# 審 査 の 結 果 の 要 旨

氏　　名　　林田　淳一郎

本論文は、「A Study on Practical Information Retrieval Systems and Formalization of Their Security Models Considering Diverse Privacy Requirements（多様なプライバシー要件を考慮した情報検索システムの効率化とその安全性モデルに関する研究）」と題し、情報検索システムにおける多様な安全性要件の厳密な定式化と、それらを満たす複数の方式を示している。論文の構成は「Introduction」を含め７章からなる。

第１章は「Introduction（序論）」で、本研究の背景として情報検索システムにおける厳密な安全性評価の重要性と証明可能安全性について述べ、研究の位置付けを明らかにしている。とくに、複雑化した情報検索システムに対応した安全性モデルを適切に設定することが重要であること、および、今後さらに複雑化していくことが予想される情報検索システムにも適用可能な安全性の基盤となる枠組みの構築には大きな意義があることが、明らかにされている。

第２章は「Preliminaries（準備）」と題し、安全性証明の対象とするシステムを構成する暗号要素技術とその諸性質の定義、さらに、証明の帰着先となる数論仮定について記述している。

第３章は「Generic Construction of Adaptively Secure Anonymous KP-ABE from Public-Key Encryption with Keyword Search（公開鍵型検索可能暗号から匿名鍵ポリシー型属性ベース暗号への一般的構成法）」と題し、暗号化されたデータ上でのキーワード検索が可能な公開鍵型の検索可能暗号方式から、柔軟なアクセス制御を可能とする鍵ポリシー型属性ベース暗号へ変換できることを示しており、構成された鍵ポリシー型属性ベース暗号が秘匿性、匿名性と正当性の三つ全てを満たすことを証明している。また、今後の鍵ポリシー型属性ベース暗号方式の構成法についての指針を与えた他、公開鍵型検索可能暗号の構成に必要となる仮定の重さに関する傍証を与えている。

第４章は「Security Notions Against Replayable CCA and the Relationship Among Them（平文を保持した暗号文の変換が可能なCCA環境における安全性概念間の関係）」と題し、公開鍵暗号におけるReplayable CCAと呼ばれる攻撃者モデルに対する複数の安全性概念について論じている。Replayable CCAに対する既存の頑強性の定式化が恣意的であることを指摘し、シミュレーションベースの定式化を行うことで、Replayable CCA環境下における頑強性の意味を捉えた厳密な定式化を与えている。また、提案した安全

性と既存の安全性概念間の関係が明らかにされており、Replayable CCAに対する安全性に関する暗号学的体系化に貢献している。このReplayable CCAは、検索可能暗号の拡張においても、重要な役割を果たす。

第５章は「New Security Notion for Private Information Retrieval Supporting Range Queries（範囲クエリをサポートしたプライベート情報検索方式に対する新しい安全性概念）」と題し、データが平文で格納されたデータベース上での検索者のクエリプライバシーについて論じている。既存研究では考えられていなかった現実的な攻撃手法が存在し、既存の範囲クエリをサポートした方式が情報を漏らす場合があることを指摘している。また、こうした攻撃に対しても安全であることを保証する新たな安全性の定式化を厳密に行い、その安全性を満たす具体的な方式の提案も同時に行っている。提案された安全性の考え方は他のシステムへも応用可能であり、複雑なプライバシー要件が求められるシステムセキュリティに新たな潮流を起こす内容となっている。

第６章は「PIR Supporting Multi-dimensional Range Queries（多次元範囲クエリをサポートしたプライベート情報検索方式)」と題し、第５章の内容の拡張を考えている。とくに、第５章で提案された方式よりも複雑な構造のデータベース上でのより柔軟なクエリを考慮したプライベート情報検索の構成とその安全性証明を与えている。提案方式は多次元範囲クエリをサポートした初めての方式であり、プライベート情報検索の実用化に向けた先駆的内容となっている。

最後に第７章は「Conclusion（結言）」で、本研究の総括を行い、併せて将来展望について高い見識で述べている。

以上これを要するに、本論文は情報検索システムにおける多様な安全性と実用化に向けた効率化の両面について論じたものであり、前者では今後さらに複雑化していく情報検索システムにおける基盤となる安全性モデルの開拓により、後者ではより現実的な攻撃モデルを厳密に考慮したのみならず、効率的な方式設計を行ったその完成度の高さにより、電子情報学、特に情報セキュリティ工学上貢献するところが少なくない。

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。