別紙様式第２号

学位論文及び審査結果の要旨

横浜国立大学

氏名	渡邉洋平
学位の種類	博士（情報学）
学位記番号	環情博甲第 380 号
学位授与年月日	平成 26 年 3 月 24 日
学位授与の根拠	学位規則（昭和 28 年 4 月 1 日文部省令第 9 号）第４条第１項及び横浜国立大学学位規則第５条第１項
学府・専攻名	環境情報学府　情報メディア環境学専攻
学位論文題目	Cryptography with Timed Access Control（時刻制御暗号技術）
論文審査委員	主査　横浜国立大学　准教授　四方順司 横浜国立大学　教授　松本勉 横浜国立大学　教授　長尾智晴 横浜国立大学　教授　森辰則 横浜国立大学　准教授　吉岡克成

論文及び審査結果の要旨

現代暗号学において、アクセス制御機能をもつ暗号技術は理論的にも応用的にも重要であることから、近年多くの注目を集めている。特に、時刻制御に関わるものとして、対象となる暗号機能をある時刻から開始する制御技術はタイムリリース技術（Timed-Release Cryptography）と呼ばれ、これまでに世界で広く研究がなされてきた。本論文は、既存のタイムリリース技術の理論的枠組みを拡張し、様々な暗号基礎技術（暗号化、認証、鍵共有、秘密分散等）に対してタイムリリース技術を実現している。また、時刻制御の新たなる概念として、対象となる暗号機能をある時刻で停止させる制御技術であるタイムリボーカブル技術（Timed-Revocable Cryptography）についても提案している。このように、本論文は時刻制御を有する暗号技術の理論研究成果を広くまとめたものであり、本論文は序論（第 1 章）と結論（第 6 章）を含めて全 6 章から構成され、全文が英語で書かれた博士論文である。

第 2 章の Preliminaries では、計算量理論および情報理論の基礎事項、そして、本論文で研究対象とする計算量的安全性および情報理論的安全性に対して説明している。また、現代暗号における暗号基礎技術として、鍵共有方式、暗号化方式（共通鍵暗号、公開鍵暗号、ID ベース暗号）、メッセージ認証方式、ディジタル署名方式、秘密分散法について解説している。

第 3 章の Computational Timed-Release Cryptography では、タイムリリース機能を持つ計算量的に安全な秘密分散法（Timed-Release Computational Secret Sharing: TR-CSS）を提案している。これまでの計算量的に安全なタイムリリース技術において、暗号化方式や署名方式の構成法については既存研究があったものの、秘密分散法についてはタイムリリース機能に関する研究報告はなかった。本章では、TR-CSS の数理モデルと安全性を定義し、TR-CSS の構成法として、暗号基礎技術をブラックボックス的に用いる一般的構成法と、代数構造を利用することでシェア情報長が短くてすむ直接的構成法の 2 つの構成法を提案している。提案の TR-CSS の構成法は、プロトコル開始時に設定する閾値が十分に大きいとき、タイムリリース機能をもたない既存の秘密分散法の最も効率的な構成法と同程度のシェア情報長を達成している。更に、TR-CSS によって、タイムリリース機能をもつ閾値暗号（Timed-Release Threshold Encryption: TR-TE）や多重暗号（Timed-Release Multiple Encryption: TR-ME）等をシンプルに構成可能であることも示しており、TR-CSS から構成した TR-TE や TR-ME は、従来の（TR-CSS を利用しない）TR-TE や TR-ME の構成法よりも効率的であることも示している。

第 4 章の Information-Theoretic Timed-Release Cryptography では、情報理論的安全性を有する鍵共有方式、暗号化方式、メッセージ認証方式、秘密分散法について、それぞれタイムリリース機能を

持つ方式を提案している。具体的には、タイムリリース鍵共有方式 (Timed-Release Key-Agreement: TR-KA)、暗号化方式 (Timed-Release Encryption: TRE)、認証方式 (Timed-Release Authentication code: TRA-code)、秘密分散法 (Timed-Release Secret Sharing: TR-SS)の各々について、数理モデルと安全性の定式化を提案し、秘密鍵長の下界の導出、及び、その下界の等号をみたす最適な構成法を提案している。このことにより、情報理論的立場からタイムリリース機能をもつ暗号基礎技術の構成法の限界が理論的に示されたことになる。

第 5 章の Information-Theoretic Timed-Revocable Cryptography では、情報理論的に安全な放送型暗号（Broadcast Encryption: BE）において暗号文の受信者集合を動的に変更可能な方式である Revocable-Storage BE（RS-BE）を考え、これにより任意のエンティティの復号機能を無効化できるタイムリボーカブル技術の実現に結び付けている。本章では、具体的には、RS-BE の数理モデルと安全性の定式化を提案し、秘密鍵長の下界の導出、及び、その下界の等号をみたす最適な構成法を提案している。また、暗号文の改ざん攻撃にも耐性のあるロバスト RS-BE も提案している。更に、放送型暗号の暗号文長と秘密鍵長間のトレードオフの解析も本章にて行っている。以上より、本章では情報理論的立場からタイムリボーカブル暗号を構成するにあたり、やや一般的なモデルである RS-BE を考え、それに関する様々な解析を通して俯瞰的立場からタイムリボーカブル技術に対する成果を記述している。

最後の第 6 章の Concluding Remarks では、本論文の成果を総括するとともに、その成果の更なる発展性に関しても論じている。

以上のように、本論文は、計算量的安全性および情報理論的安全性の双方の観点から、様々な時刻制御機能を有する暗号基礎技術に関しての研究成果を高い完成度でまとめたものであり、独創性が高く当該分野への学術的貢献度の高い論文である。

以上から、本論文は博士（情報学）の学位論文として十分な価値を有すると審査委員全員一致して認めるものである。

注　論文及び審査結果の要旨欄に不足が生じる場合には、同欄の様式に準じ裏面又は別紙によること。