

# メッセージ依存開示可能グループ署名における トークンの偽造不可能性について

井村 優斗<sup>1,a)</sup> 江村 恵太<sup>1,2</sup>

**概要：**グループ署名は、グループに所属していることを匿名で証明可能な電子署名の一種であり、その拡張方式としてメッセージ依存開示可能グループ署名 (GS-MDO: Group Signatures with Message-Dependent Opening) が, Sakai ら (Pairing 2012) により提案されている。既存研究において, Sakai らにより, GS-MDO から ID ベース暗号が構成できること, Imura ら (CANS 2025) により, GS-MDO からタイムリリース暗号が直接構成できることが示されている。これらの結果は GS-MDO がグループ署名よりも強い暗号要素技術であることを示唆する証拠と考えられる。さらなる証拠として, 本論文では新たにトークンの偽造不可能性を導入し, GS-MDO が元来満たす安全性である開示者匿名性に含まれることを示す。

**キーワード：**メッセージ依存開示可能グループ署名, 偽造不可能性

## On Token Unforgeability of Group Signatures with Message-Dependent Opening

YUTO IMURA<sup>1,a)</sup> KEITA EMURA<sup>1,2</sup>

**Abstract:** Group signatures (GS) are a type of digital signature that enables anonymous proof of group membership. As an extension of GS, Group Signatures with Message-Dependent Opening (GS-MDO) were proposed by Sakai et al. (Pairing 2012). In previous works, Sakai et al. proved that GS-MDO implies Identity-Based Encryption, and Imura and Emura (CANS 2025) proved that GS-MDO also implies Timed-Release Encryption. These results provide evidence suggesting that GS-MDO is a stronger cryptographic primitive than GS. In this paper, we newly introduce the notion of token unforgeability and prove that it is implied by opener anonymity, a fundamental security property of GS-MDO. Our result strengthens prior works by clarifying a security property that GS-MDO implicitly realizes.

**Keywords:** Group Signatures with Message-Dependent Opening, Unforgeability

### 1. はじめに

**グループ署名.** グループ署名 [9] は, 署名者があるグループに所属していることを匿名で証明可能な電子署名の一種である。秘密鍵  $ok$  を持つ開示者のみが, 署名を開示して署名者を追跡可能である。グループ署名の安全性について, Bellare-Micciancio-Warinschi (BMW) によって完全匿名性

(Full Anonymity) と完全追跡可能性 (Full Traceability) を導入した BMW モデルが定義されている [5]。BMW モデルで安全なグループ署名は公開鍵暗号 (PKE: Public-Key Encryption), 署名, 非対話ゼロ知識証明から構成できることが知られている。また, 署名鍵が流出しても匿名性を保証する完全匿名性を満たすグループ署名から, 公開鍵暗号が構成できることが知られている [1]。

**GS-MDO.** グループ署名では開示者の秘密鍵  $ok$  さえあれば任意の署名に対して開示が可能である。これは開示者の権限が強すぎるという懸念がある。この開示者への権限集

<sup>1</sup> 金沢大学 Kanazawa University

<sup>2</sup> 産業技術総合研究所 National Institute of Advanced Industrial Science and Technology (AIST)

<sup>a)</sup> imuimu@stu.kanazawa-u.ac.jp

中を改善することを目的として、メッセージ依存開示可能グループ署名 (GS-MDO: Group Signatures with Message-Dependent Opening) [25] が提案されている。GS-MDO では、開示者に加えてアドミッターと呼ばれるエンティティを定義する。ok とアドミッターが発行するメッセージに依存したトークンが揃ってはじめて、署名者の追跡が可能となる。これまでにペアリングベースの GS-MDO 方式 [3, 19, 24], 格子ベースの GS-MDO 方式 [10, 20] が提案されている。

GS-MDO の応用例として、匿名オークションが挙げられる。オークションの入札者は、入札価格に対して GS-MDO を用いて署名を行い、そのグループ署名と入札価格をアドミッターに送信する。署名の開示にはトークンと ok の両方が必要であるため、アドミッターはユーザーを特定することなく、正当な参加者であるかどうかのみを確認する。このため、アドミッターには誰がいくら入札したのかという情報が漏洩しないという利点がある。ここでは、最高価格を入札したユーザーが落札者となると仮定する。アドミッターは最高価格に依存したトークンを生成し、それを開示者に送付する。開示者はこのトークンを用いて、オークションの落札者を特定することができる。一方で、入札価格に依存するトークンがなければ署名を開示できないため、開示者には落札できなかった入札者の情報が漏洩しないという利点がある。

GS-MDO が実現する“扱うコンテンツに依存した匿名性のコントロール”に関する関連研究として、Set Pre-Constrained グループ署名が提案されている [4, 23]。End-to-End (E2EE) Secure Messaging の文脈において、禁止されたメッセージをやり取りしない限り匿名性が保たれる。GS-MDO との大きな違いとして、禁止メッセージを定義するタイミングが挙げられる。GS-MDO では、基本的にはユーザがグループ署名を作成した後、そのメッセージに依存してトークンを作成することが想定されている。そのため、上記の匿名オークションにおける落札額のように、事前に開示対象メッセージを規定するのが難しい場合におけるアドホックな対応に適しているといえる。一方、Set Pre-Constrained グループ署名では、禁止コンテンツを事前に決定する。そのため、規約等で事前に禁止事項をコミットする場合に適している。

**GS-MDO の実現可能性.** 自然な疑問として、グループ署名を拡張した GS-MDO は、従来のグループ署名を構成するために必要な暗号学的道具立てよりも、より強力なものを必要とするのかという点が挙げられる。Sakai ら [25] は、GS-MDO から ID ベース暗号 (IBE: Identity-Based Encryption) を構成できることを示している。したがって、GS-MDO の構成には IBE が不可欠であるといえる。一方、Boneh ら [8] は、PKE から IBE へのブラックボッ

クス構成が存在しないことを示している。これらの事実から、GS-MDO はグループ署名よりも強力な暗号要素技術であることが示唆される。<sup>\*1</sup>

さらに、論文 [17] では、GS-MDO からタイムリリース暗号 (Timed-Release Encryption: TRE) を構成できることが示されている。この構成では、IBE からの TRE の一般的構成 [21, 22] を通すことなく GS-MDO から直接 TRE を構成している。さらに従来の TRE には備わっていない公開検証可能性が付与されている。この結果は、GS-MDO が本来持つ特性や機能性をより明確にするものであり、Sakai らの結果を強化するものといえる。

**研究動機.** IBE の秘密鍵は Naor 変換により署名とみなすことができる [6]。Sakai らの GS-MDO からの IBE の構成では GS-MDO のトークンを IBE の秘密鍵とするため、何等かの意味でトークンの偽造不可能性が備わっていると考えられる。しかしながらトークンの偽造不可能性については定式化されていない。GS-MDO が元来満たすと想定されるトークンの偽造不可能性を明確にすることは、GS-MDO が強い暗号要素技術であることを示唆するさらなる証拠となると考えられる。

さらに GS-MDO を用いた ID 管理システム [16] では、トークンをサービス提供証明書として用いる。もしこの証明書が偽装されると、サービスを利用していないユーザに対し利用料を請求することが可能となる。このシステムの安全性を理論的に保証するという意味においても、トークンの偽造不可能性を定式化することが望ましい。

**本論文の貢献.** 本論文では、トークンの偽造不可能性という新たなセキュリティ概念を導入する。この概念は、攻撃者が開示鍵 ok を保持していたとしても、トークンを偽造できないことを保証する。この安全性により、開示者がアドミッターから正当なトークンを取得しない限り、署名者を特定できないことを保証する。さらにトークンの偽造不可能性が開示者匿名性に含まれることを証明する。すなわち、トークンの偽造不可能性は GS-MDO に本質的に備わっている性質であり、GS-MDO が強い暗号要素技術であることのさらなる証拠を示したといえる。

## 2. GS-MDO の定義

本章では GS-MDO を定義する。本論文では論文 [17] のシンタックスを採用する。ここで Sakai ら [25] の定義では、開示鍵 ok とアドミッター鍵 ask は同じアルゴリズム GKg によって生成されていることに注意されたい。開示者とアドミッターが結託しないことを想定しているため、本論文では鍵生成を独立させることとする。

<sup>\*1</sup> なお非ブラックボックス構成にて公開鍵暗号相当から IBE を構成した結果も知られている [12, 13, 15]。そのため、GS-MDO がグループ署名よりも真に強い暗号要素技術とまではここでは主張せず、示唆されると表現した。

GS-MDO 方式 GS-MDO は以下で定義される 7 つのアルゴリズム (GS-MDO.Setup, GKg, AKg, GSig, Td, GVf, Open) から構成される。

**Definition 1** (Syntax of GS-MDO).

**GS-MDO.Setup:** セットアップアルゴリズムでは、セキュリティパラメータ  $\lambda$  を入力とし、共通パラメータ  $\text{pp}_{\text{GS-MDO}}$  を出力する。以降すべてのアルゴリズムで、明示しない場合でも  $\text{pp}_{\text{GS-MDO}}$  を入力すると仮定する。

**GKg:** グループ鍵生成アルゴリズムでは、 $\text{pp}_{\text{GS-MDO}}$  とグループのメンバ数  $n \in \mathbb{N}$  を入力とし、グループ公開鍵  $\text{gpk}$ ,  $\text{ok}$ , グループ署名鍵  $\{\text{gsk}_i\}_{i \in [n]}$  を出力する。

**AKg:** アドミッター鍵生成アルゴリズムでは  $\text{pp}_{\text{GS-MDO}}$  を入力とし、アドミッター公開鍵  $\text{apk}$  とアドミッター秘密鍵  $\text{ask}$  を出力する。

**GSig:** 署名生成アルゴリズムでは  $\text{gpk}$ ,  $\text{apk}$ ,  $\text{gsk}_i$ , メッセージ  $M$  を入力とし、グループ署名  $\sigma$  を出力する。

**Td:** メッセージ依存トークン生成アルゴリズムでは  $\text{ask}$ ,  $M$  を入力とし、トークン  $t_M$  を出力する。

**GVf:** 署名検証アルゴリズムでは、 $\text{gpk}$ ,  $\text{apk}$ , メッセージ  $M$  を入力とし、1 (受理) または 0 (拒否) を出力する。

**Open:** 署名者追跡アルゴリズムでは、 $M, \rightarrow \text{gpk}$ ,  $\text{apk}$ ,  $\text{ok}$ , メッセージ  $M$ , 署名  $\sigma$ , トークン  $t_M$  を入力とし、ユーザーインデックス  $i \in [n]$  または  $\perp$  を出力する。

正当性は以下のように定義される。すべての  $\text{pp}_{\text{GS-MDO}} \leftarrow \text{GS-MDO.Setup}(1^\lambda)$ ,  $(\text{gpk}, \text{ok}, \{\text{gsk}_i\}_{i \in [n]}) \leftarrow \text{GKg}(\text{pp}_{\text{GS-MDO}}, 1^n)$ ,  $(\text{apk}, \text{ask}) \leftarrow \text{AKg}(\text{pp}_{\text{GS-MDO}})$ ,  $M \in \{0, 1\}^*$ ,  $i \in [n]$  に対して GS-MDO が正当であるとは、 $\text{GVf}(\text{gpk}, \text{apk}, M, \text{GSig}(\text{gpk}, \text{apk}, \text{gsk}_i, M)) = 1$  かつ  $\text{Open}(\text{gpk}, \text{apk}, \text{ok}, M, \text{GSig}(\text{gpk}, \text{apk}, \text{gsk}_i, M), \text{Td}(\text{ask}, M)) = i$  が成り立つことを要求する。

GS-MDO では開示者匿名性とアドミッター匿名性の二つの安全性が定義されている。開示者匿名性は、すべてのグループ署名鍵  $\{\text{gsk}_i\}_{i \in [n]}$  と開示者の秘密鍵  $\text{ok}$  をもつ開示者であっても対応するトークンがない限り、ユーザー匿名性を破ることはできないことを保証する。アドミッター匿名性は、すべてのグループ署名鍵  $\{\text{gsk}_i\}_{i \in [n]}$  とアドミッター秘密鍵  $\text{ask}$  を持つアドミッターであってもユーザの匿名性を破ることはできないことを保証する。以下、開示者匿名性を定義する。アドミッター匿名性や追跡可能性の定義は論文 [25] を参照されたい。

**Definition 2** (開示者匿名性). 以下、 $\mathcal{A}$  を攻撃者、 $\mathcal{C}$  をチャレンジャーとする。

**Setup:**  $\mathcal{C}$  は  $\text{pp}_{\text{GS-MDO}} \leftarrow \text{GS-MDO.Setup}(1^\lambda)$ ,  $(\text{gpk},$

$\text{ok}, \{\text{gsk}_i\}_{i \in [n]}) \leftarrow \text{GKg}(\text{pp}_{\text{GS-MDO}}, 1^n)$ ,  $(\text{apk}, \text{ask}) \leftarrow \text{AKg}(\text{pp}_{\text{GS-MDO}})$  を実行し、 $(\text{gpk}, \text{ok}, \text{apk}, \{\text{gsk}_i\}_{i \in [n]})$  を  $\mathcal{A}$  に送る。

**Token Query (Phase I):**  $\mathcal{A}$  は  $M$  を送付する。 $\mathcal{C}$  は  $(M, t_M)$  が保存されているかを確認する。もし保存されていれば、その  $t_M$  を  $\mathcal{A}$  に返す。保存されていなければ、 $t_M \leftarrow \text{Td}(\text{ask}, M)$  を実行し、 $(M, t_M)$  のペアを保存後、 $t_M$  を  $\mathcal{A}$  に返す。

**Challenge:**  $\mathcal{A}$  は  $i_0, i_1 \in [n]$  と  $M^*$  を  $\mathcal{C}$  に送る。ただし  $\mathcal{A}$  は以前にトークンを要求した  $M$  に対してチャレンジを行うことは許されない。 $\mathcal{C}$  は  $b \xleftarrow{\$} \{0, 1\}$  を選び、 $\sigma^* \leftarrow \text{GSig}(\text{gpk}, \text{apk}, \text{gsk}_{i_b}, M^*)$  を実行、 $\sigma^*$  を  $\mathcal{A}$  に送る。

**Token Query (Phase II):**  $\mathcal{A}$  は  $M \neq M^*$  を送付する。 $\mathcal{C}$  は  $(M, t_M)$  が保存されているかを確認する。もし保存されていれば、その  $t_M$  を  $\mathcal{A}$  に返す。保存されていなければ、 $t_M \leftarrow \text{Td}(\text{ask}, M)$  を実行し、 $(M, t_M)$  のペアを保存後、 $t_M$  を  $\mathcal{A}$  に返す。

**Guess:**  $\mathcal{A}$  は  $b' \in \{0, 1\}$  を出力する。

任意の PPT 攻撃者  $\mathcal{A}$  に対し、利得

$$\text{Adv}_{\text{GS-MDO}, \mathcal{A}}^{\text{opener-anon}}(\lambda, n) = \left| \Pr[b' = b] - \frac{1}{2} \right|$$

が無視できるとき、GS-MDO は開示者匿名性を持つと定義する。

### 3. トークンの偽造不可能性

本章では新たにトークンの偽造不可能性を定義し、開示者匿名性がトークンの偽造不可能性を含んでいることを示す。このセキュリティモデルでは、攻撃者は  $\text{ask}$  を除く全ての鍵を持ち、トークンクエリを発行することが許されている。これは、開示者がアドミッターからトークン  $t_M$  を受け取る状況を想定している。トークンの偽造不可能性はアドミッターが生成していないトークンを開示者が作成できないことを保証する。

**Definition 3** (トークンの偽造不可能性).

**Setup:**  $\mathcal{C}$  は  $\text{pp}_{\text{GS-MDO}} \leftarrow \text{GS-MDO.Setup}(1^\lambda)$ ,  $(\text{gpk}, \text{ok}, \{\text{gsk}_i\}_{i \in [n]}) \leftarrow \text{GKg}(\text{pp}_{\text{GS-MDO}}, 1^n)$ ,  $(\text{apk}, \text{ask}) \leftarrow \text{AKg}(\text{pp}_{\text{GS-MDO}})$  を実行し、 $(\text{gpk}, \text{ok}, \text{apk}, \{\text{gsk}_i\}_{i \in [n]})$  を  $\mathcal{A}$  に送る。

**Token Query:**  $\mathcal{A}$  は  $\mathcal{C}$  に  $M$  を送る。 $\mathcal{C}$  は  $(M, t_M)$  が保存されているかを確認する。もし保存されていれば、その  $t_M$  を  $\mathcal{A}$  に返す。保存されていなければ  $t_M \leftarrow \text{Td}(\text{ask}, M)$  を実行し  $(M, t_M)$  のペアを保存後、 $t_M$  を  $\mathcal{A}$  に返す。

**Forge:**  $\mathcal{A}$  は  $(M^*, t_{M^*})$  を出力する.  $\mathcal{C}$  は  $i \xleftarrow{\$} [n]$  を選び,  $\sigma^* \leftarrow \text{GSig}(\text{gpk}, \text{apk}, \text{gsk}_i, M^*)$  を実行する.  $\text{Open}(\text{gpk}, \text{apk}, \text{ok}, M^*, \sigma^*, t_{M^*}) = i$  が成立し, かつ  $\mathcal{A}$  がトークンクエリとして  $M^*$  を送信していなかった場合,  $\mathcal{A}$  が勝利すると定義する.

任意の  $PPT$  攻撃者  $\mathcal{A}$  に対し, 利得

$$\text{Adv}_{\text{GS-MDO}, \mathcal{A}}^{\text{token-unforge}}(\lambda, n) = \Pr[\mathcal{A} \text{ wins}]$$

が無視できるとき, GS-MDO はトークンの偽造不可能性を持つと定義する.

次に開示者匿名性がトークンの偽造不可能性を含むことを証明する. 開示者匿名性は GS-MDO の本質的な安全性定義であることから, トークンの偽造不可能性も GS-MDO において本質的な安全性であるといえる.

**Theorem 1.** もし GS-MDO 方式が開示者匿名性を満たすならば, トークンの偽造不可能性を満たす.

**証明の方針.** 我々の証明は, IBE の復号鍵を署名とする Naor 変換の考え方をを用いている. IBE において, 復号鍵オラクルにアクセス可能な攻撃者がオラクルに問い合わせしていない ID の復号鍵を生成できれば, その攻撃者はチャレンジ暗号文を復号して IND-CPA 安全性を破ることができる. この手法に基づき, 以下の証明では, 帰着アルゴリズム  $\mathcal{B}$  が攻撃者  $\mathcal{A}$  の偽造トークンを用いて, チャレンジグループ署名に対する Open アルゴリズムを実行し, 開示者匿名性を破る.

*Proof.*  $\mathcal{C}$  を開示者匿名性のチャレンジャーとし,  $\mathcal{A}$  をトークン偽造不可能性の攻撃者とする.  $\mathcal{A}$  を用いて開示者匿名性を破るアルゴリズム  $\mathcal{B}$  を構成する.

**Setup:**  $\mathcal{C}$  は  $\text{pp}_{\text{GS-MDO}} \leftarrow \text{GS-MDO.Setup}(1^\lambda)$ ,  $(\text{gpk}, \text{ok}, \{\text{gsk}_i\}_{i \in [n]}) \leftarrow \text{GKg}(\text{pp}_{\text{GS-MDO}}, 1^n)$ , および  $(\text{apk}, \text{ask}) \leftarrow \text{AKg}(\text{pp}_{\text{GS-MDO}})$  を実行し,  $(\text{gpk}, \text{ok}, \text{apk}, \{\text{gsk}_i\}_{i \in [n]})$  を  $\mathcal{B}$  に与える.  $\mathcal{B}$  は  $(\text{gpk}, \text{ok}, \text{apk}, \{\text{gsk}_i\}_{i \in [n]})$  を  $\mathcal{A}$  に送信する.

**Token Query:**  $\mathcal{A}$  は  $M$  を  $\mathcal{B}$  に送信する.  $\mathcal{B}$  は  $M$  を  $\mathcal{C}$  に送信する.  $\mathcal{C}$  は  $t_M$  を  $\mathcal{B}$  に送信する.  $\mathcal{B}$  は  $t_M$  を  $\mathcal{A}$  に送信する.

**Forge:**  $\mathcal{A}$  は  $(M^*, t_{M^*})$  を出力する.

安全性モデルの規定上,  $\mathcal{A}$  はトークンクエリ  $M^*$  を  $\mathcal{B}$  に送信しない. そのため,  $\mathcal{B}$  もトークンクエリ  $M^*$  を  $\mathcal{C}$  に送信していないことより,  $M^*$  をチャレンジメッセージに指定可能である.  $\mathcal{B}$  はランダムに  $i_0, i_1 \in [n]$  を選択し, チャレンジとして  $(i_0, i_1, M^*)$  を  $\mathcal{C}$  に送信する.  $\mathcal{C}$  は  $b \xleftarrow{\$} \{0, 1\}$  を選択し, チャレンジグループ署名  $\sigma^* \leftarrow \text{GSig}(\text{gpk}, \text{apk}, \text{gsk}_{i_b}, M^*)$  を計算し,  $\sigma^*$  を  $\mathcal{B}$  に与える.  $\mathcal{A}$  はトークン偽造不可能性を破ることができるため,  $\text{Open}(\text{gpk}, \text{apk}, \text{ok}, M^*, \sigma^*, t_{M^*}) = i_b$

が成り立つ.  $\mathcal{B}$  は  $b$  を出力し, 開示者匿名性を破る.  $\square$

**強存在的偽造不可能性について.** トークンの偽造不可能性定義において, トークンオラクルに入力していない  $M^*$  に対し, 攻撃者は偽造トークンを出力する. これは署名における存在的偽造不可能性と同様の制限である. ここでは強存在的偽造不可能性, すなわち攻撃者がオラクルにクエリしたメッセージとその応答として得られたトークンの集合  $(M, t_M)$  に対し,  $(M^*, t_{M^*}) \notin (M, t_M)$  を要求する場合について議論する. ここで, IBE の復号鍵生成アルゴリズムが確率的である場合, 同じ ID に対して複数の秘密鍵を生成することが可能であることに着目する. もちろん秘密鍵である以上, どの秘密鍵を用いても ID を用いて作成された暗号文を復号可能である. 同様に, もし GS-MDO のトークン生成アルゴリズムが確率的である場合, 同じメッセージに対するグループ署名の署名者を開示可能な, 異なるトークンが生成される. より正確に, 同じ  $M^*$  に対する別のトークン  $t'_{M^*} \neq t_{M^*}$  を用いて,  $M^*$  に対するグループ署名の開示に利用可能である. 開示者の目的は署名者を特定することであり, 同じメッセージに対して複数のトークンを必要とする合理的な理由はないと考えられる. すでにアドミッターがあるメッセージに対してトークンを発行済みであるにもかかわらず, 開示者が同じメッセージに対して異なるトークンを生成しようとする状況は不自然であるといえる.

開示者匿名性との包含関係について, すでにクエリされたメッセージ  $M^*$  をチャレンジメッセージとして設定できないため, 開示者匿名性に直接は帰着できない. 今回, GS-MDO に元来備わっている安全性を明らかにすることを目的としている. そのため, 開示者匿名性に (直接は) 含まれない安全性を導入することは, 今回の目的に沿わない. したがって, アドミッターがトークンを発行していないメッセージに対して, 攻撃者が有効なトークンを生成できないことを要求する, 標準的な存在的偽造不可能性で十分であると考えられる. なお Ohara らによるペアリングベースの GS-MDO 方式 [24] では, トークンが Boneh–Lynn–Shacham (BLS) 署名 [7], Libert らによる格子ベースの GS-MDO 方式 [20] では, トークンが Gentry–Peikert–Vaikuntanathan (GPV) 署名 [14] である. BLS 署名や GPV 署名は強存在的偽造不可能であることが証明されている. したがって, Ohara らや Libert らの GS-MDO 方式におけるトークンは, 本論文で定義した偽造不可能性よりも強い安全性を満たす可能性がある. これらの精査は今後の課題とする.

#### 4. 議論: トークンの公開検証可能性について

本論文で定義したトークンの偽造不可能性は GS-MDO を用いた ID 管理システム [16] の安全性を理論的に保証す

るという意味において意義があると主張した。しかしこの ID 管理システムで要求する安全性とトークンの偽造不可能性にはまだギャップがある。本章では、そのギャップとしてトークンの公開検証可能性について議論する。

まず ID 管理システムの詳細について述べる。Issiki らのグループ署名を用いた ID 管理システム [18] においてサービスが提供される前でも課金可能である問題への対策として、グループ署名の代わりに GS-MDO を用いている。このシステムでは、サービス提供者がアドミッターと署名検証者の役割を果たす。ユーザーが作成したグループ署名をサービス提供者が検証し、ユーザーがグループに所属していることが確認された場合にサービスを提供する。ここで GS-MDO におけるトークンをサービス提供証明書としてユーザに送付する。その後、サービス提供者はサービス利用料を請求するために、サービス提供証明書を開示鍵を持つ請求書発行者に送付する（そのため、トークンはいかなる偽造不可能性を満たすことが必要であることは前述した）。請求書発行者は、自身の秘密鍵（開示鍵）とサービス提供証明書（トークン）を用いてグループ署名を開示し、ユーザーを特定して料金を請求する。

ここでユーザもサービス提供証明書の正当性を確認していることに着目する。論文 [16] では、サービス提供証明書の検証のためトークンは公開検証可能であると仮定、GS-MDO のシンタックスにトークン検証アルゴリズム TVf を追加している。具体的な方式として、Ohara らの GS-MDO 方式のトークンが BLS 署名であり、アドミッター公開鍵  $apk$  のみでトークンの検証が可能であることを利用して TVf アルゴリズムを記述している。

Ohara らの GS-MDO 方式 [24]、Libert らの GS-MDO 方式 [20] 以外の他の GS-MDO 方式 [3, 10, 19] でも、トークンは公開検証可能（トークンに対応する署名方式の検証アルゴリズムが公開鍵のみで実行可能という意味）である。この事実から、トークンの公開検証可能性も GS-MDO の安全性として自然なものであることが示唆され、GS-MDO が強い暗号要素技術であることのさらなる証拠となることが期待される。トークンの公開検証可能性の定式化とその証明を今後の課題とする。

## 5. 結論

本論文では、GS-MDO に新たな安全性概念であるトークンの偽造不可能性を導入し、それが開示者匿名性に含まれることを示した。これは、GS-MDO がグループ署名よりも強力な暗号要素技術であることを示唆するさらなる証拠であり、GS-MDO から IBE と TRE が構成できるという既存結果を強化する結果といえる。トークンの強存在的偽造不可能性や公開検証可能性の精査を今後の課題とする。

Certificateless Encryption (CLE) [2] では、鍵生成センタがユーザに秘密鍵を発行するとともに、各ユーザも自身の

公開鍵/秘密鍵を持つ。Chow ら [11] が言及しているように、TRE は CLE の構造を暗に含んでいる。しかし CLE と TRE の安全性モデルの差異に起因して直接 CLE から TRE を構成することは難しい。そこで Chow らは新たな CLE と TRE のモデルを提案している。論文 [17] にて GS-MDO が TRE を含むことが示されているが、Chow らの TRE モデルとの差異より、GS-MDO が CLE (Chow らのモデル) を含むことは直接は示されない。CLE と GS-MDO の関係性を示唆する他の結果として、Zhang ら [26] は群構造維持 CLE を提案、その応用として Group Signatures with Certified Limited Opening (GS-CLO) を提案している。複数の開示者を定義、どの開示者がグループ署名者を開示できるかをマスター認証者が（署名したコンテンツに応じて）決めることが可能な方式であり、GS-CLO は GS-MDO の一般化であると彼らは主張している。これらの結果は GS-MDO、GS-CLO、TRE、CLE の間にさらなる非自明な関係性が存在する可能性を示唆していると考えられる。これらの精査を今後の課題とする。

**謝辞** 本研究は電気通信普及財団研究調査助成の助成を受けたものです。

## 参考文献

- [1] Michel Abdalla and Bogdan Warinschi. On the minimal assumptions of group signature schemes. In *ICICS*, pages 1–13, 2004.
- [2] Sattam S. Al-Riyami and Kenneth G. Paterson. Certificateless public key cryptography. In *ASIACRYPT*, pages 452–473, 2003.
- [3] Hiroaki Anada, Masayuki Fukumitsu, and Shingo Hasegawa. Dynamic group signatures with message dependent opening and non-interactive signing. In *CAN-DAR*, pages 76–82. IEEE, 2022.
- [4] James Bartusek, Sanjam Garg, Abhishek Jain, and Guru-Vamsi Policharla. End-to-End secure messaging with traceability only for illegal content. In *EUROCRYPT Part V*, pages 35–66, 2023.
- [5] Mihir Bellare, Daniele Micciancio, and Bogdan Warinschi. Foundations of group signatures: Formal definitions, simplified requirements, and a construction based on general assumptions. In *EUROCRYPT*, pages 614–629, 2003.
- [6] Dan Boneh and Matthew K. Franklin. Identity-based encryption from the weil pairing. In *CRYPTO*, pages 213–229, 2001.
- [7] Dan Boneh, Ben Lynn, and Hovav Shacham. Short signatures from the weil pairing. In *ASIACRYPT*, pages 514–532, 2001.
- [8] Dan Boneh, Periklis A. Papakonstantinou, Charles Rackoff, Yevgeniy Vahlis, and Brent Waters. On the impossibility of basing identity based encryption on trapdoor permutations. In *FOCS*, pages 283–292. IEEE Computer Society, 2008.
- [9] David Chaum and Eugène van Heyst. Group signatures. In *EUROCRYPT*, pages 257–265, 1991.
- [10] Simin Chen, Jiageng Chen, Atsuko Miyaji, and Kaiming Chen. Constant-size group signatures with message-dependent opening from lattices. In *ProvSec*, pages 166–

185, 2023.

- [11] Sherman S. M. Chow, Volker Roth, and Eleanor Gilbert Rieffel. General certificateless encryption and timed-release encryption. In *SCN*, pages 126–143, 2008.
- [12] Nico Döttling and Sanjam Garg. From selective IBE to full IBE and selective HIBE. In *TCC Part I*, pages 372–408, 2017.
- [13] Nico Döttling and Sanjam Garg. Identity-based encryption from the Diffie-Hellman assumption. In *CRYPTO Part I*, pages 537–569, 2017.
- [14] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *ACM STOC*, pages 197–206, 2008.
- [15] Rishab Goyal, Venkata Koppula, and Mahesh Sreekrumar Rajasree. A note on adaptive security in hierarchical identity-based encryption. In *CRYPTO*, 2025, to appear.
- [16] Yuto Imura and Keita Emura. An identity management system using group signatures with message-dependent opening. In *AsiaJCIS*, pages 40–47. IEEE, 2024.
- [17] Yuto Imura and Keita Emura. Group signatures with message-dependent opening directly imply timed-release encryption. In *CANS*, 2025, to appear. Available at <https://eprint.iacr.org/2025/1356>.
- [18] Toshiyuki Isshiki, Kengo Mori, Kazue Sako, Isamu Teranishi, and Shoko Yonezawa. Using group signatures for identity management and its implementation. In *DIM*, pages 73–78. ACM, 2006.
- [19] Benoît Libert and Marc Joye. Group signatures with message-dependent opening in the standard model. In *CT-RSA*, pages 286–306, 2014.
- [20] Benoît Libert, Fabrice Mouhartem, and Khoa Nguyen. A lattice-based group signature scheme with message-dependent opening. In *ACNS*, pages 137–155, 2016.
- [21] Takahiro Matsuda, Yasumasa Nakai, and Kanta Matsuura. Efficient generic constructions of timed-release encryption with pre-open capability. In *Pairing-Based Cryptography*, pages 225–245, 2010.
- [22] Yasumasa Nakai, Takahiro Matsuda, Wataru Kitada, and Kanta Matsuura. A generic construction of timed-release encryption with pre-open capability. In *IWSEC*, pages 53–70, 2009.
- [23] Tuong Ngoc Nguyen, Willy Susilo, Dung Hoang Duong, Fuchun Guo, Kazuhide Fukushima, and Shinsaku Kiyomoto. A fault-tolerant content moderation mechanism for secure messaging systems. In *ACISP Part II*, pages 269–289, 2024.
- [24] Kazuma Ohara, Yusuke Sakai, Keita Emura, and Goichiro Hanaoka. A group signature scheme with unbounded message-dependent opening. In *ACM ASIACCS*, pages 517–522, 2013.
- [25] Yusuke Sakai, Keita Emura, Goichiro Hanaoka, Yutaka Kawai, Takahiro Matsuda, and Kazumasa Omote. Group signatures with message-dependent opening. In *Pairing-Based Cryptography*, pages 270–294, 2012.
- [26] Tao Zhang, Huangting Wu, and Sherman S. M. Chow. Structure-preserving certificateless encryption and its application. In *CT-RSA*, pages 1–22, 2019.