博士請求論文審査要旨

情報セキュリティ大学院大学
情報セキュリティ研究科

論文題目　：　より現実的なモデル下で証明可能な公開鍵暗号系に関する研究
申請者　：　森山 大輔
審査委員会　：　主査　教授　有田 正剛
副査　教授　田中 英彦
副査　教授　松尾 和人
副査　准教授　満保雅浩(筑波大)
副査　教授　土井洋

Ⅰ. 論文内容の要旨

博士後期課程学生、森山大輔君の博士請求論文は「より現実的なモデル下で証明可能な公開鍵暗号系に関する研究」と題し、4 章からなっている。

第 1 章「序論」では、本論文の研究背景や研究課題について述べている。現在の情報化社会において情報の秘匿の必要性から、公開鍵暗号系の理論研究が盛んに行われていることを説明し、達成される安全性は具体的な構成方法や、安全性のモデル等に依存することを説明している。さらに、より現実的な攻撃を考慮したモデルの下で安全性を証明することが望ましいことを述べている。次に、情報の秘匿を達成するためのセキュリティ技術のうち、「鍵交換プロトコル」および「空間暗号」の構築を課題として挙げ、本論文の目的が第 2 章以降に述べる「鍵交換プロトコル」および「空間暗号」に関してより現実的なモデルで安全性が証明可能な方式を提案することにあると述べている。

第 2 章「鍵交換プロトコル」では、鍵交換プロトコルにおいて必要となる数学的知識などについて準備し、鍵交換プロトコルの実行に際して情報漏洩のリスクを考慮した安全性モデルである、eCK セキュリティモデルを取り上げ、そのもとでの安全性を満たすことを研究の目標と位置付けるとともに、従来の研究では特殊な実装手法を前提とするか（NAXOS trick)、または理想的なハッシュ関数の存在を仮定した場合のみその安全性証明がなされていたことを指摘している。これに対し、新たにプロトコルを提案し、これが特殊な実装手法、および理想的なハッシュ関数の存在のいずれも仮定せずに eCK セキュリティモデルで安全性が証明可能であることを示している。一方、eCK セキュリティモデルそのものに注目し、攻撃者がより能動的に情報漏洩を誘発する活動を行うことにより長期的秘密鍵の部分情報が漏洩する状況をも考慮したモデルを新たに考案し定義している。そして、新たな鍵交換プロトコルを提案し、新たに定義したモデル下で、特殊な実装手法を前提とするものの、理想的なハッシュ関数の存在を仮定せずに安全性が証明可能であることを示している。最後に提案プロトコルと従来の研究との比較を行い、提案プロトコルがより現実的なモデル下で安全性において優位であることを確認している。

第 3 章「空間暗号」では、暗号化時に復号のための条件を指定することで、特定の属性を持つユーザが暗号文を復号できる暗号方式の 1 つにおいて、より現実的なモデル下で安全性を証明可能な方式の検討を行っている。まず、空間暗号を用いることにより、階層 ID ベース暗号や ID ベースリング署名など、様々な方式が構

成可能であることを説明している。一方、従来の研究では、攻撃対象をシステム構築が行われる前に定めるということを前提にしたモデル下でのみ安全性の証明がなされていることを説明している。これに対し、システムが構築され攻撃者が適応的に秘密鍵などの情報を得た後で、適応的に攻撃対象を定めることができるモデル下で安全性が証明可能な方式を提案している。この結果、より現実的なモデル下で安全性が証明可能な空間暗号が構成できることを示している。

第 4 章「結論」では、第 1 章で述べた課題に対して、「鍵交換プロトコル」および「空間暗号」の 2 つのセキュリティ技術に関する研究成果は、より現実的なモデル下で安全性を満たすことを要約している。

Ⅱ. 論文審査結果の要旨

本論文では、情報化社会において情報の秘匿を実現するための課題として、より現実的なモデル下で安全性を証明可能な「鍵交換プロトコル」および「空間暗号」の構築を挙げている。これらの課題に対して、現実的なモデルについて考察し、これらのモデル下で安全な複数の鍵交換プロトコル、および空間暗号を提案することにより解決策を示したものであって、情報学並びに情報社会の発展に貢献するところが大きい。よって、本論文は情報学における博士論文として十分価値のあるものと認める。

Ⅲ. 審査経過

本審査委員会は、平成 23 年 1 月 31 日に論文内容とこれに関連する事項について口述試問を行い、申請者が学位取得にふさわしい知見を持つものと判断した。