# 審査の結果の要旨

論文提出者氏名　　松下　達之

本論文は「Black-Box Traitor Tracing Schemes for Copyright Protection（著作権保護のためのブラックボックス不正者追跡方式に関する研究）」と題し，コンテンツ配信システムなど多数の受信者が存在する暗号通信において，不正な受信者が復号鍵を第三者へ漏洩させた場合，この不正な漏洩者を特定可能な暗号方式（不正者追跡方式）を提案し，その安全性及び効率性について厳密な評価を行ったものである．本論文では，不正者追跡において望ましい性質であるブラックボックス追跡可能性（復号器の入出力を観測するのみで不正者の特定を行うことができること）と公開鍵方式に基づいていること（暗号化を公開情報である公開鍵のみで行うことができること）に焦点を当て，これらの性質を満たす実用的な不正者追跡方式を提案している．従来の不正者追跡方式では，不正者の追跡に要する処理量が過大で実際上追跡不可能であるという問題や，より強力な不正者に対しては追跡が失敗するという問題があり，これらの問題が実用化へ向けた大きな課題となっている．本論文は，これらの問題に対し，有効な解決策を示したものであり，論文の構成は「Overview of This Thesis」を含め5章からなる．

第1章は「Overview of This Thesis（論文の概要）」で，本研究の背景を明らかにした上で，研究の動機と目的について言及し，研究の位置付けについて整理している．

第2章は「Flexible Revocation for Efficient Public-Key Black-Box Tracing（効率的な公開鍵方式に基づいたブラックボックス追跡のための柔軟な復号鍵無効化）」と題し，一度に無効化できる復号鍵（すなわちユーザ）数に制限がないという意味で柔軟な復号鍵無効化方法を提案し，その復号鍵無効化方法はブラックボックス追跡に応用可能であることを示している．また，従来の不正者追跡方式においては不正者の追跡に要する処理量が過大で実際上追跡不可能であるという問題があったが，提案方式では，この問題が解決されることも示している．提案方式の安全性は，計算量的な仮定（Diffie-Hellman仮定）に基づいて数学的に証明されている．また，効率性について，復号鍵サイズや暗号文サイズなどの観点から評価が行われている．本章以降についても，全ての提案方式は，計算量的な仮定（Diffie-Hellman仮定）に基づいて安全であることが数学的に証明されており，また，復号鍵サイズや暗号文サイズなどの観点から効率性評価が行われている．

第3章は「Public-Key Black-Box Tracing with Sublinear Ciphertext Size against Self-Defensive Pirates（暗号文サイズが全ユーザ数に比例せずより強力な不正者に対しても追跡可能な公開鍵方式に基づいたブラックボックス追跡）」と題し，追跡を察知した場合，追跡を回避するような機構を備えているという意味

でより強力な不正者を想定した場合でも，ブラックボックス追跡可能な方式を提案し，より強力な不正者に対して追跡が失敗するという問題が解決されることを示している．提案方式は，このような仮定の下で，暗号文サイズが全ユーザ数に比例しない（sublinearである）初めての方式である．

第4章は「Hierarchical Key Assignment for Efficient Public-Key Black-Box Tracing against Self-Defensive Pirates（効率的でより強力な不正者に対しても追跡可能な公開鍵方式に基づいたブラックボックス追跡のための階層的な復号鍵割り当て）」と題し，第3章で提案した方式に対して，復号鍵サイズを僅かに増加させることにより暗号文サイズを大幅に削減できる階層的な復号鍵割り当て方法を提案している．また，ブラックボックス追跡と匿名性を有する復号鍵無効化との関係について指摘し，さらに，特定された不正者の排除を目的として，第2章で提案した復号鍵無効化方法と本章の提案方式を統合した方式も提案している．

最後に第5章は「Conclusion（結論）」で，本研究の総括を行い，併せて将来展望について述べている．

以上これを要するに，本論文は，不正に対する抑止力となるブラックボックス不正者追跡の基礎検討を行うとともに，従来方式における問題点を解決する具体的方法を明示したものであり，電子情報学，特に情報セキュリティ工学において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．