審 査 の 結 果 の 要 旨

氏　　名　　久保田 貴大

量子暗号プロトコルは，（特に量子エンタングルメントなど）量子的現象の非局在性を通信原理として用いる暗号通信プロトコルである．（量子でない）古典暗号はその安全性証明を Diffie-Hellman 仮定などの計算論的仮定に依存する一方，量子暗号に対しては仮定なしの絶対安全性を証明することができ，それゆえ量子暗号プロトコルは大きな注目を集めている．実際，その理論的研究は言うに及ばず，量子暗号通信はすでに商用利用が開始されている．

一方で，暗号プロトコルを正しく設計することの困難は，古典通信においてもすでに大問題であり，1990 年代以来盛んな研究の対象である．というのも，仮に完全に安全な暗号を仮定したとしても，暗号通信における能動的な侵入者のもたらす通信過程の複雑さにより，なりすまし攻撃などの組み合わせ的攻撃が容易に見逃されうるのである．量子通信においても同様の困難が予想され近年研究が盛んであるが，本論文はこの問題に対して形式的手法――システムやプロトコルの正しさの数学的証明を指し，しばしば計算機による自動化または支援を伴う――を応用することを目的とした．この目的のためには，形式的手法における複数の手法を古典から量子へ拡張する必要があり，実際，安全性パラメータに対するエラー確率も適切に扱うような，量子暗号プロトコルの安全性そのものに対する自動検証の応用としては，本論文が世界のさきがけである．

本論文の手法の概要は次のとおりである．まず，量子暗号プロトコルを量子プロセス計算を用いて記述する．プロセス計算とは並行システムを形式的に記述するための単純なプログラミング言語であり，古典暗号プロトコルの検証に応用された実績を持つが，この量子版である Feng らによる qCCS を量子暗号プロトコルの形式的記述に用いる．同時に，安全性を表現した理想的プロトコル――明らかに安全だが物理的実現は不可能である――を同じく qCCS を用いて記述し，この 2 つの qCCS プロセスの間の等価性を証明することによって，もとの量子暗号プロトコルの安全性を証明する．以上のようなプロセス等価性による暗号プロトコルの安全性証明は古典暗号プロトコルに対してしばしば用いられる手法であるが，特に本論文の主要な技術的貢献は，2 つの qCCS プロセスの等価性証明に対して 1）証明を自動で行うためのアルゴリズムを提案・実装し，ま

た 2) そのアルゴリズムのために必要な qCCS の理論の整備を行ったことの 2 点である.本論文では例として,代表的な量子鍵配送プロトコルである BB84 を検証している.

以下，論文の構成に即して，本論文の貢献についてより詳細に述べる．第一章では導入として，古典・量子両方の暗号プロトコルの安全性の形式検証について，動機と既存手法を述べ，また論文の貢献の概要を与えている．第二章では，その後の技術的展開に必要な予備知識――特に量子情報の理論の基礎と，量子符号・量子鍵配送プロトコル――が述べられる．これを受けて第三章では，Feng らによる qCCS の操作的意味論を「非決定的なもの」に簡略化する．この簡略化はおおまかには，プロセスの動作モデルとしての状態遷移系において量子測定がもたらす確率的分岐を,明示的に確率をもつ状態間の非決定的遷移として表現するというものである．また続いて，この操作的意味論に基づくプロセスの間の双模倣性を調べる Verifier1 とよばれるアルゴリズムを導入する．このアルゴリズムは項書換えに基づく構文的なものであり，その正当性――すなわち，アルゴリズムが肯定的な答えを返せば,実際に双模倣性が成り立つこと――に対して数学的証明が与えられる．

一方で，BB84 のような量子暗号プロトコルの安全性は，以上のような「厳密な」双模倣性のもとでは成立しない．これは古典通信の場合と同様，（安全性パラメータ n に対して無視できる大きさの）ある確率でエラーが発生するためである．ゆえに第四章では 2 種類の近似的双模倣性の概念を与えている．前者はパラメータ ζ，η を明示的に持つ概念であり，後者は安全性パラメータ n に対して「無視できる」誤差を許容する概念である．前者の概念の応用は今後の課題とされる一方，後者は第五章の暗号プロトコルの検証において用いられ,これを検査するための Verifier2 とよばれる Verifier1 の変種が導入され，その正当性が証明される．

第五章では，それまでに導入されたアルゴリズム Verifier1, Verifier2 を用いて実際に BB84 プロトコルの安全性証明が与えられる．より具体的には，1) BB84 プロトコルと，論文で EDP-based プロトコルとよばれるプロトコルとの間の等価性（厳密な双模倣性）が Verifier1 を用いて示され，その後 2) EDP-based プロトコルと，EDP-ideal プロトコルとよばれる（明らかに安全だが物理的実現は不可能な）理想的プロトコルとの間の近似双模倣性が Verifier2 を用いて示される．実際この過程はソフトウェアとして実装されており，項書換えによる検証の実験結果が示される．最後に第六章では結論がのべられる．

以上の Verifier1, Verifier2 の 2 つのアルゴリズムは，ユーザーが与えた等式――または「この 2 つの値の差は無視できる」という項の 2 つ組――を用いて qCCS の構文的

な項を次々に書き換えていくものであり，ユーザーが与える等式そのものの正しさの検証は行わない（正しさの保証はユーザーの責任である）．この点に改善の余地があることは確かである一方，「量子状態の静的性質に関する事実は棚上げして，プロセスの動的ふるまいに関する推論に注力する」というアイデアは Floyd-Hoare スタイルのプログラム論理における相対完全性と同様のものであると言え，その貢献は決して小さくないと考えられる．事実，BB84 プロトコルの検証において与えられた等式は Shor と Preskill による（長大な）紙上の証明の要所要所で用いられるものであり，提案アルゴリズムはそれ以外の大部分を自動化するものであると考えることができる．また本論文で与えられたソフトウェア実装は，手詰まりに至った項を表示するためのオプションを持ち，ユーザーはこのフィードバックをもとに新たな等式を与えることができる．ところでアルゴリズムが構文論的なものであることは，扱うプロセスが安全性パラメータ n という自由変数を持つことの必然の帰結である．

提案手法の具体的な応用対象は現在 BB84 プロトコルのみであり，その応用可能性とスケーラビリティを強く主張する上では，より多くの量子暗号プロトコルへの応用が待たれる．また，提案アルゴリズムによる検証においては，入力として与える等式を注意深く吟味し試行錯誤を行う必要があり，さらなる自動化の可能性は将来の研究課題となろう．以上のような今後の課題が残る一方で，量子暗号プロトコルの（エラー確率を考慮に入れた上での）安全性の自動形式検証という，世界にさきがける研究課題に対し，必要となる量子プロセス計算の理論を整備しながら，項書換えによるアルゴリズムを考案し，その正当性を証明した上で実装した本論文は，それぞれが独立に意味のある多くの貢献を積み重ねて当初の問題を解決した．このことを高く評価する．

以上により本論文は博士（情報理工学）の学位請求論文として合格と認められる。