審 査 の 結 果 の 要 旨

氏　名　　小 川　一 人

本論文は「A Study on Secure Contents Distribution Systems with Advanced Functions to Enrich User Convenience」（ユーザの利便性を考慮した効率的でセキュアなコンテンツ配信システムに関する研究）と題し、デジタルコンテンツ配信に用いられる暗号技術について、著作権管理を扱うとともに、ユーザの利便性の向上、コンテンツ提供者の利便性の向上を可能とする、従来にない技術である鍵漏洩耐性を有する不正利用者追跡方式、鍵漏洩耐性を有するグループ署名方式、マスク機能付き準同形暗号方式、鍵管理を分離可能なデジタルコンテンツ保護方式、最も効率的な不正利用者追跡方式を提案し、将来のコンテンツ配信サービスの向上に有益な暗号方式の構成、及び、その使用方法を具体的に示している。論文の構成は「Introduction」を含め５章からなる。

第１章は「Introduction（序論）」で、本研究の背景を述べ、研究の位置づけを明らかにしている。

第２章は「Systems with Advanced Functions to Enrich User Convenience（ユーザの利便性を考慮したシステム）」と題し、鍵漏洩耐性を有する効率的な不正利用者追跡方式、トークンと鍵漏洩耐性を有するグループ署名を用いたコンテンツ配信方式、マスク機能付き準同形暗号を用いた匿名視聴可能な有料放送方式、を提案している。

不正利用者追跡方式は、不正に作られた受信機に内蔵された復号鍵から不正利用者を特定する技術であり、コンテンツ配信を行う際の著作権保護等の有望な産業応用がある。本章では、従来の不正利用者追跡方式に鍵漏洩耐性を付加し、不正利用者を特定できるだけでなく、ユーザが鍵を持ち歩き、不注意により鍵を紛失した場合でもその被害を最小限に抑えることが可能な方式を提案し、さらに、その技術を応用したどこでも視聴が可能な放送方式を示している。

また、グループ署名は、グループのメンバーであることを認証できるが個人を特定されることがない署名方式である。グループ署名の利用により匿名でサービスを享受することが可能となり、プライバシー保護が要求される産業では有望な技術である。本章では、従来のグループ署名に鍵漏洩耐性を付加し、さらにトークンと組み合わせることで、匿名性だけでなく、署名鍵を持ち歩くことでどこでもサービスを享受することが可能であり、さらに、サービス利用回数をトークンの枚数で制御可能であり、署名鍵、トークンの紛失にともなう被害を最小限に抑えることが可能なコンテンツ配信方式を提案している。

また、準同形暗号は暗号化された状態で演算が可能な暗号方式である。第三者に平文を渡すことなく演算を依頼することが可能であり、第三者に対するプライバシー保護を保持しつつ、第三者に負荷を依頼でき、財務管理等の有望な産業応用がある。本章では、マスク機能を付加した準同形暗号方式を提案し、このマスク機能をコンテンツ提供者が制御し適切な課金が可能なシステムを提案し、さらに、その技術を利用した匿名有料放送方式を示している。

これらの３つの要素技術、及び、その利用方式は、「どこでも家庭と同じサービスを享受できる」「匿名でサービスを享受できる」などのこれまでにないユーザ利便性をもたらし、今後のコンテンツ配信の発展に貢献できる。

第３章は「A System with An Advanced Function to Enrich Contents Provider Convenience（コンテンツプロバイダの利便性を考慮したシステム）」と題し、コンテンツの暗号鍵と復号鍵を独立に生成が可能な高機能暗号方式を提案している。本方式にも、コンテンツ配信を行う際のコンテンツ保護、負荷分散等の有望な産業応用がある。本章では、この暗号方式のモデルと安全性を定義し、これらが「Identity-Based Encryption（IDに基づく暗号：IBE）」のモデルおよび安全性と同等であることを厳密に導いている。さらに、当該分野の従来のIBEはランダムオラクルモデル（理想的な乱数発生器が存在するという仮定）の上でしか安全性が示されていなかったが、この仮定を排除してスタンダードモデル（現実に存在する乱数発生器を用いる仮定）の上で安全な方式を提案している。この方式は全てのユーザがコンテンツ提供者になった場合でも、全てのコンテンツの著作権保護を可能とする技術であり、負荷分散に伴うコンテンツ提供者の利便性を向上させるだけでなく、ユーザの利便性をも向上させ、総ユーザー総コンテンツ提供者という新たなコンテンツ配信方法を示している。

第４章は「A More Efficient Primitive for Secure Contents Distribution Systems（セキュアなコンテンツ配信システムのための効率的な要素技術）」と題し、不正利用者追跡方式について、最も効率的な方式を提案している。本章では、秘密鍵生成のための多項式の組み合わせ方を変更することで、鍵管理者が所有する秘密情報のサイズが従来の半分になる方式を提案している。この方式は、第２章で示した不正利用者追跡方式だけでなく、多項式を用いた不正利用者追跡方式に汎用的に利用することが可能である。

第５章は「Conclusion（結論）」で、本研究の総括を行い、併せて将来展望などについて述べている。

以上これを要するに、本論文は、デジタルコンテンツ配信に用いられる暗号技術について、著作権管理を支える安全性を厳密に扱うとともに、ユーザに対する新たなサービスやコンテンツ提供者への利便性を提供する技術を提案し、将来のコンテンツ配信サービスの向上に有益な暗号方式の構成、及び、その使用方法を具体的に示し、この分野を体系的にまとめた論文であり、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。