困難さに関して議論し，第三章では，効率的な認証方式の安全性評価を与え，第四章では，パスワード復元に要する計算量を削減するアルゴリズムの提案を行っている．第五章では，論文の総括を与えている．

以下，これらの内容の詳細について説明する．

第二章では，複数離散対数問題の困難さについて議論している．暗号化方式，電子署名を含め多くの暗号方式は，離散対数問題（DLP）の困難さに安全性の根拠をおいている．これまでに，DLP および k-MDLP（k 個の離散対数問題全てを解く問題）を解く汎用アルゴリズムに関して多くの結果が知られている．Shoup は，DLP を解く汎用アルゴリズムの計算量の下限を示している．BSGS 法はその下限を達成しているため，現在知られている汎用アルゴリズムは，漸近的に最適である．k-MDLP に関しては，rho 法の拡張が提案されており，k-MDLP を解く汎用アルゴリズムの下限は，Yun によって示されている．

本論文では，一般化複数離散対数問題（GMDLP）を導入し，この問題を解くことの困難さについて研究を行っている．この問題は，k 個の離散対数のうち解 n 個を求める問題である．まず，k が大きい時の GMDLP を解く汎用アルゴリズムの計算量の下限を求めている．この結果は，全ての k に対して，GMDLP を解く計算量の下限を与えていることになり，Yun の結果の一般化とみなせる．具体的には，GMDLP を解く二つの手法を提案している．一つ目の手法は，k が小さいときに漸近的に緊密な限界を達成している．さらに，問題サイズが変化するときのトレードオフも解析している．二つ目の手法は，大きな入力に適用可能である．さらに，この手法で示したブロック分割が最適であり，n が k に対して比較的小さい場合も，求めた限界が漸近的に緊密であることを示している．

第三章では，認証方式の安全性評価を与えている．GPS 認証方式は，秘密鍵が低ハミング重み積であり，証明者が要求する計算コストが比較的小さいという特徴を持つ．この方式に対して，Coron らは，分割システムを用いた攻撃を示し，安全なパラメータセット（CLP パラメータ）を提案している．Kim らは，パラメータ化された分割システムを導入し，CLP パラメータに対する攻撃の効率化に成功している．

本論文では，パラメータ化された分割システムの考え方を拡張し，パラメータ依存分

割システムの概念を導入し，低ハミング重み積を指数に持つ様々な離散対数問題を解く一般的な方法を提案している．さらに，CLP パラメータを持つ GPS 認証方式に対して，実際の攻撃アルゴリズムを二つ提案している．最初のものは，メモリ量を増加させずに，既知のものより小さい計算時間で解読に成功するアルゴリズムである．二つ目のものは，GPS認証方式が2の64乗未満の計算量で破られること示した初めての攻撃手法である．この研究成果は，低ハミング重み積を指数に持つ離散対数問題に基づく暗号方式が安全に利用するための設計指針を与えている．

第四章では，パスワード復元に要する計算量を削減するアルゴリズムの提案を行っている．パスワードを平文で保存する場合，パスワードファイルが漏洩したときには，安全性が損なわれる．そのため，多くの場合，暗号学的ハッシュ関数を用いて，パスワードのダイジェストを格納している．ハッシュ値の逆元を求め，パスワードを回復する方法として，全数探索，時間メモリトレードオフを用いた方法など，多くの方法が提案されている．

本論文では，一般にパスワードは一様に分布しておらず偏りがある，パスワードは，様々なデータベースにわたって同一である傾向があるという事実を用いて効率化を実現している．従来の研究では，単一のレインボーチェーン内に割り当てたパスワードが少数の状況しか解析されていないが，多くのパスワードを組み込む方式を提案し，さらに，頻繁に使用されるパスワードをレインボーチェーンに組み込むことにより，オンラインフェーズでのパスワード復元時間が短縮されることが示した．

本論文の第二章，第三章，第四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１９８６字