様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　６ 年　 ６ 月 １２ 日現在

機関番号：１２１０２
研究種目：研究活動スタート支援
研究期間：2023～2023
課題番号：２３Ｋ１９９５２

研究課題名（和文）復号が確率的に制御可能な暗号スキームの研究

研究課題名（英文）Research on Cryptographic Schemes with Probabilistically Decryptable Encryption Scheme

研究代表者
高橋　大成（Takahashi, Taisei）

筑波大学・システム情報系・助教

研究者番号：５０９７５６１２

交付決定額（研究期間全体）：（直接経費）　　1,100,000円

研究成果の概要（和文）：本研究では，復号が事前に定められた確率でのみ可能な，新しい暗号スキームの開発を行ってきた．具体的には，Verifiable Secret Sharing，Commited Oblivious Transfer等の既存の暗号技術を発展させ，暗号を作成する側が不正を行うことができないよう，復号者側にて暗号文が適切に作成されたか検証を行う仕組みを考案した．研究成果としては，国内シンポジウムに参加し，暗号スキームを"Oblivious Encryption"と命名し発表を行った．

研究成果の学術的意義や社会的意義
本研究では，復号を確率的に制御可能な，新しいタイプの暗号スキームの開発を行ってきた．従来，暗号では適切な鍵を持つ参加者は確率1で復号を行うことが可能である．本研究は，事前に合意された確率でのみ復号を可能とする．本提案手法を利用することで，強いプライバシーが求められる電子マネーにおいて，マネーロンダリング等の犯罪を，確率的に操作可能にすることや，新たなデータ共有基盤の構築を可能とする．

研究成果の概要（英文）：In this research, I have developed a new cryptographic scheme where decryption is possible only with a predetermined probability. Specifically, I have developed existing cryptographic techniques such as Verifiable Secret Sharing and Commited Oblivious Transfer and considered a mechanism to verify that the ciphertext was properly created by the decrypter so that the encrypter cannot cheat. As a result of our research, I participated in a symposium in Japan and presented our cryptographic scheme, "Oblivious Encryption."

研究分野：情報セキュリティ

キーワード：情報セキュリティ　暗号　ブロックチェーン

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

ブロックチェーンや電子通貨の研究は幅広く行われており，近年では利用者のプライバシーを保護する技術が発展している．一般的に，通貨の利用者間の送金履歴や送金額は暗号化されており，第三者は閲覧することができず，追跡ができない仕組みが設けられている．これらの仕組みは善良な利用者の保護を目的としている．悪意ある利用者については，一つのコインを二重に利用するといった不正を発見し，発見後は参加者をシステムから排除する仕組みが設けられている．電子通貨が社会で広く普及するためには，マネーロンダリング等の，一見すると不正ではないグレーゾーンの犯罪に対しての対応策が必要となる．例として，海外への高額な送金は監査対象とし，送金の目的等を把握するためには送金者，受取人を捜査機関が閲覧可能とすべきであるが，現状の電子通貨では，高いプライバシーによって捜査が困難となっている．

先行研究では，通常は匿名であるが，一定期間内に一定額以上の送金のみは，捜査機関が監査対象とすることのできる仕組みが提案された[1]．しかし，悪意ある参加者は，少額を大量に送金することで，監査対象になることを免れることができる．プライバシーを保護しつつ，柔軟な監査を可能とする技術については，研究が行われていない．

２．研究の目的

プライバシーを保護しつつ，柔軟な監査を可能とするためには，送金額に応じて確率的に捜査機関に身元が開示される仕組みがあればよい．少額の送金であっても，大量であれば，いずれ送金者の身元が開示される．そこで本研究では，あらかじめ合意した確率で復号が可能となる，新しい暗号スキームの開発を行う．送金者は，自身の ID 情報を暗号化し，送金時に暗号文を付与する．受信者は暗号文を監査機関に送信し，監査機関は確率的に送金者の身元を把握することが可能となる．本研究では，暗号文が適切に作成されているか，確かに確率的に復号が可能であるかといった，暗号文を作成する側が不正を行っていないか検証可能とする仕組みを設ける．

３．研究の方法

本研究では確率的に復号可能な暗号文を作成するため，既存の暗号技術である Verifiable Secret Sharing (VSS)，Commited Oblivious Transfer(COT)等を組み合わせ，確率的な復号を可能にするための暗号スキームを考案した．

(1)　暗号文の生成：
単体のファイルとしての暗号文を生成し，それを復号者に送信する手法は，復号者の計算能力に応じて確率が変動するため，確率を制御する方法がない．本研究では，暗号文を作成する側が復号者と双方向に通信して，暗号文を送信する仕組みを考案した．VSS は検証可能な Secret Sharing 方式であり，秘密情報（平文）を n 個のシェアに分け，n 個の内 k 個のシェアが集まれば，秘密情報を得ることができる暗号スキームである．また，各シェアが適切に作成されているか，シェアを受け取った側で検証可能にしている．COT は不正防止機能のある Oblivious Transfer である．Oblivious Transfer では，送信者は 2 つのメッセージを持つ．受信者はどちらかを選択し選択した側を得ることができるが，選択しなかった方のメッセージは得ることができない．また送信者は，どちらのメッセージを受信者が得たかを知ることができない．COT では，送信者側で 2 つのメッセージのどちらかが確かに送信されたことを，受信者側で検証可能にする手法である．本研究では，まず秘密のメッセージを VSS で n 個のシェアに変換し，COT で各メッセージを乱数とともに COT で送信する仕組みを提案した．これにより，受信者は n 個のうち k 個以上のシェアを得ることができたならば，平文を得ることができる．

(2)　復号の確率的制御：
VSS と COT では，ともにメッセージを Pedersen 型コミットメントに変換して利用することが可能である．本研究では，シェアを Pedersen 型コミットメントにして送信することで，COT で送信される 2 つのメッセージのうち，片方が確かに VSS のシェアであり，適切に作成されたものであるかを，受信者で検証可能としている．これにより，受信者側で確かに暗号文が事前に合意した確率で復号できることを検証可能とした．

４．研究成果

暗号文の生成，および確率的制御について，研究成果を国内の学会(A)で発表した．

(A)Taisei Takahashi, Akira Otsuka, and Kazumasa Omote, "Oblivious Encryption: Toward an encryption scheme where decryption can be probabilistically controllable," 暗号と情報セキュリティシンポジウム (SCIS 2024), 3C2-1, 長崎県長崎市, 2024 年 1 月 23-26 日.

参考文献

[1] Karl Wu ¨st et al. “Platypus: A Central Bank Digital Currency with Unlinkable Trans- actions and Privacy-Preserving Regulation.” In ACM CCS ’22, ACM, 2022.

５．主な発表論文等

〔雑誌論文〕　計0件

〔学会発表〕　計1件（うち招待講演　0件／うち国際学会　0件）

１．発表者名 Taisei Takahashi, Akira Otsuka, and Kazumasa Omote
２．発表標題 Oblivious Encryption: Toward an encryption scheme where decryption can be probabilistically controllable
３．学会等名 暗号と情報セキュリティシンポジウム (SCIS 2024)
４．発表年 2024年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関