審 査 の 結 果 の 要 旨

氏　　名　　アッタラパドゥン　ナッタポン

本論文は「Unified Frameworks for Practical Broadcast Encryption and Public Key Encryption with High Functionalities（放送型暗号と高機能公開鍵暗号方式のための統合的枠組みに関する研究）」と題し、デジタルコンテンツの著作権管理や高度な機能を伴った秘密情報保護に用いられる暗号技術について、それらを統一的に取り扱う世界で初めての理論的枠組みを提案するとともに、もっとも効率的な放送型暗号方式やもっとも高度なキーワード検索機能付き暗号方式など、多様かつ完成度の高い暗号方式の具体的構成を示している。論文の構成は「Introduction」と「Preliminaries」を含め 6 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。さらに本章では、放送型暗号と高機能公開鍵暗号の関連研究について整理して記述している。

第 2 章は「Preliminaries（準備）」で、本論文の第 3 章以降に使われる記号や暗号要素技術などを体系的に記述している。

第 3 章は「Practical Symmetric-Key Broadcast Encryption（実用的な放送型対称暗号）」と題し、効率的な放送型対称暗号方式とその枠組みを提案している。放送型暗号とは、秘密情報を複数の機器に配信する技術である。不正なユーザにコンテンツを再生できないようにさせる無効化が可能なため、映画や音楽などのデジタルコンテンツを配信する際の著作権保護等の有望な産業応用がある。本章では、対称鍵タイプの放送型暗号に関して従来方式を整理し、擬似乱数生成器、落とし戸なし RSA 暗号、落とし戸付き RSA 暗号、それぞれに基づく三つの枠組みを提案した。これらの枠組みの利点は、根本的な組み合わせ論的構造を決めればそれぞれの枠組みに当てはめることで証明可能安全性を持つ放送型暗号の具体的構成が自動的に得られることである。本章で新たに導いた具体的な構成の中でももっとも重要な結果は、「Subset-Incremental-Chain」という構造に基づく。この構造は、ユーザ鍵サイズと暗号文の長さがシステムの全体ユーザ数に依存せず、かつ計算量を抑えた初めての放送型暗号方式を与える。本方式は、今後デジタルメディアの主流となるであろう Blu-ray Disc と HD-DVD の両方の規格への採用が報じられている既存の放送型暗号方式（Subset-Difference Method）よりもはるかにスケーラビリティの優れた効率的な方式である。

第 4 章は「Unifying Public Key Encryption with “High Functionalities”（高機能公開鍵暗号の統一的枠組み）」と題し、多様な高機能公開鍵暗号（Public-key Encryption: PKE）を統一して取り扱うことが可能な枠組みを初めて提案している。ここで高機能公開鍵暗号とは、高度な機能を付加した公開鍵暗号方式、あるいは公開鍵暗号の変形のことをいう。具体例としては、「Forward-secure PKE（フォーワードセキュア公開鍵暗号）」、「Identity-based Encryption（ID 情報に基づく暗号）」、「Certificate-based PKE（証明書に基づく公開鍵暗号）」、「Certificate-less PKE（証明書不要な公開鍵暗号）」、「Key-insulated PKE」とそれぞれを階層化した方式などが挙げられる。第 3 章の放送型暗号の公開鍵版もその一例である。本章の一つ目の成果は、これらの暗号プリミティブを統一し、「Directed Acyclic Graph Encryption」という枠組みでまとめたことである。この枠組みでは、それぞれのプリミティブのグラフ表現を、プリミティブを規

定するために必要十分な情報と見なすことが出来る。そのプリミティブの「アルゴリズムの定義」と「安全性概念の定義」と「証明可能安全性をもつ具体的構成法」は、グラフによって自動的に得られる。さらに、新しい機能を持つ公開鍵暗号や、多様な機能の組み合わせを持つ公開鍵暗号などを設計することが出来る。本章の二つ目の成果は、任意の二つのプリミティブがお互いに帰着出来るかどうかの判断の条件（Graph Syntactic Consequence）を提案し、その健全性（Soundness）の定理を示したことである。この条件の利点は、従来の一般的帰着判断に利用されている条件と違い、計算量理論に基づかず完全にフォーマルロジックに基づいているため、自動的な証明検証（Automated Verification）が可能なことである。

第 5 章は「Practical Forward-Secure and Searchable Broadcast Encryption（効率的なフォーワードセキュア放送型公開鍵暗号とキーワード検索機能付き放送型公開鍵暗号）」と題し、放送型公開鍵暗号について、効率的な高機能暗号方式を提案している。本章では、第 4 章の統一的構成法よりも効率を向上させるために、対象となる機能を絞り、Forward Security（フォワードセキュリティ）と Keyword Searchability（キーワード検索機能）に着目した。結果として、ユーザ鍵サイズと暗号文の長さがユーザ数に依存しない初めてのスケーラブルなフォーワードセキュア放送型公開鍵暗号の提案と、Poly-logarithmic サイズの効率を持つキーワード検索機能付き放送型公開鍵暗号の提案を行っている。

第 6 章は「Conclusions（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、世界でもっとも効率的な放送型暗号方式を提案するだけでなく、多様な高機能公開鍵暗号方式を統一して取り扱うことが可能な枠組みを初めて提案して幾多の完成度の高い具体的構成を示し、この分野の集大成として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。