論文審査の結果の要旨

氏名　　山田　翔太

本博士論文は全六章からなる．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，第四章では電子署名をはじめとした各種暗号技術の効率性を改善する研究において得られた結果が記述されている．一方，第五章では，述語暗号の安全性を高める方法が記述されている．第六章では，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．現代の情報化社会を支える暗号技術が，有用であるためには，その暗号技術が，実用に十分な効率性と安全性を兼ね備えている必要性がある．一方で，暗号技術は安全性を高めると効率性が低下し，効率性を高めると安全性が低下する傾向があり，両者の性質を兼ね備えた暗号方式の設計は困難である．本博論は，大きく分けて二つの研究結果によって，この状況の改善を図った．一つ目の研究結果では，従来の暗号技術を，安全性を落とさずに効率性を改善した(第三章，第四章)．二つ目は，従来の暗号技術を，効率性をほとんど落とさずに，安全性を改善した(第五章)．以下，これらの内容の詳細について説明する．

第三章では，まず，二次元的なカバーフリーファミリーの利用法という新しいテクニックを導入している．カバーフリーファミリーとは，ある組み合わせ論的な有用な性質を持つような集合族で，数多くの暗号方式の設計に利用されてきた．本博論で提案しているテクニックでは，カバーフリーファミリーと，双線形写像を組み合わせることによって，従来よりも公開鍵長あるいは暗号文長の短い q-耐性を持つ ID ベース暗号や，q 回使い捨て署名，q-制限付き選択暗号文攻撃に対して安全な公開鍵暗号を提案している．

上記とは別に，署名長の短い電子署名方式設計のための新しい方法論も提案した．具体的には，q-回使い捨て署名と，弱安全な電子署名を組み合わせることによって，署名長の短い電子署名方式を得る方法論を提示した．これは，従来の，プログラム可能ハッシュ関数と弱安全な電子署名を組み合わせることで存在的偽造不可能性を満たす電子署名方式を設計するという方法論の拡張となっている．また，この方法論と，上記で提案した二次元的なカバーフリーファミリーの利用法を組み合わせることによって，現存する方式の中で最短の署名長を達成しており，また，同じ署名長を満たす従来方式に比べて公開鍵長が非常に短くなっているような署名方式を提案した．

第四章では，第三章で提案した署名長の短い電子署名方式設計のための方法論を，RSA 合成数位数群の上でも実現した．具体的には，効率的な q 回使い捨て署名方式を疑似ランダム関数の性質を利用して設計し，これを既存の RSA 合成数位数群上の弱安全な電子署名方式を組み合わせることによって，新たな電子署名方式を設計した．第四章ではこの方針に従って複数の方式が提案されているが，その中の一つの方式は，現存する電子

署名方式の中で，公開鍵長，署名長ともに最短である．

第五章では，述語暗号の安全性を高める汎用的な変換法を示した．述語暗号とは，暗号文と秘密鍵に属性が付与されており，それらがある条件を満たすときに復号が可能になるような暗号技術である．本博論で提案した変換法は，具体的には，検証可能性という性質と，いくつかの自然な性質を見たし，さらに選択平文攻撃に対する安全性という弱い安全性を満たす述語暗号を，選択暗号文攻撃に対する安全性というより強い安全性を持つ述語暗号へ変換するものである．この変換法は，多くの既存の述語暗号に適用可能である．また，匿名否認可能述語認証という新しい要素技術を提案し，上記変換法を通して得られる述語暗号を用いてこれが構成可能であることを示した．匿名否認可能述語認証は，証明者がある条件を満たす属性を持つことを検証者に，自分の属性がその条件を満たすということ以上の情報を漏らさずに証明することを可能とする認証方式である．さらに，証明者は，検証者と過去に通信した事実を否認することが可能である．そのため，この技術は，内部告発などを安全に行うために有用であると考えられる．

本論文の第三章と第四章は花岡悟一郎，國廣昇との共同研究，第五章は，Nuttapong Attrapadung，Bagus Santoso，Jacob C. N. Schuldt，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１８３４字