別紙1－1

論文審査の結果の要旨および担当者

報告番号	※ 甲　第 11911 号

氏　　名　森田 啓

論 文 題 目

関連鍵攻撃に対する公開鍵暗号要素技術の安全性に関する研究
(A Study on the Security of Cryptographic Public Key Primitives against Related-Key Attacks)

論文審査担当者

主査	名古屋大学	准教授	岩田　哲
委員	名古屋大学	教授	河口　信夫
委員	名古屋大学	教授	藤井　俊彰
委員	産業技術総合研究所	研究グループ長	花岡　悟一郎
委員	名古屋大学	教授	楫　勇一

別紙１－２

論文審査の結果の要旨

森田啓君提出の論文「関連鍵攻撃に対する公開鍵暗号要素技術の安全性に関する研究」は、非対話型鍵交換および署名方式の二つの公開鍵暗号要素技術を取り上げ、それらの関連鍵攻撃に対する安全性を明らかにしている。各章の概要は以下の通りである。

第１章では、まず暗号技術のうち公開鍵暗号系の技術に着目することを述べ、関連鍵攻撃が暗号技術が実装されたデバイスに対する物理的な攻撃を理論的にとらえた安全性概念であることを述べている。また、非対話型鍵交換が共通鍵暗号技術を使用する際に必要な鍵を共有する技術であるとともに、公開鍵暗号方式の構成などに応用可能であることを述べ、署名方式がメッセージの正当性を保証するための技術であることを述べている。それぞれについての関連研究をまとめ、本論文の成果の概要を述べている。

第２章では、本論文で使用する記法を定め、数学的仮定をまとめている。また、安全性証明で利用する補題を述べ、関連鍵攻撃の数学的な導入を行っている。

第３章では、非対話型鍵交換の安全性を解析している。従来の攻撃モデルにおいて、4つの安全性定義が提案されており、これらが等価であることが知られていた。これに対し、まず非対話型鍵交換の関連鍵攻撃に対する安全性の数学的な定義を4つ示している。次に、従来の攻撃モデルとは異なり、関連鍵攻撃の下では4つの安全性定義が等価ではないことを示している。具体的には4つの安全性定義は1つの弱い安全性定義と、より強い3つの等価な安全性定義の2つのクラスに分割されることを示している。帰着可能な安全性定義については帰着を示し、帰着不可能な安全性定義には実際に差があることを示す方式が存在することを、具体例を挙げることにより示している。これは、取り扱いの容易な弱い安全性定義が、最も強力な安全性定義を意味しないことを示唆しており、関連鍵攻撃の取り扱いが従来の攻撃モデルよりも顕著に困難であることを示す重要な知見である。また、関連鍵攻撃に対する最も強力な安全性を証明可能な方式が存在することを示している。

第４章では、署名方式の安全性を解析している。広く利用されている一般的な署名方式としてSchnorr署名方式、DSA、ElGamal署名方式の3つの方式を取り上げ、これらが関連鍵攻撃に対して安全ではないことを具体的な攻撃法を挙げることによって示している。さらに、これらの方式に簡素な修正を加えることで、関連鍵攻撃に対する証明可能安全性を達成できることを示している。提案する修正は元の署名方式の公開鍵と秘密鍵に変更を加える必要はなく、署名を生成する手順において1つの累乗計算を増やすだけであり、その他の計算コストや署名長が増えることがないという利点がある。これは、関連鍵攻撃が現実の社会で脅威となった場合に、多くの既存のネットワークシステムが危険である可能性を示唆するとともに、簡素な修正で安全性を達成できる可能性があることを示す重要な知見である。

第５章では、本論文の結論を与えている。本論文の結果をまとめ、今後の課題について述べている。本論文で扱っている関連鍵攻撃が数学的に取り扱いやすい代数的な攻撃手法に限定されているため、ビットフリップなどのより現実に近い攻撃モデルでの解析を今後の課題として挙げている。

以上のように本論文では非対話型鍵交換および署名方式の関連鍵攻撃に対する安全性を明らかにしている。これらの一連の解析手法、改良手法は、公開鍵暗号要素技術に対する関連鍵攻撃に関する知見を広げ、暗号理論および情報セキュリティの基礎研究に貢献するとともに、実際的な文脈においても重要であり、工学の発展に寄与するところが大きいと判断できる。よって、本論文の提出者である森田啓君は博士（工学）の学位を受けるに十分な資格があると判断した。