転売ヤーに制約を課すチケットシステム実現のための暗号プロトコル

佐古 美由紀[1,a)]　金廣 理央[1]　吉村 昌也[1]　岩本 貢[1]　渡邉 洋平[1,2]

概要：2019 年にチケット不正転売禁止法が施行されたにもかかわらず，依然としてチケット転売サイトには定価の何倍もの価格でチケットが出品されているのが現状である．そこで本研究では，チケット転売者側の抑制を目指した暗号学的枠組み FRESNO を提案する．FRESNO はチケット購入者の本人確認とプライバシー保護を暗号学的に両立するプロトコルであり，本人確認にはチケット購入者の個人情報を必要とする．そのため，チケットの転売にはチケット購入者が自身の個人情報を共有する必要があり，それによって不正転売の抑制につながることが期待できる．本稿では，FRESNO のモデル，安全性を定式化し，その定義を満たす証明可能安全な構成法を提案する．

キーワード：不正転売対策，証明可能安全性，ゼロ知識証明

Cryptographic Protocol for a Secure Ticket System against Scalper Resale

Miyuki Sako[1,a)]　Rio Kanehiro[1]　Masaya Yoshimura[1]　Mitsugu Iwamoto[1]　Yohei Watanabe[1,2]

Abstract: In 2019, the Act on Prohibiting the Unauthorized Resale of Specified Show and Event Tickets was enforced. Nevertheless, many tickets are still being sold at prices higher than the original on resale platforms. In this paper, we propose a cryptographic protocol for a secure ticket system against scalper resale, called FRESNO. FRESNO simultaneously achieves identity verification of ticket purchasers, called users, and protection of their privacy in a cryptographic way. To prove the possession of a legitimate ticket, FRESNO requires users to know (or possess) their personal information tied to the ticket. Therefore, scalpers are required to share their personal information to transfer tickets, which is expected to deter unauthorized ticket resale. In this paper, we formalize the model of FRESNO and the requirements of correctness and security, and propose a provably secure construction that meets these definitions.

Keywords: Countermeasures against Unauthorized Ticket Resale, Provable Security, Zero-Knowledge Proof

1. はじめに

1.1 研究背景

不正転売とは，興行主の事前の同意を得ず，反復継続の意思をもって，販売価格を超える価格で転売する行為のことをいう．転売目的で興行入場券（以下，チケットと表す）を入手し高額で転売する転売者が台頭することで，イベント参加目的の正当な観客への適正価格でのチケットの流通を滞らせることになる．転売者の台頭によりチケットが入手困難になりやすくなる上，転売者から購入するチケットは高額になることもある．さらに興行主も観覧者数減少などの不利益を被っている．不正転売によりチケットの適正な流通が滞ってしまうため，不正転売の防止策として「特

[1] 電気通信大学
The University of Electro-Communications
[2] 国立研究開発法人 産業技術総合研究所
National Institute of Advanced Industrial Science and Technology
[a)] m-sako@uec.ac.jp

定興行入場券の不正転売の禁止等による興行入場券の適正な流通の確保に関する法律 [2]」(チケット不正転売禁止法と呼ばれる) が 2019 年 6 月に施行され，転売目的でのチケットの譲り受けと不正転売に対して罰則が設定されたが，依然として不正転売は横行しており，引き続き議論及び対策が必要である．また，現在のチケットの不正転売の対応は各興行主に依存し，統一的な対策が取られているわけではないが，その多くは本人確認の徹底により本人のみ入場を許可するようにすると共に，行けなくなった場合のための公式リセール機能の導入を行っている．

本人確認の徹底により，転売者からのチケットは入場不可になるという懸念を生じさせることができるため，転売チケットの買い手側の抑制をすることができる．しかし，本人確認を徹底することで入場に時間を要するため，しばしば全員ではなくランダムに選んだ一部の入場者の確認のみ実施される．このような運用上の課題のため，現状全ての転売を防ぐことができているわけではない．そこでこれまでの対策を相補的に埋めるような追加の対策を考える．具体的には，暗号学的な観点から，転売チケットの売り手側の抑制を行うと共に本人確認徹底の効率的な実現を目指す．

1.2 本研究の目的と貢献

本研究の目標は「チケット不正転売を抑制する証明可能安全なプロトコルを構成する」ことである．不正転売が元々出来ないようなシステムの構築や，不正転売を検知・チケットの無効化することによる不正転売の完全な防止策を実現することが理想的な目標だが，不正転売の定義自体が難しいことから，本研究では不正転売をすることによって経済的または社会的な不利益を被るような，不正転売を抑制できる暗号プロトコル FRESNO (Framework for unauthorized RESale deterrent and aNOnymous identity verification) を提案する．FRESNO は従来のチケット発券から入場に至るまでにわたる暗号プロトコルであり，入場時の正規のチケットを所有することを証明する際に，チケットに紐づけられた個人情報も知っていることが必要となる点が特徴である．そのためチケットの譲渡には個人情報の開示が必要となることから，チケットの不正転売の抑制につながると考える．具体的には，FRESNO のモデル及び安全性を定義し，またその安全性が証明できるような構成を提案する．ID ベース署名に，署名から ID（個人情報）が漏れないという匿名性の要件を追加したタグ付き ID ベース署名とゼロ知識証明プロトコルを部品として用いた一般的構成法を提案する．

1.3 関連研究との比較

上述したような本人確認や公式リセールといった運用上の対策や法律に加え，チケット不正転売に対する研究はいくつかなされている．例えば西山らの顔認証ソフトウェアを用いたチケット本人確認システム [8] では本人確認に顔認証システムを用いて転売防止に効果のあるシステムが提案された．顔認証システムを用いて本人確認の正確性が高まると，転売チケットを購入しても入場できない懸念を生むことができるため，転売チケット購入者に対して制約を課すことができる．

また，チケット購入後にイベントに参加できなくなった場合に定価でチケットを売ることのできる公式リセールに対するアプローチを行う研究も存在する．中川らが提案したチケット管理システム [6] では，ブロックチェーンと電子署名技術を用いてチケット転売に関わるチケット管理システムを提案している．このような基盤を作り上げることによって，定価でのチケット購入希望者のための機能を提供することができる．しかし，このような機能が提供されていても，より高い金額でのチケット転売者とチケット購入希望者の取引に制約を課すことは難しい．坂之下らが提案したチケット管理システム [7] では，不正転売を完全に防ぐことは難しいという考えから，転売者が得た利益から所定の割合を，アーティストや運用側に還元する仕組みを提案した．他にも，梅本らは入場後に金銭授受を伴う座席交換を防ぐためのシステムを提案した [9]．このシステムによって入場後の不正転売を抑制することができる．本研究では，チケット転売者（転売ヤー）に制約を課すことに焦点を当てた，暗号学的な観点から入場前に不正転売を抑制できるチケットシステムを初めて提案する．その意味で，本提案はこれまでになされてきた上記の（特にチケット購入者に着目した）不正転売対策に取って代わるものではなく，それらと併用可能な相補的対策である．

2. 暗号要素技術

2.1 ゼロ知識証明

ゼロ知識証明 [4] とは，ある命題が真であることを，それ以上の情報を明かすことなく証明する暗号プロトコルである．形式的には，命題 x が以下に示す言語 $\mathcal{L}$ に属していることを，$x \in \mathcal{L}$ 以上の情報を明かさずに証明することが目的とする．

$$\mathcal{L} = \{x \mid \exists w \text{ such that } (x, w) \in R_{\mathcal{L}}\}.$$

ここで，$R_{\mathcal{L}} \subseteq \{0,1\}^* \times \{0,1\}^*$ は **NP 関係**と呼ばれる．ゼロ知識証明では，命題 $x \in \mathcal{L}$ が成り立つことを，対応する証拠 w の内容を一切開示することなく，証明することが可能である．特に本稿では以下のものを考える．

定義 1 (ゼロ知識証明アーギュメント)**.** ゼロ知識証明アーギュメント (Zero-Knowledge Argument: ZKA) $\langle \mathcal{P}, \mathcal{V} \rangle_{\mathrm{ZKA}}$ とは，証明者 $\mathcal{P}$ と PPT 検証者 $\mathcal{V}$ 間で NP 関係 $(x, w) \in R_{\mathcal{L}}$ を証明する対話プロトコルであり，次の 3 つの性質を満たす．

完全性: $x \in \mathcal{L}$ ならば，証明者 $\mathcal{P}$ は有効な証拠 w を持っており，検証者 $\mathcal{V}$ を納得できる．すなわち，任意の $(x, w) \in R_{\mathcal{L}}$ に対して，$\Pr[\langle \mathcal{P}(x, w), \mathcal{V}(x) \rangle = 1] = 1 - \alpha(\lambda)$ が成り立つ．本稿では一貫して $\alpha(\lambda) = 0$ とする．

健全性: $x \notin \mathcal{L}$ ならば，どんな確率的多項式時間証明者 $\mathcal{P}^*$ も，検証者 $\mathcal{V}$ を納得させることができない．すなわち，任意の確率的多項式時間アルゴリズム $\mathcal{P}^*$，任意の $x \notin \mathcal{L}$ に対し，$\Pr[\langle \mathcal{P}^*(x), \mathcal{V}(x) \rangle = 1] < \mathsf{negl}(\lambda)$ が成り立つ．

ゼロ知識性: 証明者 $\mathcal{P}$ と検証者 $\mathcal{V}$ の対話を証拠 w を用いずに模倣することができる．すなわち，任意の確率的多項式時間検証者 $\mathcal{V}^*$ に対して，シミュレーター Sim が存在し，任意の $(x, w) \in R_{\mathcal{L}}$ に対して，$\langle \mathcal{P}(x, w), \mathcal{V}^*(x) \rangle \approx_c \mathsf{Sim}(x)$ が成り立つ．

2.2 ID ベース署名

ID ベース署名（Identity-Based Signatures: IBS）[1], [3], [5] とは，任意の文字列を用いて検証可能なディジタル署名である．

$\mathcal{ID}$ を ID 空間とする．IBS は 4 つのアルゴリズム $\Pi_{\mathrm{IBS}} = (\mathrm{IBS.KG}, \mathrm{IBS.EXT}, \mathrm{IBS.SIGN}, \mathrm{IBS.VRFY})$ で構成される．

$\mathrm{IBS.KG}(1^\lambda) \to (\mathrm{PK}, \mathrm{SK})$; セキュリティパラメータ λ を入力とし，マスター公開鍵 PK とマスター秘密鍵 SK を出力する．

$\mathrm{IBS.EXT}(\mathrm{SK}, \mathsf{id}) \to \mathrm{USK}[\mathsf{id}]$; 入力 SK と $\mathsf{id} \in \mathcal{ID}$ に対して，識別子 $\mathsf{id} \in \mathcal{ID}$ の秘密鍵 USK[id] を出力する．

$\mathrm{IBS.SIGN}(\mathrm{USK}[\mathsf{id}], \mathrm{m}) \to \mathrm{SIG}$; ユーザ秘密鍵 USK[id] とメッセージ m を入力とし，m に対する署名 SIG を出力する．

$\mathrm{IBS.VRFY}(\mathrm{PK}, \mathsf{id}, \mathrm{m}, \mathrm{SIG}) \to \mathbf{1/0}$; 入力 PK, id, m および署名 SIG に対して，1 または 0 を出力する．

検証正当性． Π_{IBS} は以下の検証正当性を要求する．

定義 2 (検証正当性)．任意の $\lambda \in \mathbb{N}$，任意の $\mathsf{id} \in \mathcal{ID}$，任意の m に対して，$\mathrm{IBS.VRFY}(\mathrm{PK}, \mathsf{id}, \mathrm{m}, \mathrm{SIG}) = 1$ を満たすとき，Π_{IBS} は検証正当性を満たすという．ただし，$(\mathrm{PK}, \mathrm{SK}) \leftarrow \mathrm{IBS.KG}(1^\lambda), \mathrm{USK}[\mathsf{id}] \leftarrow \mathrm{IBS.EXT}(\mathrm{SK}, \mathsf{id}), \mathrm{SIG} \leftarrow \mathrm{IBS.SIGN}(\mathrm{USK}[\mathsf{id}], \mathrm{m})$ である．

存在的偽造不可能性． IBS 方式 Π_{IBS} に対する存在的偽造不可能性ゲームを図 1 で定義する．ここでオラクル $O_{\mathrm{IBS.EXT}}$ は以下のように定義する．

$O_{\mathrm{IBS.EXT}(\cdot)}$ クエリ id に対して，$\mathrm{IBS.EXT}(\mathrm{SK}, \mathsf{id})$ を実行して得られた USK[id] を返す．

定義 3 (存在的偽造不可能性)．任意の確率的多項式時間偽造者 $\mathcal{F}$ に対して，以下のアドバンテージ $\mathsf{Adv}^{\mathsf{EUF\text{-}CMA}}_{\Pi_{\mathrm{IBS}}, \mathcal{F}}(\lambda)$ が λ に関して無視できるほど小さい場合，Π_{IBS} は存在的偽造不可能性を満たすという．

$$\mathsf{Adv}^{\mathsf{EUF\text{-}CMA}}_{\Pi_{\mathrm{IBS}}, \mathcal{F}}(\lambda) := \Pr\left[\mathsf{Exp}^{\mathsf{EUF\text{-}CMA}}_{\Pi_{\mathrm{IBS}}, \mathcal{F}}(\lambda) = 1\right].$$

$\mathsf{Exp}^{\mathsf{EUF\text{-}CMA}}_{\Pi_{\mathrm{IBS}}, \mathcal{F}}(\lambda)$

1: $(\mathrm{PK}, \mathrm{SK}) \leftarrow \mathrm{IBS.KG}(1^\lambda)$
2: $(\mathsf{id}^*, \mathrm{m}^*, \mathrm{SIG}^*) \leftarrow \mathcal{F}^{O_{\mathrm{IBS.EXT}}}(\mathrm{PK})$
3: $b' \leftarrow \mathrm{IBS.VRFY}(\mathrm{PK}, \mathsf{id}^*, \mathrm{m}^*, \mathrm{SIG}^*)$
4: **return** b'

図 1 IBS の存在的偽造不可能性ゲーム
Fig. 1 The unforgeability game for IBS

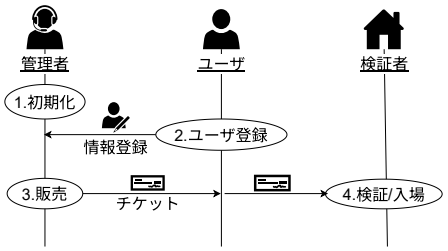

図 2 一般的なチケット流通の流れ
Fig. 2 General Flow of Ticket Distribution

3. 不正転売抑制プロトコル FRESNO

以下のモデルに登場する人物は，チケットの発行を行う**チケット管理者**（以下，単に管理者）と入場資格者であるかどうか検証し入場を許可する**チケット検証者**（以下，単に検証者）と**ユーザ**に分類される．ユーザの中にはチケットシステムからチケットを購入したチケット購入者と，チケットを購入していない非チケット購入者に振り分けられる．さらにチケット購入者のうちチケットを転売する者を転売者といい，非チケット購入者のうち転売者から転売チケットを譲り受ける者を転売チケット購入者とする．また別の指標として，ユーザの中には入場資格者と非入場資格者が混在しており，チケットに紐づく証明情報を有するユーザを入場資格者と呼ぶ．

3.1 一般的なチケット流通の流れ

FRESNO は図 2 で示す般的なチケット流通の流れに基づいた暗号プロトコルである．まず，管理者がイベントを行うための情報を作成し，公開する．次に，ユーザは管理者に対して必要な情報を送信し，管理者はユーザの情報を登録する（ユーザ登録）．続いて，管理者はユーザの中からチケットを購入する権利のある者を選び，各購入者に有効なチケットを発行する．入場時には，ユーザがチケットを提示して本人確認を受ける．入場資格者であることが証明で

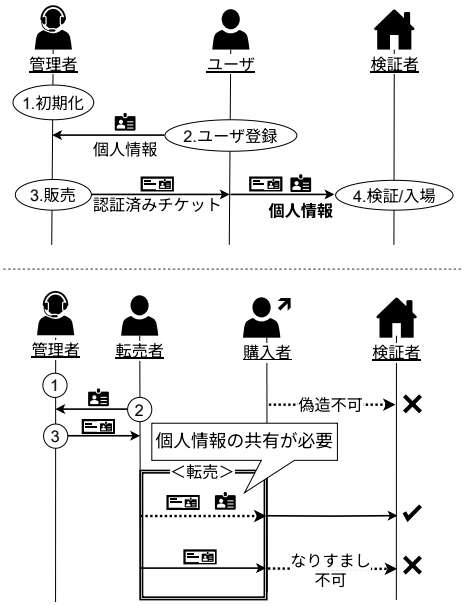

図 3 提案方式 FRESNO の流れ（上図：正規利用時，下図：転売時）
Fig. 3 Flow of FRESNO (Upper Diagram: Regular case, Lower Diagram: Resale case)

きれば入場を許可し，できなければ入場を拒否する．

3.2 FRESNO の概要

従来の手法では身分証の提示や事前に登録した顔写真との照合などにより本人確認を実施しており，また上記の流れではチケット購入者の非チケット購入者へのチケットの転売・譲渡の防止や，本人確認におけるなりすましを防ぐことができない．そこで，FRESNO では，チケットが正規のものであるかどうかの検証に事前に登録した情報を必須とする（図 3 参照）．ここで事前に送信する情報を**個人情報**とし，他人には明かしたくない情報であると仮定する（別のサービスなどと併せて利用することで，適当な情報は登録できないものとする）．提案方式である FRESNO ではチケットの転売にはチケット購入者が自身の個人情報を共有する必要があるため，この仮定が成り立つ限り，不正転売の抑制につながることが期待できる．なお，個人情報を知らずになりすますことは暗号理論的に防止する．一方で，検証時に個人情報が必要であることは，すなわち検証者に個人情報を渡さなければ検証ができないことを意味する．実際の運用を考えれば多くの検証者が必要となり，アルバイト等，社会的責任の小さい人間が担当する可能性を考える．従来行われている身分証確認による本人確認であれば，物理的なものを提示するため個人情報が悪用される可能性は低いが，電子データの場合は複製が容易であり，悪用されることを考慮する必要がある．そのため，個人情報は必要だがその開示は不要とする検証アルゴリズムとすることで検証者への信頼がなくても検証可能にする．

3.3 不正転売抑制プロトコル FRESNO のモデル

FRESNO は $\Pi_{\mathsf{FRESNO}} = (\mathrm{Init}, \mathrm{Add}, \mathrm{Sign}, \mathrm{IVrfy})$ の 4 つのアルゴリズムの組で構成される．以下にプロトコルの流れと合わせてモデルを説明する．

3.3.1 初期化（管理者）

管理者がイベントを行うための情報を作成し公開する．管理者はセットアップアルゴリズム **Init** を実行し，マスター公開鍵 mvk とマスター秘密鍵 msk を得る．マスター公開鍵 mvk は公開し，マスター秘密鍵 msk は管理者が厳正に管理する．

$\mathbf{Init}(1^{\lambda}) \to (\mathbf{mvk}, \mathbf{msk})$; セキュリティパラメータ λ を入力とし，マスター公開鍵 mvk とマスター秘密鍵 msk を出力する．

3.3.2 ユーザ登録（管理者とユーザ）

ユーザが個人情報を含む情報を管理者に送付する．ここで前提として，管理者の個人情報の取り扱いについて信頼し，ユーザに正しく紐づく個人情報を送付することとする．ユーザ登録では，ユーザは自身の個人情報 P_i を（安全な通信路を用いて）管理者に送付する．

管理者は送付された個人情報 P_i を用いて，ユーザ登録アルゴリズム **Add** を動かし管理者用データベース mDB を更新する．ここで，管理者用データベース mDB はユーザ識別子 i と個人情報 P_i で構成され，管理者はユーザの個人情報 P_i を厳正に管理する．

$\mathbf{Add}(\mathbf{mvk}, \mathbf{msk}, \mathbf{mDB}, \boldsymbol{i}, \boldsymbol{P_i}) \to \mathbf{mDB'}$; 個人情報の集合を $\mathcal{P}$ とする．マスター鍵 $(\mathsf{mvk}, \mathsf{msk})$ と管理者データベース mDB，ユーザの識別子 i，ユーザの個人情報 $P_i \in \mathcal{P}$ を入力とし，更新されたデータベース mDB' を出力する．

3.3.3 販売（管理者とチケット購入者）

管理者は先着や抽選などでチケット購入者を決め，チケット M_j を振り分ける．チケットには整理番号や席番号などのチケット購入者固有に割り当てられた情報が含まれ，チケット番号 j は管理上の通し番号とする．

管理者は各チケット購入者に対して認証済みチケット発行アルゴリズム **Sign** を動かして検証用トークン t と認証済みチケット $\hat{M}_i$ を発行するが，チケット購入者には認証済みチケット $\hat{M}_i$ のみ送付する．検証用トークン t は検証者用データベース vDB に登録し，更新する．

$\mathbf{Sign}(\mathbf{mvk}, \mathbf{msk}, \boldsymbol{i}, \mathbf{mDB}, \boldsymbol{M_j}, \mathbf{vDB}) \to (\boldsymbol{\hat{M}_i}, \boldsymbol{t}, \mathbf{vDB'})$; チケット番号の集合を $\mathcal{M}$ とする．マスター鍵 $(\mathsf{mvk}, \mathsf{msk})$ とユーザの識別子 i，管理者データベース mDB，チケット番号 $M_j \in \mathcal{M}$，検証用データベース vDB を入力とし，認証済みチケット $\hat{M}_i$ とその検証用トークン t，更新された検証用データベース vDB' を出力する．

3.3.4 検証/入場（検証者とユーザ）

入場では，ユーザは検証者に対して認証済みチケット $\hat{M}_i$ を提示し，検証者はその正当性を確認する．この際，ユーザは $\hat{M}_i$ を発行時に用いられた個人情報 P_i と検証用トークン t が正しく紐付いていることを，検証者に納得させる必要がある．素朴な方法として，ユーザが $P_i, \hat{M}_i$ を検証者に渡して検証者に検証してもらう方法があるが，P_i が検証者の手に渡り，プライバシーが失われる．そこで，本方式では，対話型の検証アルゴリズムを定義し，ゼロ知識証明的に P_i の情報を明かすことなく検証を実行する．具体的には，ユーザ $\mathcal{U}_{\mathsf{FRE}}$ および検証者 $\mathcal{V}_{\mathsf{FRE}}$ 間の対話を $\langle \mathcal{U}_{\mathsf{FRE}}(P_i, \hat{M}_i), \mathcal{V}_{\mathsf{FRE}}(\mathsf{mvk}, \mathrm{vDB}, \hat{M}_i)\rangle$ と表し，略して $\mathrm{IVrfy}(P_i, \hat{M}_i; \mathsf{mvk}, \mathrm{vDB}, \hat{M}_i)$ とも書く．

$\mathbf{IVrfy}(P_i, \hat{M}_i; \mathsf{mvk}, \mathrm{vDB}, \hat{M}_i) \to 0/1$；ユーザ $\mathcal{U}_{\mathsf{FRE}}$ は $P_i, \hat{M}_i$ を入力とし，検証者 $\mathcal{V}_{\mathsf{FRE}}$ は $\mathsf{mvk}, , \mathrm{vDB}, \hat{M}_i$ を入力とし，対話を通じて P_i（と検証用データベース vDB 内の対応する検証用トークン t）が $\hat{M}_i$ に正しく紐付いていることを証明する．このアルゴリズムの出力は $\mathcal{V}_{\mathsf{FRE}}$ の最終出力であり，受理の場合は 1，拒否の場合は 0 を返す．

3.4 FRESNO の正当性/安全性要件

以上のモデルから，満たすべき要件を整理する．

3.4.1 検証正当性

検証正当性とは，正当なユーザに対して，アルゴリズムに従って正しく発行されたチケットが，検証アルゴリズムにおいて必ず受理することである．つまり，個人情報 P_i に紐づく正当なチケットであることを個人情報 P_i，検証用トークン t，およびマスター公開鍵 mvk を用いれば検証アルゴリズムと対話検証アルゴリズムを実行した場合，いずれも受理することを意味する．

定義 4 (検証正当性)．全ての $\lambda \in \mathbb{N}$，全ての $(\mathsf{mvk}, \mathsf{msk}) \leftarrow \mathrm{Init}(1^\lambda)$，全ての $P_i \in \mathcal{P}$，全ての $M_j \in \mathcal{M}$ に対して，以下が確率 1 で成り立つとき，Π_{FRESNO} は検証正当性を満たすという．

$$\langle \mathcal{U}_{\mathsf{FRE}}(P_i, \hat{M}_i), \mathcal{V}_{\mathsf{FRE}}(\mathsf{mvk}, \mathrm{vDB}', \hat{M}_i)\rangle = 1.$$

ここで，$\mathrm{mDB}' \leftarrow \mathrm{Add}(\mathsf{mvk}, \mathsf{msk}, \mathrm{mDB}, i, P_i)$，$(\hat{M}_i, t, \mathrm{vDB}') \leftarrow \mathrm{Sign}(\mathsf{mvk}, \mathsf{msk}, i, \mathrm{mDB}', M_j, \mathrm{vDB})$ である．

3.4.2 偽造不可能性

偽造不可能性とは，悪意のあるユーザに対して，マスター秘密鍵 msk なしで検証を通るような認証済みチケットを作れないことである．図 4 の偽造不可能性ゲームでは自身の個人情報から認証済みチケットを偽造することを考える．

ここでオラクル O_{Sign} は以下のように定義する．

$O_{\mathbf{Sign}(\cdot,\cdot)}$　個人情報 P_i とチケット番号 M_j を入力し，まず P_i がデータベースに登録されているかを確認し，そうでなければ $\mathrm{Add}(\mathsf{mvk}, \mathsf{msk}, \mathrm{mDB}, i, P_i)$ を実行して P_i を登録する．次に，既に P_i に対して認証済みチケット $\hat{M}_i$ を発行しているかどうかをリスト List から確認し，そうでなければチケット番号 M_j に対して，新しい認証済みチケット $\hat{M}_i \leftarrow \mathrm{Sign}(\mathsf{mvk}, \mathsf{msk}, i, \mathrm{mDB}, M_j, \mathrm{vDB})$ を生成して返す．リスト List を用意し，タプル $(P_i, M_j, \hat{M}_i)$ を追加する．

$\mathsf{Exp}^{\mathsf{UNF}}_{\Pi_{\mathsf{FRESNO}},\mathcal{F}}(\lambda)$

1 : $(\mathsf{mvk}, \mathsf{msk}) \leftarrow \mathrm{Init}(1^\lambda)$
2 : $(P_i^*, \hat{M}_i^*, \Omega^*) \leftarrow \mathcal{F}^{O_{\mathrm{Sign}}}(\mathsf{mvk})$
3 : **if** $(P_i^*, \cdot, \hat{M}_i^*) \notin$ List **then**
4 : $\quad \mathrm{res} \leftarrow \langle \Omega^*(P_i^*, \hat{M}_i^*), \mathcal{V}_{\mathsf{FRE}}(\mathsf{mvk}, \mathrm{vDB}, \hat{M}_i)\rangle$
5 : $\quad$ **return** res
6 : **return** 0

図 4　FRESNO の偽造不可能性ゲーム
Fig. 4　The unforgeability for FRESNO

$\mathsf{Exp}^{\mathsf{ImpRes}}_{\Pi_{\mathsf{FRESNO}},\mathcal{F}}(\lambda)$

1 : $(\mathsf{mvk}, \mathsf{msk}) \leftarrow \mathrm{Init}(1^k)$
2 : $(M_j^*, \mathrm{st}) \leftarrow \mathcal{F}^{O_{\mathrm{Sign}}}(\mathsf{mvk})$
3 : **if** $(\cdot, M_j^*, \cdot) \notin$ List **then**
4 : $\quad P_i^* \leftarrow\!\!\$\ \mathcal{P}$
5 : $\quad \mathrm{mDB}' \leftarrow \mathrm{Add}(\mathsf{mvk}, \mathsf{msk}, \mathrm{mDB}, i, P_i^*)$
6 : $\quad (\hat{M}_i^*, t^*, \mathrm{vDB}') \leftarrow \mathrm{Sign}(\mathsf{mvk}, \mathsf{msk}, i, \mathrm{mDB}', M_j^*, \mathrm{vDB})$
7 : $\Omega^* \leftarrow \mathcal{F}^{O_{\mathrm{Sign}}}(\hat{M}_i^*, \mathrm{st})$
8 : $\mathrm{res} \leftarrow \langle \Omega^*(\hat{M}_i^*), \mathcal{V}_{\mathsf{FRE}}(\mathsf{mvk}, \mathrm{vDB}, \hat{M}_i^*)\rangle$
9 : **return** res

図 5　FRESNO のなりすまし耐性ゲーム
Fig. 5　The impersonation resilience game for FRESNO

定義 5 (偽造不可能性)．任意の確率的多項式時間で動作する攻撃者 $\mathcal{F}$ に対して，アドバンテージ

$$\mathrm{Adv}^{\mathsf{UNF}}_{\Pi_{\mathsf{FRESNO}},\mathcal{F}}(\lambda) = \Pr\left[\mathsf{Exp}^{\mathsf{UNF}}_{\Pi_{\mathsf{FRESNO}},\mathcal{F}}(\lambda) = 1\right]$$

が λ に関して無視できるほど小さい場合，Π_{FRESNO} は偽造不可能性を満たすという．

3.4.3 なりすまし耐性

なりすまし耐性では，悪意のあるユーザに対して，発行した認証済みチケットに対して，マスター秘密鍵 msk と紐づいた個人情報なしで検証時に受理されないことを意味する．なりすまし耐性ゲームを図 5 で定義する．

定義 6 (なりすまし耐性)．任意の確率的多項式時間で動作する攻撃者 $\mathcal{F}$ に対して，アドバンテージ

$$\mathrm{Adv}^{\mathsf{ImpRes}}_{\Pi_{\mathsf{FRESNO}},\mathcal{F}}(\lambda) = \Pr\left[\mathsf{Exp}^{\mathsf{ImpRes}}_{\Pi_{\mathsf{FRESNO}},\mathcal{F}}(\lambda) = 1\right]$$

が λ に関して無視できるほど小さい場合，Π_{FRESNO} はなりすまし耐性を満たすという．

$\mathsf{Exp}^{\mathsf{ANON}}_{\Pi_{\mathsf{FRESNO}},\mathcal{A}}(\lambda)$

1: $(\mathsf{mvk}, \mathsf{msk}) \leftarrow \mathrm{Init}(1^k)$
2: $(P_0^*, P_1^*, M_j^*, \mathrm{st}) \leftarrow \mathcal{A}^{O_{\mathrm{Sign}}}(\mathsf{mvk})$
3: $b^* \leftarrow\!\!\$\ \{0,1\}$
4: $\mathrm{mDB}' \leftarrow \mathrm{Add}(\mathsf{mvk}, \mathsf{msk}, \mathrm{mDB}, i, P_b^*)$
5: $(\hat{M}_i^*, t^*, \mathrm{vDB}') \leftarrow \mathrm{Sign}(\mathsf{mvk}, \mathsf{msk}, i, \mathrm{mDB}', M_j^*, \mathrm{vDB})$
6: $b' \leftarrow \mathcal{A}^{O_{\mathrm{Sign}}, O_{\mathrm{IVrfy}}}(\hat{M}_i^*, \mathrm{st})$
7: **if** $b' = b^*$ **then**
8: **return** 1
9: **else then**
10: **return** 0

図 6 FRESNO の匿名性ゲーム
Fig. 6 The anonymity game for FRESNO

3.4.4 匿名性

匿名性とは，正当なユーザに対して，検証時に個人情報を漏らさないことを要求する．匿名性ゲームを図 6 で定義する．ここでオラクル O_{IVrfy} は以下のように定義する．

$\boldsymbol{O_{\mathbf{IVrfy}(\cdot)}}$ アルゴリズム Ω を入力に取り，個人情報 P_{b^*} と認証済みチケット $\hat{M}_i^*$ を入力した $\mathcal{U}_{\mathsf{FRE}}$ と対話検証アルゴリズム $\langle \mathcal{U}_{\mathsf{FRE}}(P_{b^*}, \hat{M}_i^*), \Omega(\mathsf{mvk}, \mathrm{vDB}, \hat{M}_i) \rangle$ を実行した結果を返す．

定義 7 (匿名性)．任意の確率的多項式時間で動作する攻撃者 $\mathcal{A}$ に対して，アドバンテージ

$$\mathrm{Adv}^{\mathsf{ANON}}_{\Pi_{\mathsf{FRESNO}},\mathcal{A}}(\lambda) = \left| \Pr\left[\mathsf{Exp}^{\mathsf{ANON}}_{\Pi_{\mathsf{FRESNO}},\mathcal{A}}(\lambda) = 1 \right] - \frac{1}{2} \right|$$

が λ に関して無視できるほど小さい場合，Π_{FRESNO} は匿名性を満たすという．

4. FRESNO の一般的構成法

4.1 構成の概要

まず，有効なチケットを所持していることの証明としてディジタル署名を考える．ディジタル署名とはユーザが公開鍵と秘密鍵を作成し，秘密鍵で任意のメッセージに対して署名を生成したものを，他のユーザが公開鍵を用いて検証するものである．今回はチケットを管理者が発行することを考えると，管理者が公開鍵と秘密鍵を作成，秘密鍵でチケット番号に対して署名を生成し，チケット番号と署名の組を認証済みチケットとしてチケット購入者に送付し，入場の際に検証者が公開鍵で検証するということが考えられる．ここで，管理者は秘密鍵を厳重に管理するものとする．

上記のディジタル署名を用いたアプローチでは，有効なチケットであることは証明できるが，なりすましに対する対策が取られていない．すなわち，別のユーザからチケットとそれに対する署名を受け取り，自身のチケットと署名であると主張しても検証を通ってしまう．

そこで，他人に渡したくないであろう個人情報をもっていないと検証を通ることができない，つまり自分のチケットであることを証明できないようにすることを考える．そのようなディジタル署名として，メッセージと署名の他，検証の際に署名鍵に対応した任意の文字列が必要となる IBS を考える．この IBS を用いて，検証の際に個人情報の入力を必要とすることによって他人へのチケット譲渡を抑制することを考える．すなわち，チケットと署名だけがあっても正しいチケットであることは証明できず，本来のチケット所有者の個人情報も必要となることから，他人にチケットを譲渡しにくくなることを想定する．

一方で，検証の際に検証者にユーザの個人情報が漏れてしまうことを危惧すると，個人情報そのものは開示せず，認証済みチケットに紐づく個人情報を知っていることを示すことが要求される．このような要件を達成するために ZKA の導入を図る．ZKA を利用することで，チケットに対応する個人情報を知っているということを個人情報そのものの情報は明かさずに証明することが可能である．

また，認証済みチケット自体からチケット購入者の個人情報が漏れることを防ぐことも要求される．一般的な IBS においては，ID（今回でいう個人情報）は公開し秘匿することは想定していないため，署名から個人情報が漏れないようにすることは一般的な IBS の要件には含まれていない．このような IBS に匿名性の要件を追加したタグ付き ID ベース署名（Tagged Identity-Based Signatures: TIBS）を新たに提案し，一般的構成法に導入する．

以上の TIBS と ZKA の二つの暗号技術を用いて，他人へのチケット転売・譲渡を抑制するプロトコル FRESNO を構成する．

4.2 タグ付き ID ベース署名

TIBS とは，検証時に ID に加えて署名生成時に付与されたタグを用いる IBS である．TIBS は IBS と同じく 4 つのアルゴリズム $\Pi_{\mathrm{TIBS}} = (\mathrm{TIBS.KG}, \mathrm{TIBS.EXT}, \mathrm{TIBS.SIGN}, \mathrm{TIBS.VRFY})$ で構成されるが，そのうち署名生成アルゴリズム TIBS.SIGN と検証アルゴリズム TIBS.VRFY が異なるため，その 2 つだけ以下に説明する．

$\mathbf{TIBS.SIGN(USK[id], m) \rightarrow (}\boldsymbol{t}\mathbf{, SIG)}$; ユーザ秘密鍵 USK[id] とメッセージ m を入力とし，タグ t と m に対する署名 SIG を出力する．

$\mathbf{TIBS.VRFY(PK, id,}\ \boldsymbol{t}\mathbf{, m, SIG)} \rightarrow \mathbf{1/0}$; 入力 PK, id, m, t および署名 SIG に対して，1 あるいは 0 を出力する．

検証正当性． Π_{TIBS} は以下の検証正当性を要求する．

定義 8 (検証正当性)．任意の $\lambda \in \mathbb{N}$，任意の $\mathsf{id} \in \mathcal{ID}$，任意の m に対して，$\mathrm{TIBS.VRFY}(\mathrm{PK}, \mathsf{id}, t, \mathrm{m}, \mathrm{SIG}) =$

$\mathsf{Exp}^{\mathsf{ANO\text{-}CMA}}_{\Pi_{\mathrm{TIBS}},\mathcal{A}}(\lambda)$

1 : $(\mathrm{PK},\mathrm{SK}) \leftarrow \mathrm{TIBS.KG}(1^\lambda)$
2 : $(\mathsf{id}_0^*, \mathsf{id}_1^*, \mathrm{m}^*, \mathrm{st}) \leftarrow \mathcal{A}^{O_{\mathrm{TIBS.EXT}}}$
3 : $b \leftarrow\!\!\$\ \{0,1\}$
4 : $(t^*, \mathrm{SIG}^*) \leftarrow \mathrm{TIBS.SIGN}(\mathrm{USK}[\mathsf{id}_b^*], \mathrm{m}^*)$
5 : $b' \leftarrow \mathcal{A}^{O_{\mathrm{TIBS.EXT}}}(\mathrm{SIG}^*, \mathrm{st})$
6 : **if** $b' = b^*$ **then**
7 : **return** 1
8 : **else then**
9 : **return** 0

図 7 TIBS の匿名性ゲーム
Fig. 7 The anonymity game for TIBS

1 を満たすとき，Π_{TIBS} は検証正当性を満たすという．ただし，$(\mathrm{PK},\mathrm{SK}) \leftarrow \mathrm{TIBS.KG}(1^\lambda), \mathrm{USK}[\mathsf{id}] \leftarrow \mathrm{TIBS.EXT}(\mathrm{SK},\mathsf{id}), (t,\mathrm{SIG}) \leftarrow \mathrm{TIBS.SIGN}(\mathrm{USK}[\mathsf{id}],\mathrm{m})$ である．

存在的偽造不可能性． タグの存在以外，IBS のものと同様に定義されるため省略する．

匿名性． タグを知らない限り，署名から対応する ID の情報が漏れないことを匿名性と呼び，次のように定義する．TIBS 方式 Π_{TIBS} に対する匿名性ゲームを図 7 で定義する．ここでオラクル $O_{\mathrm{TIBS.EXT}}$ は以下のように定義する．

$\boldsymbol{O_{\mathrm{TIBS.EXT}(\cdot)}}$ クエリ id に対して，$\mathrm{TIBS.EXT}(\mathrm{SK},\mathsf{id})$ を実行して得られた $\mathrm{USK}[\mathsf{id}]$ を返す．

定義 9 (匿名性)．任意の確率的多項式時間攻撃者 $\mathcal{A}$ に対して，以下のアドバンテージ $\mathsf{Adv}^{\mathsf{ANO\text{-}CMA}}_{\Pi_{\mathrm{TIBS}},\mathcal{A}}(\lambda)$ が λ に関して無視できるほど小さい場合，Π_{TIBS} は匿名性を満たすという．

$$\mathsf{Adv}^{\mathsf{ANO\text{-}CMA}}_{\Pi_{\mathrm{TIBS}},\mathcal{A}}(\lambda) \coloneqq \left| \Pr\left[\mathsf{Exp}^{\mathsf{ANO\text{-}CMA}}_{\Pi_{\mathrm{TIBS}},\mathcal{A}}(\lambda) = 1\right] - \frac{1}{2} \right|.$$

4.3 FRESNO の構成

$\mathcal{ID}$ に対する $\Pi_{\mathrm{TIBS}} = (\mathrm{TIBS.KG}, \mathrm{TIBS.EXT}, \mathrm{TIBS.SIGN}, \mathrm{TIBS.VRFY})$ を TIBS とし，$\mathcal{P} \coloneqq \mathcal{ID}$ とする．$\langle \mathcal{P},\mathcal{V}\rangle_{\mathrm{ZKA}}$ を次の NP 言語に対する ZKA とする：$\mathcal{L}_{\mathrm{IBS}} = \{(\mathrm{m},\mathrm{SIG},t) \mid \exists \mathsf{id}$ such that $\mathrm{TIBS.VRFY}(\mathrm{PK},\mathsf{id},t,\mathrm{m},\mathrm{SIG}) = 1\}$．$\mathsf{H} : \mathcal{P} \to \mathcal{P}$ を暗号学的ハッシュ関数とする．これらを用い，$\Pi_{\mathsf{FRESNO}} = (\mathrm{Init},\mathrm{Add},\mathrm{Sign},\mathrm{IVrfy})$ を以下のように構成する．

$\mathrm{Init}(1^\lambda) \to (\mathsf{mvk},\mathsf{msk})$: $\mathrm{TIBS.KG}(1^\lambda)$ を実行し $(\mathrm{PK},\mathrm{SK})$ を得て，マスター公開鍵 $\mathsf{mvk} \coloneqq \mathrm{PK}$，マスター秘密鍵 $\mathsf{msk} \coloneqq \mathrm{SK}$ を出力する．

$\mathrm{Add}(\mathsf{mvk},\mathsf{msk},\mathrm{mDB},i,P_i) \to \mathrm{mDB}'$: 管理者データベース mDB に識別子と個人情報の組 (i,P_i) を追加し，mDB' として出力する．

$\mathrm{Sign}(\mathsf{mvk},\mathsf{msk},i,\mathrm{mDB},M_j,\mathrm{vDB}) \to (\hat{M}_i,t,\mathrm{vDB}')$: mDB より (i,P_i) を抽出し，$\mathrm{TIBS.EXT}(\mathsf{msk},P_i)$ を実行，$\mathrm{USK}[\mathsf{id}]$ を得る．次に $\mathrm{TIBS.SIGN}(\mathrm{USK}[\mathsf{id}],\mathrm{m}))$ を実行し，署名 SIG と検証用トークン t を得る．$\hat{M}_i \coloneqq (M_j \coloneqq \mathrm{m}, \sigma_i \coloneqq \mathrm{SIG}, \mathsf{H}(t))$ とし，検証用データベース vDB に $(\mathsf{H}(t),t)$ を登録，vDB' に更新する．$(\hat{M}_i,t,\mathrm{vDB})$ を出力する．

$\langle \mathcal{U}_{\mathsf{FRE}}(P_i,\hat{M}_i), \mathcal{V}_{\mathsf{FRE}}(\mathsf{mvk},\mathrm{vDB},\hat{M}_i)\rangle \to 0/1$: $\mathcal{U}_{\mathsf{FRE}}$ は $\mathsf{H}(t)$ を $\mathcal{V}_{\mathsf{FRE}}$ に送り，$\mathcal{V}_{\mathsf{FRE}}$ は検証者用データベース vDB から $\mathsf{H}(t)$ に対応する検証用トークン t を $\mathcal{U}_{\mathsf{FRE}}$ に返す．$\mathcal{U}_{\mathsf{FRE}}$ は $\mathcal{P}((M_j,\sigma_i,t),P_i)$ を，$\mathcal{V}_{\mathsf{FRE}}$ は $\mathcal{V}(M_j,\sigma_i,t)$ を実行し，$\mathcal{V}_{\mathsf{FRE}}$ は得られた出力を出力する．

4.4 正当性/安全性証明

提案した FRESNO の構成は，H をランダムオラクルとした上で，検証正当性，偽造不可能性，なりすまし耐性，匿名性を満たす[*1]．紙面の都合上，証明の概要のみ記す．

定理 1 (検証正当性)．TIBS Π_{TIBS} の検証正当性と ZKA $\langle \mathcal{P},\mathcal{V}\rangle_{\mathrm{ZKA}}$ の完全性が成り立つならば，提案プロトコル Π_{FRESNO} の検証正当性が成り立つ．

証明の概要． Π_{TIBS} の検証正当性から，$\langle \mathcal{P},\mathcal{V}\rangle_{\mathrm{ZKA}}$ の NP 言語 $\mathcal{L}_{\mathrm{IBS}}$ の正しさ，すなわちステートメント $x \in \mathcal{L}_{\mathrm{IBS}}$ の時かつその時に限り証拠 w が存在することが保証される．したがって，$\langle \mathcal{P},\mathcal{V}\rangle_{\mathrm{ZKA}}$ の完全性が成り立つならば，任意の $(\mathsf{mvk},\mathsf{msk}) \leftarrow \mathrm{TIBS.KG}(1^\lambda)$，任意の $P_i \in \mathcal{P}$，任意の $\mathrm{USK}[\mathsf{id}] \leftarrow \mathrm{TIBS.EXT}(\mathsf{msk},P_i)$，任意の $\mathrm{m} \in \mathcal{M}$，任意の $(t,\mathrm{SIG}) \leftarrow \mathrm{TIBS.SIGN}(\mathrm{USK}[\mathsf{id}],\mathrm{m})$ に対して，確率 1 で $\langle \mathcal{P}((\hat{M}_i,\mathrm{SIG},t),P_i), \mathcal{V}(\hat{M}_i,\mathrm{SIG},t)\rangle = 1$ が成り立つ． □

定理 2 (偽造不可能性)．TIBS Π_{TIBS} の存在的偽造不可能性と ZKA $\langle \mathcal{P},\mathcal{V}\rangle_{\mathrm{ZKA}}$ の健全性が成り立つならば，ランダムオラクルモデルの下で提案プロトコル Π_{FRESNO} の偽造不可能性が成り立つ．

証明の概要． FRESNO の偽造不可能性ゲームのチャレンジにて，攻撃者は $(P_i^*, \hat{M}_i^* = (M_j^*, \mathrm{SIG}^*, h^*), \Omega^*)$ の組を提出するが，Π_{TIBS} の存在的偽造不可能性より，この組が $\mathrm{TIBS.VRFY}(\mathrm{PK},P_i^*,t^*,\hat{M}_i^*) = 1$ を満たす確率は無視できるほど小さい[*2]，つまり圧倒的な確率で $(M_j^*,\mathrm{SIG}^*,t^*) \notin \mathcal{L}$ が成り立つ．また，$\langle \mathcal{P},\mathcal{V}\rangle_{\mathrm{ZKA}}$ の健全性より，全ての確率的多項式時間アルゴリズム Ω^* 及び全ての $(M_j^*,\mathrm{SIG}^*,t^*) \notin \mathcal{L}$ に対して，$\langle \Omega^*(P_i^*,\hat{M}_i^*), \mathcal{V}(M_j^*,\mathrm{SIG}^*,t^*)\rangle$ が 1 を出力する確率も無視できるほど小さい． □

定理 3 (なりすまし耐性)．TIBS Π_{TIBS} の偽造不可能性，匿名性と ZKA $\langle \mathcal{P},\mathcal{V}\rangle_{\mathrm{ZKA}}$ の健全性が成り立つならば，ラ

[*1] ハッシュ関数の代わりに疑似ランダム関数を用いることで標準モデルでも証明可能である．
[*2] すなわち，$h^* = \mathsf{H}(t^*)$ となるような t^* も見つけられない．

ンダムオラクルモデルの下で提案プロトコル Π_{FRESNO} のなりすまし耐性が成り立つ．

証明の概要． FRESNO のなりすまし耐性ゲームのチャレンジにて，偽造者 $\mathcal{F}$ はチケット番号 M_j^* に対してランダムに選ばれた P_i^* の認証済みチケット $\hat{M_i^*} = (M_j^*, \mathrm{SIG}^*, h^*)$ を得る．ここで，Π_{TIBS} の匿名性により，チャレンジで返す SIG^* をまったく異なる P_i' の署名 SIG' に置き換えることができる．この時点で，Π_{TIBS} の偽造不可能性から，圧倒的な確率で $(M_j^*, \mathrm{SIG}', t^*) \notin \mathcal{L}$ が成り立つ．また，h^* はタグ t^* をランダムオラクルに入力した結果であり，h^* から P_i^* の値が漏れることはない．したがって，P_i^* をランダムに推測し当てることができた場合を除き，$\mathcal{F}$ は Ω^* を提出する時点で P_i^* に関する情報を一切得られていない．$\langle \mathcal{P}, \mathcal{V} \rangle_{\mathrm{ZKA}}$ の健全性より，全ての確率的多項式時間アルゴリズム Ω^* 及び全ての $(M_j^*, \mathrm{SIG}', t^*) \notin \mathcal{L}$ に対して，$\langle \Omega^*(\hat{M_i^*}), \mathcal{V}(M_j^*, \mathrm{SIG}', t^*) \rangle$ が 1 を出力する確率は無視できるほど小さい． □

定理 4 (匿名性)**.** TIBS Π_{TIBS} の匿名性と ZKA $\langle \mathcal{P}, \mathcal{V} \rangle_{\mathrm{ZKA}}$ のゼロ知識性が成り立つならば，ランダムオラクルモデルの下で提案プロトコル Π_{FRESNO} の匿名性が成り立つ．

証明の概要． FRESNO の匿名性ゲームの O_{IVrfy} オラクルでは対話を通じて P_b^* と t が認証済みチケット $\hat{M_i^*}$ に紐づいているかどうかを検証するが，Π_{TIBS} の匿名性より認証済みチケット $\hat{M_i^*}$ から P_b^* の情報を得ることはできない．また，$\langle \mathcal{P}, \mathcal{V} \rangle_{\mathrm{ZKA}}$ のゼロ知識性より，IVrfy から証拠 P_b^* に関する情報を得ることはできない． □

4.5 タグ付き ID ベース署名の一般的構成法

本節は，4.2 節の TIBS が，2.2 節の IBS から構成できることを示す．ただし，用いる IBS の ID 空間が加法巡回群であり，そのサイズが指数的に大きくなくてはならない[*3]．

$\mathbf{TIBS.KG(1^\lambda) \to (PK, SK)}$: $\mathrm{IBS.KG}(1^\lambda)$ を実行し，得られた $(\mathrm{PK}, \mathrm{SK})$ を出力する．

$\mathbf{TIBS.EXT(SK, id) \to USK[id]}$: $\mathcal{ID}$ から一様ランダムに t を選び，$\overline{\mathrm{USK}}[\mathsf{id}+t] \leftarrow \mathrm{IBS.EXT}(\mathrm{SK}, \mathsf{id}+t)$ を実行，$\mathrm{USK}[\mathsf{id}] := (t, \overline{\mathrm{USK}}[\mathsf{id}+t])$ を出力する．

$\mathbf{TIBS.SIGN(USK[id], m) \to (t, SIG)}$: $\mathrm{SIG} \leftarrow \mathrm{IBS.SIGN}(\overline{\mathrm{USK}}[\mathsf{id}+t], \mathrm{m})$ を実行し，(t, SIG) を出力する．

$\mathbf{TIBS.VRFY(PK, id, t, m, SIG) \to 0/1}$: $\mathrm{IBS.VRFY}(\mathrm{PK}, \mathsf{id}+t, \mathrm{m}, \mathrm{SIG})$ の実行結果を出力する．

以下の定理が成り立つ．紙面の都合上，証明は割愛する．

定理 5. IBS Π_{IBS} の検証正当性が成り立つならば，TIBS Π_{TIBS} の検証正当性が成り立つ．

定理 6. IBS Π_{IBS} の存在的偽造不可能性が成り立つならば，TIBS Π_{TIBS} の存在的偽造不可能性が成り立つ．

定理 7. $\mathcal{ID}$ が加法巡回群であり，かつその位数がセキュリティパラメータ λ に対して指数的に大きいならば，TIBS Π_{TIBS} の匿名性が成り立つ．

[*3] 多くの既存 IBS 方式がこの条件を満たす．

5. おわりに

本稿では，チケット転売の抑制を目指した暗号プロトコル FRESNO を提案し，その定式化と構成を行った．チケット購入者側の抑制を目的とした既存対策とは異なり，FRESNO はチケット転売者側の抑制を目指したプロトコルである．今後の課題として，本研究で捉えきれていない運用上・実装上の課題を明確にし，更なる改良を行っていくことが挙げられる．

謝辞 CSS 2024 デモンストレーションセッションにて議論してくださった皆様に感謝いたします．本研究は JSPS 科研費 JP23H00468, JP23H00479, JP23K17455, JP23K21644, JP23K21668, JP23K24846 の助成，および JST CREST JPMJCR23M2 の支援を受けたものです．

参考文献

[1] Bellare, M., Namprempre, C. and Neven, G.: Security proofs for identity-based identification and signature schemes, *Journal of Cryptology*, Vol. 22, No. 1, pp. 1–61 (2009).
[2] GOV 法令検索：特定興行入場券の不正転売の禁止等による興行入場券の適正な流通の確保に関する法律 (2018). https://elaws.e-gov.go.jp/document?lawid=430AC0000000103.
[3] Galindo, D., Herranz, J. and Kiltz, E.: On the Generic Construction of Identity-Based Signatures with Additional Properties, *Advances in Cryptology - ASIACRYPT 2006*, LNCS, Vol. 4284, Springer, pp. 178–193 (2006).
[4] Goldwasser, S., Micali, S. and Rackoff, C.: The Knowledge Complexity of Interactive Proof Systems, *SIAM J. Comput.*, Vol. 18, No. 1, pp. 186–208 (1989).
[5] Shamir, A.: Identity-based cryptosystems and signature schemes, *Workshop on the theory and application of cryptographic techniques*, Springer, pp. 47–53 (1984).
[6] 中川紗菜美，佐古和恵，小出俊夫，梶ヶ谷圭祐：不正転売問題を配慮したブロックチェーンベースのチケット管理システムの提案，暗号と情報セキュリティシンポジウム 2018 予稿集 (2018).
[7] 坂之下未羽，松崎なつめ：チケットの二次流通と利益還元の提案，コンピュータセキュリティシンポジウム 2022 予稿集，pp. 1345–1351 (2022).
[8] 西山雄吾，奥村明俊，半田 享，星野隆道，津雲 淳，高木 剛，窪田清仁：顔認証ソフトウェアを用いたチケット本人確認システム，第 78 回全国大会講演論文集，情報処理学会，pp. 493–494 (2016).
[9] 梅本琉奈，松崎なつめ：チケットの中売り対策の提案，コンピュータセキュリティシンポジウム 2024 予稿集，pp. 69–75 (2024).