審査の結果の要旨

氏名　　長沼　健

本博士論文は全五章からなる．第一章は，序章で分散台帳技術に関するセキュリティ・プライバシ上の課題を述べている．第二章では，量子計算機耐性を有するゼロ知識証明の構成と分散台帳への応用が述べられている．第三章では，信頼できる第三者(以下，TTP と称する)がいない状況下においてゼロ知識証明を構成する一般的な方法が提案され，既存方式への応用が述べられている．第四章では，分散台帳を利用するユーザ向けに，生体認証技術を用いた秘密鍵管理技術が提案されている．第五章では，分散台帳上でネッティング決済を行う方式が述べられている．

現在，分散台帳技術は新しい決済基盤として注目を集めているが，台帳情報のプライバシや秘密鍵の管理方法などセキュリティに関してはまだ課題が多い．分散台帳技術が広く安心・安全に利用されるためには，これらの課題を解決する事が不可欠である．本博士論文では，これらの課題に対して解決策を提案し，全ての提案方式に対して実機による実装を行い有効性の検証を行った．

第二章で提案されている量子計算機耐性を有するゼロ知識証明方式の構成について述べる．現在，多くの分散台帳では zk-SNARK と呼ばれるゼロ知識証明方式と，そのライブラリ libsnark が利用されている．このライブラリはペアリング暗号をベースにしており，離散対数問題の困難さを安全性の根拠としているため量子計算機に対する耐性を有していない．本博士論文では，量子計算機耐性を有する LWE (Learning with Error)暗号方式をベースとする zk-SNARK 方式を構成した．また，提案した方式を libsnark ライブラリ向けに実装し有効性を検証した．検証の結果，提案方式の計算処理には 300GB という多大なメモリを必要とするが，処理時間は数十から数百秒程度であるため，環境によっては十分実用に耐えるとの見通しを得た．

第三章で提案されている TTP が存在しない状況におけるゼロ知識証明の構成について述べる．前章の提案方式を含め，現在分散台帳で利用されているゼロ知識証明方式は，TTP によるシステムパラメータの設定を必要とする．元来，TTP を排除する事が分散台帳の目的であったため，ゼロ知識証明の利用にあたっても可能な限り TTP を必要としない方式が望ましい．本博士論文では，ベクトルコミットメント方式からゼロ知識証明を構成する一般的な手法を提案した．また，ベクトルコミットメント方式のシステムパラメータ設定に，TTP が必要なければ，ゼロ知識証明の構成自体にも TTP が必要ない事を示した．システムパラメータの設定に TTP を必要としないベクトルコミットメント方式として，Pedersen コミットメント方式，Ajtai コミットメント方式が知られている．これらコミットメント方式を利用する事で，TTP 不要なゼロ知識証明が構成可能な事を示した．また実機での処理性能評価の結果，実運用にはあと 10 倍程度の高速化が必要な事が示された．高速化は今後の課題としている．

第四章で提案されている生体認証を用いた秘密鍵管理技術を述べる．分散台帳では，本人認証のために秘密鍵情報を用いた PKI ベースの認証が行われているが，万が一，秘密鍵を紛失した場合，台帳上の資産も同時に失う問題がある．本博士論文では，この秘密鍵管理の問題に対して，生体情報から電子署名を生成する技術を用いた解決方法，及びシステムアーキテクチャを提案した．この技術を利用する事で，生体情報を秘密鍵として利用できるため，秘密鍵をユーザが保存する必要が無くなり秘密鍵の紛失リスクを軽減する事が可能である．

第五章で提案されている分散台帳上でネッティング決済を行うプロトコルについて述べる．現状，金融機関間の決済は日本銀行などの中央機関が行っている．これら決済を分散台帳上で実行する場合，不特定多数の参加者に決済の内容が漏洩する問題が発生する．本博士論文では，乱数を用いたマルチパーティ計算を提案し，処理内容を秘匿したまま決済を行うプロトコルを提案した．

本論文の第二章と第三章は吉野雅之，國廣昇，井上淳雄，松岡幸典，岡崎嶺明，第四章は高橋健太，加賀陽介，鈴木貴之，吉野雅之，國廣昇，第五章は吉野雅之，佐藤尚宜，山田仁志男，鈴木貴之，國廣昇との共同研究であるが，論文提出者が主体となり貢献を行っている．そのため，論文提出者の寄与が十分であり，博士（科学）の学位を授与できると認める．

以上１８３４字