審査の結果の要旨

論文提出者氏名　　渡邊 裕治

本論文は「Security of Cryptographic Protocols based on the Trusted Party（信頼機関に基づく暗号プロトコルの安全性に関する研究）」と題し，効率的な暗号プロトコルを構成する上で不可欠である信頼機関（TP）の安全性に関して，①安全性の向上，②安全性の評価，③TPの安全性に対する仮定の緩和，といった3つの観点から検討している．効率的な暗号プロトコルを構成する上でTPは不可欠であるが，これを実際に用いる場合，TPに対して仮定される安全性をどう具体化し，その安全性をどのように評価するかが鍵となってくる．またTPに対する安全性の仮定を緩和して，その具体化を容易にすることも実用上重要である．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，「Introduction」を含め7章からなる．

第1章は「Introduction（序論）」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「Forward Security against the Leakage of the CA's Secret（公開鍵証明書発行機関の秘密漏洩時における安全性対策）」と題し，認証機関（CA）の署名鍵が漏洩した後も，証明書の偽造を困難にする手法を示している．CA とは公開鍵認証基盤における TP であり，CA の署名鍵は長期間に渡り高度な安全性が要求される情報である．また，その運用負荷は極めて高く，効率的な署名生成法が必要とされる．本章では，CA の署名鍵が漏洩したという事態においても，証明書の偽造が困難であるように，署名方式を効率よく変換する手法を示している．

第3章は「Security Analysis on the Proactive System（時限更新型分散暗号方式の安全性評価）」と題し，TP の経年劣化を防ぐために近年提案された時限更新型分散暗号方式の不正侵入・潜伏に対する耐性を評価している．ここでは，時限更新型分散暗号方式が持つウイルスの侵入・潜伏攻撃に対する安全性を，確率モデルを用いることにより評価している．特に，潜伏力の強いウイルスに対して，この方式が持つ脆弱性について明らかにするとともに，それに対する耐性を高めるために必要となる対策を示している．

第4章は「Traitor Traceable Signature Scheme（署名付き文書の不正漏洩者の追跡が可能な署名方式）」と題し，署名を添付した文書が特定の受信者から他者に漏洩した場合に，誰がその署名を漏洩したかを公開検証可能な署名方式を示している．この署名方式は，従来方式に比べ，メモリ量・通信量ともに数十分の一となる．また，提案方式と電子透かしと組み合わせることにより，不正コピーの公開検証が可能なコンテンツ保護システムを示している．

第5章は「Optimistic Sealed-bid Auction Protocol（信頼機関に対する仮定を低減した電子入札方式）」と題し，電子入札方式において入札者のプライ

バシーを保護する手法を示している．近年，入札者のプライバシー保護を目的として，落札値以外の入札値を秘匿したまま落札値を決定できる電子入札方式が研究されている．しかし，従来，入札管理者に対する信頼を仮定せずに，効率的なプロトコルを構成できなかった．本章では，例外処理以外の TP の関与を必要とせずに，前述の性質を満たす電子入札プロトコルを提案している．提案方式は，入札管理者の不正に対しても耐性があり，開票時における入札者の通信回数が少ないという特長を持つ．

第6章は「Asymmetric Public-Key Traitor Tracing without Trusted Agents（信頼機関を用いない非対称型公開鍵不正加入者追跡法）」と題し，放送型デジタルコンテンツ配信システムの著作権保護方式を示している．不正者追跡法は，ユーザ個人に割り当てられた秘密情報を他人に再配布するという不正を防止する手段として有力視されている．しかし，従来方式では，コンテンツ配布者側の不正があり得る場合の安全性を考慮すると，TP の存在を仮定する必要があった．本章では，TP の存在を仮定せずにこのような場合にも安全な手法を示している．

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述べている．

以上これを要するに，本論文は，暗号プロトコルにおける信頼機関の安全性に関する基礎検討を行うとともに，暗号プロトコルの具体的な応用に対する信頼機関の安全な運用手法を明示したものであり，情報セキュリティ工学，特に暗号プロトコルの応用分野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（工学）の学位請求論文として合格と認められる．