# 論文審査の結果の要旨

氏名 Taniguchi, Elliot Tadashi

本論文は「The Design and Analysis of Secure Communication Systems Distributed Over Broadcast Channels（放送型通信を利用した安全な通信システムの設計と解析）」と題し、6章から構成されている。放送やネットワークを通して、情報サービスの配信やネットオークションが既に実用化されているが、今後ますますきめ細かいサービスや安全性が必要となる。本論文では、放送型通信を用いて、効率よくかつ安全に暗号化鍵を配信あるいは共有するためのプロトコルや、安全でかつ落札価格を部外者に信頼できる形で伝えることができないネットオークションを実現するプロトコルを提案し、その安全性を理論的に解析している。

第1章「Introduction」では，本論文で取り扱う放送型通信を用いた情報セキュリティシステムに対する研究の背景と目的を述べると共に、本論文の構成を示している。

第2章「Mathematical Foundations and Cryptographic Tools」では，暗号理論で用いられる代数の基本定理、本論文で仮定する計算困難問題（因数分解問題や離散対数問題）を示すと共に、本論文で必要となるハッシュ関数，公開鍵暗号，署名方式，ゼロ知識証明などを紹介している。

第3章「Broadcast Encryption」では、放送型通信を通して、ユーザで異なる多種類の情報を多くのユーザに配信するためのセッション暗号鍵配布方式を取り扱っている。 情報配信サービスは、多くの場合階層構造になっている。その階層構造を利用して、上位サービスのマスター鍵を配送すれば全ての下位サービスのセッション鍵を安全に作成・更新ができる暗号方式を本章で提案している。マスター鍵を一定期間ごとにリセットするが，途中でのユーザの加入や脱退を許さない方式に加えて、任意の時刻に脱退のみ，加入のみ，および加入と脱退を許す方式の構成法を与えている。安全性は離散対数問題の困難さに根拠を置いており、提案したシステムの安全性を理論的に解析している。

第 4 章「Deniable Key Establishment」では，匿名性を保持した鍵共有方式を提案している。ネットワークを通して、アンケート調査や公開討論を行なうときに、匿名性を保持しつつ、回答する人があるグループに属していることを確証したい場合がある。本章では、そのような要求を満たすことができる暗号鍵の共有手法を提案している。グループの選定者が任意の人でよい場合と、選定者がそのグループに含まれていなければならない場合を取り扱っている。安全性は公開鍵暗号の安全性に根拠を置いているが、一部でハッシュ関数や離散対数を利用することにより、計算量を減らした方式も提案している。また、提案したシステムの安全性を理論的に解析している。

第５章「General Auction Schemes with Deniable Settlement」では，放送型通信を用いたネットオークション方式を取り扱っている。公平で信頼性のおけるオークションを実現するためには、オークションの落札価格を、全参加者に信頼できる形で伝える必要がある。しかし、参加者が落札価格を部外者に信頼できる形で伝えることができると、

オークションの手数料の支払いを逃れるために、その落札価格を参考にしたオークション外取引が増えてしまう問題がある。本章では、この問題を解決するために、オークションの正規の参加者には、各時刻の最大入札価格や落札価格を信頼できる形で伝えるが、オークション外の人にはそれらの情報が全く漏洩しないようにし、さらに、オークションの正規の参加者が入札価格や落札価格を部外者に伝えても、信頼できない情報になるというオークションシステムを実現している。なお、オークションへのユーザの登録時には、部分的に信頼できる登録マネージャーを仮定しているが、登録マネージャー以外には信頼できる第３者を必要としない特徴がある。また、通常のオークションで必要とされる「入札者の匿名性」「登録マネージャーと競売者の協力の下での、不正者の追跡可能性」「入札の公平性」などの安全性も満たされていることを理論的に解析している。さらに、上記のような公開入札(open-price auction)の代わりに、封印入札(sealed-bid auction)に提案方式を用いる場合のプロトコルも示されている。

第6章「Conclusions」では、本論文の成果をまとめると共に、今後の研究課題を示している。

なお，本論文の成果は、山本博資との共同研究であるが、論文提出者が主体となって新しい情報セキュリティシステムの提案および解析を行なったものであり、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。