審 査 の 結 果 の 要 旨

氏　　名　　川本　　裕輔

形式的手法による暗号プロトコルの検証は、プロトコルで用いる暗号が全く解読できないことを仮定しているため、単純で自動化しやすいが、攻撃を見逃すこともある。そこで、近年、形式的手法の「計算論的健全性」、すなわち「プロトコルで用いられる暗号プリミティブが計算量理論に基づく一定の安全性を満たすならば、形式的手法によるプロトコル検証がいかなる攻撃も見逃さない」という性質の研究が数多く行われている。

本学位請求論文は、先行研究で仮定されていた安全性よりも弱い安全性やより現実的な安全性を持つ暗号プリミティブを用いるプロトコルを解析できるような形式的モデルを与え、新たな証明技法を導入することによって、その形式的モデルの計算論的健全性を示すものである。

本論文の第 1 章では、研究の背景と動機、研究の目的及び貢献が述べられている。第 2 章では、予備知識として計算論的識別不能性の概念を導入し、公開鍵暗号、リング署名、ハッシュ関数などの暗号プリミティブを紹介し、その計算量的安全性を定義している。

第 3 章では、再暗号化可能な公開鍵暗号を扱える形式的モデルを与え、その形式的モデルにおける制限された攻撃者の下でのパターン等価の計算論的健全性を示している。再暗号化可能な公開鍵暗号方式は、IND-CCA2 安全性よりも弱い性質を満たす暗号方式であるが、このような弱い暗号方式に対して計算論的に健全な形式的モデルを与えるのは、本研究が初めてである。健全性を証明するために、パターンにおいて乱数の合成を扱うための新たな技法を導入している。第 4 章では、リング署名を扱える形式的モデルを与え、能動的攻撃者の下でのトレース性質に対する健全性を示している。リング署名に対して計算論的に健全な形式的モデルを与えるのは、本研究が初めてである。最も重要な貢献は、健全性を得るために、署名の乱数部分を書き換える演繹規則を導入し、形式的攻撃者の能力を強めていることである。また、リング署名の異なる計算量的安全性に対してどのような演繹規則が必要になるのかを明らかにしている。

第 5 章では、公開鍵暗号、リング署名、ハッシュ関数を扱える applied pi-calculus を与え、二つのプロセスの間の観測同値の健全性を示している。これらの暗号プリミティブに関して、能動的攻撃者と非有界個のセッションの下での等価性に対する健全性の結果を与えるのは、本研究が初めてである。最も重要な貢献は、先行研究と違って、計算可能パーズ関数を使わずに健全性を証明している点である。この新たな証明技法により、さらに多くの暗号プリミティブを扱えるようになっている。例えば、原像計算困難性と衝突計算困難性を満たすハッシュ関数や、元のメッセージを伴うとは限らないような署名ビット列が扱えるようになっている。第 6 章では、本論文によるパーズ関数を用いない証明技法と、先行研究によるパーズ関数を用いる証明技法を比較し、パーズ関数を用いる証明技法の限界を述べている。また、本論文では、計算量的健全性を得るために、記号的攻撃者のプロセスで使える関数記号や述語記号を追加したり、プロトコルのクラスに制限を加えたりしているが、これらが暗号プリミティブの計算量的安全性に対応していることが述べられている。第 7 章では、論文の内容をまとめ、将来の研究の方向性を示している。

以上をまとめると、本論文は、先行研究で仮定されていた安全性よりも弱い安全性やより現実的な安全性を持つ暗号プリミティブを扱えるような形式的モデルを与え、新たな証明技法を導入することにより、その形式的モデルの計算論的健全性を証明した。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。