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　：　Privacy-Preserving Blockchain with Homomorphic Encryption
申請者　：　三谷 辰雄
審査委員会　：　主査　教授　有田 正剛
副査　准教授　首藤 一幸（東京工業大学）
副査　教授　土井　洋
副査　教授　大塚　玲

Ⅰ. 論文内容の要旨

本論文は “Privacy-Preserving Blockchain with Homomorphic Encryption”（準同型暗号を用いたプライバシー保護ブロックチェーン）と題し、6 章からなっている。

第 1 章“Introduction”では、本論文の研究背景を述べている。ブロックチェーン、準同型暗号をこの 10 年で発見された重要なブレークスルー技術と位置付け、ブロックチェーンの未解決問題である取引の機密性と非連結性を解決するために準同型暗号を用いた動機を述べている。分散型台帳では各参加者が取引内容を確認する必要があり、これは取引の機密性・非連結性と矛盾する要求である。これらの矛盾する要求を同時に満たすためには、極めて柔軟な演算が可能な暗号技術が求められ、準同型暗号を用いたブロックチェーンを提案するに至った動機が述べられている。

第 2 章“Building blocks”では、準備として、本論に必要な RLWE 暗号とゼロ知識証明について、その定義、暗号学的仮定と主要な補題について述べている。

第 3 章“Traceability in permissioned blockchain”では、許可型ブロックチェーンにおける機密性と透明性を同時に達成する方法について述べている。ここでは許可型ブロックチェーンの高スループットを活かしつつ、公開型ブロックチェーンの参加者に対して(1) 取引の機密性を保ちながら、(2) 許可型ブロックチェーン内での流通量の不変性、(3) 許可型ブロックチェーンの参加者が特定取引への非関与であることを証明可能とすることで、トレーサビリティを実現できることを明らかにしている。論文では、隠れマルコフモデルに基づいてトレーサビリティをモデル化し、ブートストラップ不要な準同型暗号で暗号化モデルを構築している。このとき、平文モデルにおける高次等式の成立を、暗号化モデルにおける高次多項式の値がゼロの暗号文集合に含まれるという等価な関係を用いて、Benhamouda らの知識のゼロ知識証明で解決している。

第 4 章“Confidential and auditable payments”では、公開型ブロックチェーンにおいて、取引情報を秘匿したまま、裁判所や当局による監査を可能にする方法を明らかにしている。匿名取引に関しては既に Zerocoin, Zerocash, Zether などが知られているが、いずれも裁判所や当局による監査には対応できない。そこで、高次等式の成立をゼロ知識証明可能な RLWE 暗号を用いることで、全ての取引を暗号文として台帳に記載することで、自然に取引の機密性と監査可能性を両立する方式を示している。提案方式について、匿名性は Zerocoin で導入された Ledger Indistinguishability を満たし、システムの安全性はゼロ知識証明の健全性への帰着が示されている。

第 5 章“Anonymous probabilistic payment in payment hub”では、匿名性を保ちつつ公開型ブロックチェーンで大幅にスループットを向上できる確率的ペイメントが実現可能であることを明らかにしている。確率的ペイメントは、大量の小額決済処理の負荷抑制を目的として Wheeler や Rivest らによって提案された技術である。公開型ブロックチェーンにおいて、プライバシー保護と高スループットを同時に解決する研究は極めて少ない。完全準同型性を持つ新しい暗号プリミティブとして Ring Fractional Oblivious Transfer(RFOT)を導入することで、確率的ペイメントに求められる確率の不可塑性とプライバシー保護が両立できることを示している。プライバシー保護は TumbleBit で提案された、エポックでの k-匿名性に従い、取引仲介者である Tumbler に対しても取引当事者の対応の秘匿が可能なことを示している。
第 6 章“Conclusion”では、準同型暗号を用いたプライバシー保護ブロックチェーンの成果について要約し、これらによって取引の秘匿性を守りつつ、許可型ブロックチェーンと公開型ブロックチェーンの間のトレーサビリティの確保、プライバシー保護と監査可能性を両立する公開型ブロックチェーン、プライバシー保護と高スループットを両立する確率的ペイメントが構成できることから、実社会においてブロックチェーンの適用範囲拡大の際に求められる要求の多くが解決可能であることを示している。

Ⅱ. 論文審査結果の要旨

本論文は、情報社会の基盤技術になりつつあるブロックチェーンについて、プライバシー保護と透明性を両立しつつ、高いスループットを達成するための、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、令和 2 年 7 月 17 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、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。