氏　名	長尾　若

（論文内容の要旨）

本論文は，暗号理論における鍵共有，データ暗号化，3つの暗号化チャネルの汎用的結合可能性について研究した結果をまとめたものであり，8章から構成されている．

第１章は序論であり，本研究の目的とその内容について概観している．

第２章では，本研究の準備について述べている．また，ハイブリッド暗号を構成する公開鍵（PKE），鍵共有（KEM）とデータ暗号化（DEM）について，その定義を述べている．本章ではハイブリッド暗号の構成について説明し，本研究が対象とする鍵共有およびデータ暗号化の定義とすでに提案されている安全性についての定義を述べている．また，これまでの公開鍵暗号に関する結果についても報告するとともに，他者研究者による弱い安全性定義の結果と本研究との差異についても説明している．

第３章では，汎用的結合可能性（UC）の説明を述べている．このモデルでは，2つの世界を区別しようとする環境によっても，確率的多項式時間内で差異が見出せないことを証明して安全性を示す．さまざまな暗号プロトコルが理想機能として定義され，各機能を組み込んだプロトコルの安全性が成り立つことを示す定理についても述べている．また，攻撃者のモデル（適応的，能動的など）の定義についても述べており，汎用的結合可能性のフレームワークについて網羅した説明を述べている．

第４章では，非決定性を扱えるタスク構造確率的入出力オートマトン（task-PIOA）について説明を延べている．この手法では，3章の汎用的結合可能性フレームワークでは扱うことのできない特別なスケジュールにおいて暗号プロトコルの安全性を証明できる．このフレームワークを用いることで，3つの暗号チャネルである，セキュアチャネル（Secure Channel），２者匿名チャネル(Two-Anonymous Channel)，方向不明チャネル(Direction Indeterminable Channel)の相互等価性について証明が可能となる．本章では，タスク構造確率的入出力オートマトンの定義とスケジュールについて説明し，タスク構造確率的入出力オートマトンのフレームワークについて網羅した説明を述べている．

第５章では，鍵共有とデータ暗号化の安全性定義を定義し，それらの関係性について示している．鍵共有については，3つの頑強性と攻撃手法を定義し，3つの頑強性定義が等価であること，頑強性よりも弱いと信じられていた強秘匿性と頑強性が適応的選択暗号文攻撃の下で等価になることを証明している．この証明により，適応的選択暗号文攻撃における強秘匿性が最も強い安全性定義であることがわかった．また，データ暗号化について，強秘匿性と頑強性，それぞれの攻撃方法について定義し，強秘匿性と頑強性について，適応的選択暗号文/平文攻撃の下で等価性が成り立つことを証明している．

第６章では，汎用的結合可能性における鍵共有とデータ暗号化の理想機能の定義を提案し，汎用的結合可能性における鍵共有機能が，上記で定義される最も強い安全性定義である選択暗号文攻撃における強秘匿性と等価であることを証明している．この証明により，汎用的結合可能性を満たすには，現在最も強い安全性である選択暗号文攻撃における強秘匿性が必要であることがわかった．また，データ暗号化についても，汎用的結合可能性におけるデータ暗号化機能が現在最も強い安全性定義である選択暗号文/平文攻撃における強秘匿性と等価であることを証明している．この証明により，汎用的結合可能性を満たすには，現在最も強い安全性である選択暗号文/平文攻撃における強秘匿性が必要であることがわかった．

第７章では，3つの暗号チャネルである，セキュアチャネル(SC)，２者匿名チャネル(2AC)，　方向不明チャネル(DIC)の理想機能の定義を提案している．また，タスク構造確率的入出力オートマトン上での定義もそれぞれ提案している．そして，各チャネル間で等価性が成り立つことを証明している．この等価性は4つの帰着により成り立つ．①方向不明チャネルから２者匿名チャネルへの帰着②２者匿名チャネルから方向不明チャネルへの帰着③方向不明チャネルからセキュアチャネルへの帰着④セキュアチャネルから方向不明チャネルへの帰着である．これらの帰着をタスク構造確率的入出力オートマトンのフレームワークを用いて証明している．また，方向不明チャネルと２者匿名チャネルとの間，方向不明チャネルとセキュアチャネルとの間の等価性はあるスケジュールをランダムに動かせるといった特定のスケジュール上で成り立つことを証明している．この証明により，現在良く使用されているセキュアチャネルの代替として２者匿名チャネルや方向不明チャネルを用いることが可能である．

第８章は結論で，本論文で得られた成果を要約している．

氏　名	長尾　若

（論文審査の結果の要旨）

本論文は，暗号理論における、セキュアチャネル(SC)の構成方法である鍵共有とデータ暗号化，3つの暗号化チャネルの汎用的結合可能性について研究した結果をまとめたもので，得られた主な成果は次のとおりである．

１．鍵共有(KEM)とデータ暗号化(DEM)の安全性定義を提案し，それらの関係性について証明を通して明らかにしている．鍵共有については，3つの頑強性と攻撃手法を定義し，3つの頑強性定義が等価であることを証明している．また，頑強性よりも弱いと信じられていた強秘匿性と頑強性が適応的選択暗号文攻撃の下で等価になることを証明している．この証明により，適応的選択暗号文攻撃における強秘匿性が鍵共有における最も強い安全性定義として妥当であることがわかった．また，データ暗号化について，強秘匿性と頑強性，それぞれの攻撃方法について定義し，強秘匿性と頑強性について適応的選択暗号文/平文攻撃の下で等価性が成り立つことを証明している．これらの定義及び等価性の証明を通して，暗号の安全性について深く研究し，また寄与している．

２．汎用的結合可能性(UC)における鍵共有とデータ暗号化の理想機能の定義を提案し，汎用的結合可能性における鍵共有機能が，１で定義される最も強い安全性定義である，選択暗号文攻撃における強秘匿性と等価であることを証明している．これにより、汎用的結合可能性を満たすには，現在最も強い安全性である選択暗号文攻撃における強秘匿性が必要であることがわかった．また，データ暗号化についても，汎用的結合可能性におけるデータ暗号化機能が現在最も強い安全性定義である選択暗号文/平文攻撃における強秘匿性と等価であることを証明している．これにより，汎用的結合可能性を満たすには，現在最も強い安全性である選択暗号文/平文攻撃における強秘匿性が必要であることがわかった．汎用的結合可能性の定義から，他の暗号プロトコルと組み合わせて使用した場合にもその安全性が保証されるため，実暗号プロトコル構成への寄与も大きい．

３．3つの暗号チャネル，セキュアチャネル(Secure Channel)，２者匿名チャネル(Two-Anonymous Channel)，方向不明チャネル(Direction Indeterminable Channel)の理想機能の定義を提案し，タスク構造確率的入出力オートマトン(Task-PIOA)上の定義をそれぞれ提案している．これらの定義に対し，各チャネル間で等価性が成り立つことを証明している．この等価性は4つの帰着により成り立つ．①方向不明チャネルから２者匿名チャネル②２者匿名チャネルから方向不明チャネル③方向不明チャネルからセキュアチャネル④セキュアチャネルから方向不明チャネルへの帰着である．これらの成果を証明する際に，非決定性を考慮したスケジュールが必要になること示している．この証明により，現在良く使用されているセキュアチャネルの代替として２者匿名チャネルや方向不明チャネルを用いることが理論的に可能となる．

以上，本論文は鍵共有とデータ暗号化，3つの暗号化チャネルの汎用的結合可能性について研究した結果をまとめたものであり，学術上，実際上寄与するところが少なくない．よって，本論文は博士（情報学）の学位論文として価値あるものと認める．

また，平成２０年１２月４日実施した論文内容とそれに関連した試問の結果，合格と認めた．