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 ： Sybil-Resistant Self-Sovereign Identity Based-on Attested Execution Secure Processors
申請者 ： 森山 光一
審査委員会 ： 主査　教授　大塚 玲
副査　教授　有田 正剛
副査　教授　佐古 和恵（早稲田大学）
副査　教授　面 和成（筑波大学）

Ⅰ. 論文内容の要旨

本論文は“Sybil-Resistant Self-Sovereign Identity Based-on Attested Execution Secure Processors”と題し、7 章からなっている。

第 1 章では、研究の背景として、ブロックチェーンなどの登場によって、政府当局や大組織への依存を解決できる自己主権型アイデンティティ（SSI: Self-Sovereign Identity）の実現に向けて活発に研究が行われていることを指摘し、先行研究を系統的に概観している。その中で、SSI においてはプライバシー保護と本人の実在性確認といった対立する問題を解決することの重要性を指摘し、プライバシーを保護しつつ複数人格へのなりすましを防ぐ、いわゆるシビル耐性を有する SSI を実現する方式に関し、実行証跡付きセキュアプロセッサと集合帰属に関するゼロ知識メンバーシップ証明に立脚した 2 つのコアアイデアの概要を述べている。

第 2 章では、分散型デジタルアイデンティティに関する研究と産業界の動向、ハードウェア支援によるセキュリティモジュールの技術環境、自己主権型デジタルアイデンティティに関連する議論について網羅的にまとめている。特に、分散型デジタルアイデンティティにおいてプライバシー保護とシビル耐性を両立する Maram らの先行研究がマルチパーティ計算（MPC）に基づいて暗号学的に主張の正しさを証明していることから、本研究においてもプライバシー保護とシビル耐性のセキュリティ要件として引用し、本研究のアプローチと関連研究を比較している。

第 3 章では、本論文で提案する暗号プロトコルの主要な構成要素である実行証跡付きセキュアプロセッサの形式的表現、検証可能証明書で主要な役割を果たす Strong RSA 仮定に基づく Camenisch と Lysyanskaya による墨塗署名と q-SDH 仮定に基づく Boneh らによる BBS+署名、および効率の良いゼロ知識メンバーシップ証明の 3 つを取り上げ、それらの暗号学的な性質と構成法の概略を述べている。

第 4 章では、本研究におけるコアアイデアの一つである実行証跡付きセキュアプロセッサに基づく自己主権型アイデンティの安全性概念とその構成法を述べている。自由参加型ブロックチェーンと実行証跡付きセキュアプロセッサを組み合わせることで、利用者が検証可能な証明書から派生証明書を生成・検証できる仕組みを提案し、その具体的なシステム構成を示している。また、派生証明書の生成方法のフレキシビリティを高めると同時に不正処理の懸念を払拭するため、オープンソースプログラムの実行証跡機構を導入することで、処理の柔軟性と透明性を実現している。提案した方式は、自己主権型アイデンティティに求められる諸性質として、シビル耐性に対応する実在性(Existence)、偽造不可能性、プログラムを越えた結合不能性、派生証明書の生

成と検証に関する二つのプライバシーを定義し、提案する構成がこれらの性質を満たすことを示している。

第 5 章では、本研究における 2 つ目のコアアイデアとして、第 4 章の議論を発展させ、検証者が実行証跡付きセキュアプロセッサを保有せずとも証明書の検証を可能とするように仮定を緩和した自己主権型デジタルアイデンティの実現法を提案している。特に、実在性(Existence)についてゼロ知識メンバーシップ証明等を用いて実現する構成法を提案し、これが自己主権型アイデンティティに求められる諸性質を満たすことを示している。この構成法は参加者数の対数オーダーの通信量で実現されることから、実用性を十分に備えていることを明らかにしている。

第 6 章では、本研究の成果の適用が期待される応用の可能性がある重要なアプリケーションとして、仮想空間での本人確認、デジタル ID ウォレットやモバイル運転免許証、予防接種パス、公的個人認証などを例示している。また、実行証跡付きセキュアプロセッサの耐タンパー性が崩れた場合についての考察を示した上で、本研究の将来の応用を展望している。

第 7 章で結論として、ハードウェア支援によるセキュリティモジュール、自由参加型ブロックチェーン、ゼロ知識メンバーシップ証明を含む署名スキームを活用することで、プライバシーを保護するための匿名性と、資金洗浄対策（AML）等で実社会において求められるシビル耐性の確保といった、自己主権型アイデンティティに求められる課題の多くが、本研究で示した暗号学的アプローチによって解決できることを示したと結論づけている。

Ⅱ. 論文審査結果の要旨

本論文は、情報社会における個人認証の基盤を成すと期待される自己主権型アイデンティティの問題に関し、個人が自身の情報を高度にコントロールする権利を拡大し、プライバシー保護とシビル耐性と呼ばれるなりすましや人格創造等の不正に対応するための、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、2024 年 2 月 15 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 2 月 17 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。