審査の結果の要旨

論文提出者氏名　　ナシメント　アンダーソン

本論文は「Bounds and Constructions for Mutually Distrustful Information Theoretically Secure Cryptographic Protocols （情報論的に安全な暗号プロトコルの理論的考察）」と題し，二者間あるいは多者間で，相互に信頼しなくても，また，いかなる計算量的仮定を置くことなく安全に実行できる暗号プロトコルの理論的限界と構成法に関し，コミットメント容量などの新たな概念を導入し，それらに基づきプロトコルの効率などに対する理論的限界を導出するとともに，新たな暗号プロトコルを提案したものである．論文の構成は，「序論」「結言」を含めて8章からなる．

第1章は「Introduction（序論）」で，本研究の背景を明らかにした上で，研究の動機と目的について言及し，本論文の構成について述べている．

以下の第2章から第7章までは三つの部分に分けられ，それぞれが二つの章からなる．最も基本的な暗号プロトコルとしてコミットメントと紛失通信（Oblivious Transfer）とがあるが，第 2 章，第 3 章ではコミットメントを，第 4 章，第 5 章では紛失通信を，そして第 6 章，第 7 章では一般のプロトコルをそれぞれ扱っている．

第2章は「Commitment Capacity of Discrete Memoryless Channel（離散無記憶通信路のコミットメント容量）」と題し，まず誤りのある離散無記憶通信路によって，情報量的に安全なコミットメントが実現できることを証明する．ついで，コミットメントできる情報量の限界を与えるコミットメント容量の概念を導入し，これが簡潔な式により表現できることを示す．これらの結果は量子通信路に対しても拡張できる．

第3章は「Pre-distributed Commitment（事前分散コミットメント）」と題し，事前に分散されたデータに基づく情報量的に安全なコミットメントについて，その限界を一般的に証明している．これは，基本的な分散型の暗号プロトコルの一つであり，それについての最も重要な未解決問題を解決したと言うことができる．

第4章は「Oblivious Transfer from any Genuine Noise（真性雑音による紛失通信）」と題し，雑音のある通信路において，情報量的に安全な紛失通信を実現するための必要十分条件について考察し，0でない雑音が存在する通信路では，紛失通信を実現できることを証明している．これは，15 年以上にわたる暗号学の未解決問題を解決したものである．

第5章は「Oblivious Polynomial Evaluation（紛失多項式評価）」と題し，もう一つの基本的分散型暗号プロトコルである情報量的に安全な紛失多項式評価について，それを実現するための通信量の下限を導き，それを達成する具体的プロトコルを提案している．

第 6 章は「Secure Two-Party Computations（安全な二者間計算）」と題し，二者間の計算を安全に実現するために，相関のあるデータに基づいた情報量的に安全な一般的暗号プロトコルを提案している．

第 7 章では「Secure Multiparty Computations and Verifiable Secret Sharing（安全な多者間計算と証明可能な秘密分散）」と題し，第 6 章の結果を多者間の場合に一般化している．

最後に第8章は「Conclusion（結論）」で，本研究の総括を行い，併せて今後解決すべき課題について述べている．

以上これを要するに，本論文は，情報量的に安全な暗号プロトコルに関し新しい概念を導入するとともに，それに基づいて，重要な未解決問題を解決し，情報量的に安全な暗号プロトコルの基礎理論を確立したものであり，これらの研究成果は電子情報学，特に情報セキュリティ分野に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．