審査の結果の要旨

論文提出者氏名　　張　鋭

本論文は「On The Security Of Multiple Encryptions（多重暗号化の安全性に関する研究）」と題し，高い安全性を持ち効率的な暗号プロトコルの構成に不可欠な多重暗号化の安全性に関する，評価・解析を行ったものである．特に

①一般的な構成手法に固有の安全性問題

②安全性の定義（厳密なモデルと安全性評価手法）

③選択暗号文攻撃に対し安全な方式の構成手法

の三つの観点から詳細な考察を行っている．

多重暗号化は従来の暗号化方式の拡張であり，暗号の国際標準においても従来の暗号に長期的な安全性を付与する方式として推奨されている．また，暗号プロトコルの汎用的な構成手法の一つとして，理論・実用上の両面において極めて重要な基礎技術であることが知られている．しかし，必要な安全性を厳密に定義できるモデルや，選択暗号文攻撃に対し安全な多重暗号化方式の構成手法などは，これまで未解決であり，多重暗号理論の整備が急務の課題とされていた．本論文は，これらの課題に対し厳密な考察を行い，有効な解決策を示したものである．本論文は「Introduction」を含めて7つの章から構成されている．

第1章「Introduction（序論）」では，本研究の背景を明らかにし，研究の動機と目的について言及し研究の位置付けについて整理している．

第2章「Model and Security Definitions（モデルと安全性定義）」では，多重暗号化のモデルを厳密に定義している．具体的には，①鍵を漏洩するオラクルを導入し，②強秘匿性（Indistinguishability）と頑強性(Non-Malleability)，および弱選択暗号文攻撃（weak Chosen Ciphertext Attack）と弱頑強性(generalized Non-Malleability)に基づく定義を行っている．

第3章「Relations among Security Notions（安全性定義の関係）」では，多重暗号のモデルを定式化し，多重暗号のための安全性の概念を理論的に整備した．安全性の概念の理論的整備については，さまざまな安全性概念の間の関係を明らかにすると共に，安全性証明に必要な概念を簡単な操作で扱う手法を示す．

第4章「Secure Constructions（安全な構成手法）」では，前章で定義した安全性を満たす多重暗号が存在するかどうか，また，存在するとすれば，どのようにそれを実現できるか，という実際的に二つの問題に対し，肯定的な解答を与えている．ここでは，ランダムオラクルを仮定した定式化を行うだけでなく，ランダムオラクルを仮定しないスタンダードモデルにおいてもその定式化が可能なことについて詳細に説明している．

第5章「Multiple Encryption with Fewer Keys（より少ない鍵を使った多重暗号）」では，構成要素となっている各暗号方式の数より秘密鍵が少ない場合の多重暗号方式のモデルを示し，さらに三つの汎用的な構成手法を提案している．また，この手法の応用として，IDベース暗号を考察し，そこで未解決問題であった帰着効率についても，双線形DH判定問題に基づく手法を用いて解決した．

第6章「Applications（応用）」では，多重暗号化技術を使った，さまざまな応用例を挙げている．具体的に，鍵隔離暗号，閾値暗号，証明書に基づく暗号（証明書不要暗号），放送暗号，耐解読暗号，キーワードサーチ可能な公開鍵暗号，代理暗号，ミックスネット，オニオンルーチングなどについて，汎用的な構成法を提案した．特に，鍵隔離暗号については，選択暗号文攻撃に対し安全な汎用的構成法を初めて提案している．また，あわせて閾値暗号についても考察を行い，従来手法より効率のいい方式の導出に成功している．

第7章は「Conclusion（結言）」で，本研究の総括を行い将来の展望について述べ，本論文をまとめている．

最後に，付録では並列多重暗号と密接な関係があるAll-or-Nothing と呼ばれるある種の秘密分散

方式を用いた暗号システムの安全性について解析を行っている.

以上これを要するに, 本論文は, 多重暗号化の安全性に関する基礎検討, 厳密なモデルとそれに基づく安全性の定義, およびその理論的整備を行い, その応用として汎用的かつ安全な暗号プロトコルの構成手法を示したものであり, 電子情報学, 特に情報セキュリティ工学上貢献するところが少なくない.

よって本論文は博士 (情報理工学) の学位請求論文として合格と認められる.