SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

eKYC における安全な失効機能 - 中央銀行デジタル通貨のプライバシー保護
Secure Revocation Features in eKYC - Privacy Protection in Central Bank Digital Currency

宝木 和夫 * 久保田 隆 † ウォルゲムト スベン ‡ 梅澤 克之 §
Kazuo Takaragi Takashi Kubota Sven Wohlgemuth Katsuyuki Umezawa
小柳 洋貴 § 渡邊 創 *
Hiroki Koyanagi Hajime Watanabe

キーワード eKYC、中央銀行デジタル通貨、PKI、ブロックチェーン、匿名クレデンシャル、ゼロ知識証明

あらまし

スマートフォンの普及、あるいは、COVID-19 の影響などにより、デジタルトランスフォーメーションの動きが加速している。 金融業界では、世界中で 1 年間にマネーロンダリングされる金額は全世界 GDP の 2.7%に達するとの報告がある。これらの対応として行われる規制強化策を考慮すると、金融などの業務を効率的かつ安全に行うためには、eKYC（Electronic Know Your Customer）の機能を強化する必要性が高い。eKYC とは、銀行口座の開設やクレジットカードの申し込みなどの際にオンラインでのみ行われる本人確認方法のことをいう。

階層型 PKI を使用して eKYC に適用可能な暗号システムの研究が進んでいる。そこで、ルート認証局からローカル認証局へのクレデンシャル発行と認証のチェーンが生成される。ゼロ知識証明を適用してルート認証局のみを開示するだけでエンドユーザー認証を可能にする、委任可能な匿名認証メカニズムが開発された。これは、ユニバーサル構成可能性モデル (universal composability model) で安全であることが証明されており、階層型 PKI において特定のローカル認証局の存在を秘匿にするのに役立つ。これとは別に、属性を単に非表示にするのではなく、特定の数値範囲内にあることを証明するゼロ知識証明の開発が最近かなり進んでいる。

本研究では、さまざまなセキュリティドメインにわたって情報授受を行う際、ユーザーのプライバシーを保護するために、委任可能な匿名クレデンシャルとゼロ知識範囲証明を組み合わせる。このメカニズムを政府発行の国民 ID カードに組み込んだうえで eKYC に適用する基本的な方法を提案する。この方法では、ユーザーは、セキュリティドメインをまたいで複数の PKI 組織から、生体認証、資産、時刻などの属性の認証をプライバシーが保護された形で取得する。そして、取得されたユーザーの個人情報が取引相手に必要以上に開示されるのを防ぐため、ゼロ知識範囲証明によってユーザの属性の値そのものを開示することなく、特定の範囲内にあることのみを取引相手に証明する。

このゼロ知識範囲証明をタイムスタンプサーバにより刻印される 2 つの時刻（署名提示、公開鍵の有効/失効）の不等式関係の判定に用いる。つまり、国民 ID カード使用時に、氏名等の個人情報が隠された形で登録情報が失効、あるいは、非失効であることが証明される。本研究により、自己主権アイデンティティ管理に基づく持続可能な金融システムの実現を可能にすることを目指す。

* 産業技術総合研究所, サイバーフィジカルセキュリティ研究センター, 〒 135-0064 東京都江東区青海 2 − 4 − 7 臨海副都心センター, CPSEC, AIST Tokyo Waterfront, 2-4-7 Aomi, Koto-ku, Tokyo 135-0064, Japan
† 早稲田大学大学院法務研究科, 〒 169-8050 東京都新宿区西早稲田 1-6-1 169-8050, Waseda Law School, 1-6-1, Nishi-waseda, Shinjuku-ku, Tokyo, 169-8500, Japan
‡ セコム株式会社 IS 研究所, 東京都三鷹市下連雀 8-10-16 〒 181-8528, Intelligent Systems Laboratory, SECOM CO., Ltd., 8-10-16 Shimorenjaku, Mitaka-shi, Tokyo 181-8528, Japan
§ 湘南工科大学, 神奈川県藤沢市辻堂西海岸 1-1-25, Shonan Institute of Technology, 1-1-25 Tsujido-Nishikaigan, Fujisawa, Kanagawa 251-8511, Japan