博士後期課程

博士請求論文審査要旨

情報セキュリティ大学院大学
情報セキュリティ研究科

論文題目 : Cryptographic Schemes Towards Transparent and Fair Digital Currency
申請者 : 樋口 大志
審査委員会 : 主査 教授 大塚 玲
副査 教授 土井 洋
副査 准教授 橋本 正樹(香川大学)
副査 教授 宮地 充子(大阪大学)

Ⅰ. 論文内容の要旨

本博士論文は、Cryptographic Schemes Towards Transparent and Fair Digital Currency と題し、5章で構成されている。

第一章では、本博士論文の導入として、「匿名性と法令順守」の両立というテーマに関する背景及び核となる2つアプローチの概要と関連研究と貢献について述べている。

第二章では、第一のコアアイディアとして、デジタル通貨の匿名性と不正取引防止の両立を目指し、Brands型ブラインド署名と実行証跡付きセキュアプロセッサに基づき、二重支払を未然に防ぐことが可能なオブザーバー方式を提案している。第一の結果として、耐タンパー装置にオープンソース形式のプログラム実行を検証可能な形で実現することにより、匿名性に起因する不正使用を防ぎつつ、オブザーバーによる過度な監視への不信感を軽減する監視機能を実現できることを明らかにしている。

第三章では、前の章に続き、オブザーバー方式デジタル通貨スキームがブラインド署名だけでなく、BBS+署名に基づくゼロ知識証明を用いても同等のセキュリティ特性を達成できることを示している。BBS+署名ベースのプロトコル構築はq-SDH仮定に基づき、デジタル通貨のコイン（発行体のデジタル署名）の所持に関するゼロ知識証明で構成する点に特徴がある。すなわち、ブラインド署名では引き出し時に署名を秘匿した状態で取得することでユーザーの匿名性を確保するのに対し、BBS+ 署名では支払時に署名をゼロ知識証明で提示することで匿名性を達成している。BBS+署名のゼロ知識証明プロトコルの構造は極めてシンプルであり、BBS+署名で発行された身分証等の証明書（BBS+署名）の所持に関するゼロ知識証明（SPK）を統一的に扱えることから、現代社会の要請に合う透明性の高いデジタル通貨スキームへの自然な拡張が可能であると指摘している。

第四章では、第二のコアアイディアとして、取引回数に依らず、取引額のみに応じた確率で取引当事者の匿名性を解除するFair-Anonymityの安全性概念を提案し、その暗号学的な構成法を示している。提案する方式は、Committed Oblivious Transferと飽和指数関数を用いることにより、匿名性の解除確率を不正に操作できない形で，匿名性と透明性のバランスの取れたデジタル通貨を実現している。Committed Oblivious Transfer を用いることで、この確率が当局によって操作されないことを保証し、公開検証者は送信者のプライバシーを完全に保護しつつ取引を検証できる。また、飽和指数関数を確率関数として用いることで、コインの総額のみで決定される公平な確率的関係を提供し、コイン分割に依存しないユーザー追跡を可能にしている。提案手法は、Bitcoin等の暗号資産やStable Coinを含む多くのデジタル通貨に適用可能であるとしている。

第五章では、結論として、本博士請求論文に示された内容は、デジタル通貨における匿名性と透明性の両立という課題に対し、革新的な解決策を提供するものであり、進化し続けるデジタル経済の要請に応えつつ、安全でプライバシーが確保され、かつ社会的に求められる透明性の高いデジタル通貨の実現へと道を拓くものであると述べている。

Ⅱ. 論文審査結果の要旨

本論文は、情報社会における経済取引の基盤を成すと期待されるデジタル通貨に関し、匿名性を達成しながら社会的に求められる透明性を実現し、安全かつ公正なデジタル通貨の実現するための、具体的かつ基盤的な方法を示したものであって、情報学ならびに情報社会の発展に貢献するところが大きい。よって、本論文は情報学における博士論文として十分価値のあるものと認める。

Ⅲ. 審査経過

本審査委員会は、2025 年 2 月 19 日に論文内容とこれに関連する事項について口述試問を行い、その後、2025 年 9 月 10 日に関連する事項の最終試験審査を行った。審査に当たっては、博士学位のディプロマ・ポリシーに基づいて総合的に評価し、申請者が学位取得にふさわしい知見を持つものと判断した。