先端科学技術研究科　修士論文要旨

所属研究室 （主指導教員）	大規模システム管理 （笠原　正治　（教授））		
学籍番号	2411180	提出日	令和 8年 1月 14日
学生氏名	知念　朋輝		
論文題目	zkSABER: ブロックチェーンにおける生体特徴量表現を用いたゼロ知識簡潔生体認証		

要旨

ブロックチェーン上での生体認証の実現には，透明性に起因するプライバシー侵害のリスクとブロックガスリミットによる計算リソース制約の二つの主要な課題が存在する．そこで本稿では，特徴量ベクトルの次元数に依存せず証明サイズおよび検証コストを定数オーダー（O(1)）に抑えた，プライバシー保護可能なブロックチェーン生体認証方式 zkSABER を提案する．提案方式は，マークルツリーを用いた匿名メンバシップ証明とコサイン類似度に基づく生体照合証明を単一のzkSNARK回路上で統合する．これにより，ユーザは自身のアイデンティティや生体情報を秘匿にしたまま，登録されたグループの正当なメンバであることかつ入力された生体情報が登録テンプレートと一致することを第三者に対してゼロ知識で証明可能となる．さらに，本来は実数値（浮動小数点数）で表現されるDNNモデルの特徴量をzkSNARKでの処理に適した有限体上の表現へ変換する量子化パイプラインを導入する．評価実験の結果，特徴量ベクトルの次元数に関わらず，トランザクションのガスコストおよび証明サイズが一定であることに加え，高次元ベクトル特有の量子化耐性により低ビットでも精度が維持されることを実証した．これにより，検討コストと認証精度を高度に両立させた，実用的なオンチェーン生体認証の実現を示した．