匿名性・追跡可能性・説明責任性を両立するデジタル署名とプライバシ保護の枠組の設計

代表研究者	穴田　啓晃	長崎県立大学　情報システム学部　教授
共同研究者	長谷川　真吾	東北大学　データ駆動科学・AI 教育研究センター　助教
共同研究者	福光　正幸	北海道情報大学　情報メディア学部　准教授

1 はじめに

1-1 研究の背景

ネットワーク上のサービスを利用するヒトやモノ（以降ユーザー）が匿名で扱われ，匿名性が保証されることは，サービスに期待される重要な性質である．これに対し，サービスを運用する者は，もし不具合が発生したときにその原因を追及するため,匿名を開封しユーザーを特定することが期待される.例えば，ソーシャルネットワークサービス（SNS）等の運営業者が法等に基づく要請を受けログを調査し容疑者を追跡する場合などである．しかし，請求が無いにも関わらず運営業者が追跡をしているのか否か，また，対象や頻度がどの程度かを SNS 利用者が知ることは難しい.つまり,追跡可能性が必須と認知される一方，匿名性の保証は不透明であり，濫用の懸念が排除出来ない．このように，匿名性と追跡可能性の両立は一見相反する性質である．このため，公平性（フェアネス）の保証を模索する課題がある．

この「匿名性と追跡可能性のフェアネスの保証」を課題とする状況に対し，サービスを運用する者が匿名を開封した事実を説明する責任を果たす場を設けることで保証を試みる方策が考えられる.この説明責任性とこれを果たす場の導入には，理論，技術，運用，ペナルティそして法といった幾つかのアプローチがありうる．本研究は，理論及び技術を含む暗号学のアプローチにより説明責任性を適切に導入し，匿名性・追跡可能性・説明責任性を両立する手法を構成しようとする動機に基づく．この研究は，理論計算機科学及び社会情報学の両方にまたがるものである．

1-2 先行研究の状況

暗号学のアプローチにおいても，これまで研究の状況は類似してきた．即ち，匿名性と追跡可能性を暗号理論・暗号技術によって両立するのは一見難しい．しかしながら近年，匿名型デジタル署名の研究領域で幾つかの試みがなされてきた．ここで，匿名型デジタル署名とは，デジタル署名を生成したユーザーを特定することが計算量的あるいは情報理論的に不可能という意味で高機能なデジタル署名の種を指す.ただし，署名したユーザーが含まれる集合までは特定されうるという種が多い．匿名型デジタル署名には，グループ署名 （[1]），リング署名（[2]），属性ベース署名（[3]）等がある．匿名性と追跡可能性の両立の試みとして次のものを挙げることが出来る.「メッセージ依存開封」(message- dependent opening, [4]等),「説明可能追跡」(accountable tracing, [5]等),「説明可能リング署名」(accountable ring signatures, [6]等)，そして「二分岐匿名署名」(bifurcated anonymous signatures, [7]等）といった先行研究である.（これらの匿名型デジタル署名の詳細についてはそれぞれの文献を参照されたい.）

1-3 本研究の貢献

上記の先行研究を踏まえた上で，本研究は「指定された追跡可能性を有するグループ署名」(group signatures with designated traceability, GSdT）を提案する．GSdT は，署名者が追跡者（開封者）を指定することが可能なグループ署名スキームである．ここで，指定とは「追跡者の属性の全体集合に対するアクセス構造を能動的に選択できること」を指す．すなわち，グループ署名を生成する者が主体的に追跡可能性の一部分を制御出来る．本研究の初めの成果は次のとおりである．

1. GSdT のアルゴリズムのシンタックスを与えた.
2. GSdT の安全性をアルゴリズムで叙述することでその定義を与えた.
3. GSdT のアルゴリズムの一般的構成を与えた.構成要素としてデジタル署名，属性ベース暗号及び非対話型ゼロ知識証明を用いた.

また，本研究では，双線形群の構造を用いた GSdT の具体的構成を例示した．なお，本稿の例は，双線形群の中でも“Type III pairing”[8]として特徴付けられたものを前提とする．その性能としては，追

公益財団法人電気通信普及財団
研究調査助成報告書　第37号　2022年度

跡者（開封者）の数 L をスキームセットアップ時に決定しなければならないものの，L 及び追跡者属性の数 N に比例する形で計算量及び署名長が決まることが分かった．

本稿の以降は，次の節から成る．第 2 節では，GSdT の一般的構成の構成要素を説明する．第 3 節では，GSdT のシンタックスと安全性定義を与える．第 4 節では，GSdT の一般的構成の方針を説明する．第 5 節では，前節の一般的構成が有する安全性を述べる．第 6 節では，双線形群の構造に基づく GSdT の具体的構成の例について構成の方針と漸近性能を述べる．第 7 節では，むすびとしてシンタックス，安全性定義，一般的構成及び具体的構成を振り返り，今後の課題に触れる．

2 準備

本節では，以降の節に必要な概念や記法をまとめる．自然数の集合を$\mathbb{N}$ と記す．$\lambda \in \mathbb{N}$ はセキュリティパラメータを表す．

2-1 デジタル署名

デジタル署名スキーム Sig は，三つのアルゴリズム(KG, Sign, Vrfy)から成る（[9]等）．

- KG(1^λ) → (pk, sk)．この確率的多項式時間アルゴリズムは，鍵を生成する．1^λ を入力に取り，公開鍵 pk 及び秘密鍵 sk を返す．
- Sign(sk, m) → s．この確率的多項式時間アルゴリズムは，署名を生成する．秘密鍵及びメッセージ m を入力に取り，署名 s を生成する．
- Vrfy(pk, m, s) → d．この確定的多項式時間アルゴリズムは，署名を検証する．公開鍵 pk，メッセージ m 及び署名 s を入力に取り，ブール値 d=0 or 1 を返す．

Sig は，正当性を満たすべきである．即ち，任意のλ，任意の m に対し，次の等式が成り立つべきである．

Pr[Vrfy(pk, m, s) → 1 | KG(1^λ) → (pk, sk); Sign(sk, m) → s] = 1.

Sig の安全性は，次の存在的偽造不可実験アルゴリズム Exp^{euf-cma}_{Sig, A}を用いて定義される．ここで，A は（攻撃）アルゴリズムを表す．

$$\begin{aligned}&\mathsf{Exp}^{\text{euf-cma}}_{\mathsf{Sig},\mathbf{A}}(1^\lambda)\\&(pk, sk) \leftarrow \mathsf{KG}(1^\lambda); (m^*, s^*) \leftarrow \mathbf{A}(pk : \mathsf{SignO}(sk, \cdot))\\&\text{If } \mathsf{Vrfy}(pk, m^*, s^*) = 1 \text{ and } m^* \text{ was not queried}\\&\text{then return 1 else return 0}\end{aligned}$$

ただし，SignO は署名オラクルである．A の Sign に対する優位度 Adv^{euf-cma}_{Sig, A}は次の式で定義される．

$$\mathbf{Adv}^{\text{euf-cma}}_{\mathsf{Sig},\mathbf{A}}(\lambda) \stackrel{\text{def}}{=} \Pr[\mathsf{Exp}^{\text{euf-cma}}_{\mathsf{Sig},\mathbf{A}}(1^\lambda) = 1].$$

任意の確率的多項式時間アルゴリズム A に対し，Adv^{euf-cma}_{Sig, A}(λ)がλの無視可能な関数であるとき，Sig は選択メッセージ攻撃に対し存在的偽造不可であると言われる．

2-2 属性ベース暗号

属性ベース暗号スキーム ABE は，四つのアルゴリズム(Setup, KG, Enc, Dec)及び関数 R^κから成る（[10]等）．

- κ．この指数は，正当な属性集合及び述語関数を指し示す．ある定数 c に対し$\mathbb{N}$ ^c に属する．
- X．この記号は，鍵属性を表す．
- Y．この記号は，暗号文属性を表す．
- R^κ：(X, Y) ↦ 0 or 1．この関数は，述語関数である．
- Setup(1^λ, κ)→(pk, msk)．この確率的多項式時間アルゴリズムは，スキーム ABE をセットアップする．1^λ及びκを入力に取り，公開鍵 pk 及びマスター秘密鍵 msk を返す．
- KG(msk, i, X)→sk^i_X．この確率的多項式時間アルゴリズムは，個別秘密鍵を生成する．msk，アイデンティティ指数 i，鍵属性 X を入力に取り，個別秘密鍵 sk^i_X を返す．
- Enc(pk, Y, M)→C．この確率的多項式時間アルゴリズムは，暗号文を生成する．pk，暗号文属性 Y，メッセージ M を入力に取り，暗号文 C を返す．

公益財団法人電気通信普及財団
研究調査助成報告書 第37号 2022年度

- Dec(pk, skˆi_X, C)→ M'. この確定的多項式時間アルゴリズムは，暗号文を復号する．pk，skˆi_X，C を入力に取り，復号メッセージ M'を出力する．

ABE は，正当性を満たすべきである．即ち，任意のλ，任意のκ，任意の i，任意の X，任意の Y，任意の M に対し，次の等式が成り立つべきである．

Pr[Dec(pk, skˆi_X, C) = M | Setup(1ˆλ, κ) → (pk, msk); KG(msk, i, X) → (skˆi_X); Enc(pk, Y, M)→C] = 1.

ABE の安全性は,次の適応的選択平文攻撃に対する識別不可能性実験アルゴリズム Expˆ{ind-cpa-b}_{ABE, A}を用いて定義される．ここで，A は（攻撃）アルゴリズムを表す．

$$\begin{aligned}&\mathsf{Exp}^{\text{ind-cpa-}b}_{\mathsf{ABE},\mathbf{A}}(1^\lambda,\kappa)\\&(pk,msk)\leftarrow\mathsf{Setup}(1^\lambda,\kappa)\\&d\leftarrow\mathbf{A}(pk:\mathsf{KGO}(msk,\cdot,\cdot),\mathsf{LRO}_b(pk,\cdot,\cdot,\cdot))\\&\text{Return } d\end{aligned}$$

ただし，KGO, LRO_b はそれぞれ個別秘密鍵生成オラクル，b-チャレンジ暗号文生成オラクルである．A の ABE に対する優位度 Advˆ{ind-cpa}_{ABE, A}は次の式で定義される．

$$\mathbf{Adv}^{\text{ind-cpa}}_{\mathsf{ABE},\mathbf{A}}(\lambda)\stackrel{\text{def}}{=}|\Pr[\mathsf{Exp}^{\text{ind-cpa-1}}_{\mathsf{ABE},\mathbf{A}}(1^\lambda,\kappa)=1]-\Pr[\mathsf{Exp}^{\text{ind-cpa-0}}_{\mathsf{ABE},\mathbf{A}}(1^\lambda,\kappa)=1]|.$$

任意の確率的多項式時間アルゴリズム A に対し，Advˆ{ind-cpa}_{ABE, A}(λ)が λ の無視可能な関数であるとき，ABE は適応的選択平文攻撃に対し識別不可能であると言われる．

2-3 シミュレーション健全非対話ゼロ知識証明系

シミュレーション健全非対話ゼロ知識証明系Πは，二つのアルゴリズム(P, V)から成る（[11]等）．本稿では，V のみならず P もまた多項式時間アルゴリズムであるとする．また，P は確率的，V は確定的であるとする．P と V は共通参照文字列 R にアクセスするものとする．二つの多項式ℓ，p が存在して次の二性質が成り立つものとする．

- 完全性.

$$\begin{aligned}&\forall\lambda\in\mathbb{N}\ \forall(x,w)\in\rho\text{ s.t. }|x|\le\ell(\lambda)\text{ and }x\in\mathrm{Dom}\\&\Pr[R\leftarrow_R\{0,1\}^{p(\lambda)};\pi\leftarrow\mathsf{P}(1^\lambda,x,w,R):\mathsf{V}(1^\lambda,x,\pi,R)=1]\\&\quad=1.\end{aligned}$$

- 健全性.

$$\begin{aligned}&\forall\lambda\in\mathbb{N}\ \forall\hat{\mathsf{P}}:\text{PPT}\ \forall x\in\mathrm{Dom}\text{ s.t. }x\notin L_\rho\\&\Pr[R\leftarrow\{0,1\}^{p(\lambda)};\pi\leftarrow\hat{\mathsf{P}}(1^\lambda,x,R):\mathsf{V}(1^\lambda,x,\pi,R)=1]\\&\quad<2^{-\lambda}.\end{aligned}$$

更に，第三の性質を要請する．

- ゼロ知識性．Πに対しシミュレータと呼ばれる確率的多項式時間アルゴリズム Sim が存在する．次の実験アルゴリズム Expˆ{zk-b}_{P, Sim, D}を考える．ここで，D は（識別）アルゴリズムを表す．

$$\begin{aligned}&\mathsf{Exp}^{\text{zk-0}}_{\mathsf{P},\mathsf{Sim},\mathbf{D}}(1^\lambda)\\&\quad(R,St)\leftarrow\mathsf{Sim}(\mathtt{gen},1^\lambda);\ d\leftarrow\mathbf{D}(R:\mathsf{P}_1(\cdot,\cdot));\ \text{return } d\\&\mathsf{P}_1(x,w):\pi\leftarrow\mathsf{Sim}(\mathtt{prv},St,x);\ \text{return }\pi\\&\mathsf{Exp}^{\text{zk-1}}_{\mathsf{P},\mathsf{Sim},\mathbf{D}}(1^\lambda)\\&\quad R\leftarrow\{0,1\}^{p(\lambda)};\ d\leftarrow\mathbf{D}(R:\mathsf{P}_2(\cdot,\cdot));\ \text{return } d\\&\mathsf{P}_2(x,w):\pi\leftarrow\mathsf{P}(1^\lambda,x,w,R);\ \text{return }\pi\end{aligned}$$

D のΠに対する優位度 Advˆ{zk}_{P, Sim, D}は次の式で定義される．

$$\mathbf{Adv}^{\text{zk}}_{\mathsf{P},\mathsf{Sim},\mathbf{D}}(\lambda)\stackrel{\text{def}}{=}|\Pr[\mathsf{Exp}^{\text{zk-0}}_{\mathsf{P},\mathsf{Sim},\mathbf{D}}(1^\lambda)=1]-\Pr[\mathsf{Exp}^{\text{zk-1}}_{\mathsf{P},\mathsf{Sim},\mathbf{D}}(1^\lambda)=1]|.$$

任意の確率的多項式時間アルゴリズム D に対し，Adv^{zk}_{P, Sim, D}(λ)が λ の無視可能な関数であるとき，Π は計算量的ゼロ知識性を有すると言われる．

加えて，本稿では次の性質を要請する．

- シミュレーション健全性

$$\begin{aligned}&\mathsf{Exp}^{\mathrm{ss}}_{\Pi,\mathbf{A}}(1^\lambda)\\&(R, St) \leftarrow \mathsf{Sim}(\mathtt{gen}, 1^\lambda);\ (x, \pi) \leftarrow \mathbf{A}(R : \mathsf{Sim}(\mathtt{prv}, St, \cdot))\\&\text{If } x \notin L_\rho \wedge \pi \text{ was not given to } \mathbf{A} \wedge \mathsf{V}(1^\lambda, x, \pi, R) = 1\\&\quad \text{then return 1 else return 0}\end{aligned}$$

A の Π に対する優位度 Adv^{ss}_{Π, A} は次の式で定義される．

$$\mathbf{Adv}^{\mathrm{ss}}_{\Pi,\mathbf{A}}(\lambda) \stackrel{\mathrm{def}}{=} \Pr[\mathsf{Exp}^{\mathrm{ss}}_{\Pi,\mathbf{A}}(1^\lambda) = 1].$$

任意の確率的多項式時間アルゴリズム A に対し，Adv^{ss}_{Π, A}(λ)が λ の無視可能な関数であるとき，Π はシミュレーション健全であると言われる．より正確には，ワンタイムシミュレーション健全であると言われる．

3 シンタックスと安全性定義

本節では，「指定された追跡可能性を有するグループ署名」のスキーム GSdT のシンタックス及び安全性定義を与える．以下で，第 2 節で準備した記法を用いる．

3-1 シンタックス

スキーム GSdT は九つのアルゴリズム(GKG, OKG, UKG, Join, Iss, GSign, GVrfy, Open, Judge)から成る．

- GKG(1^λ, κ)→(gpk, ik, omk)．この確率的多項式時間アルゴリズムは，グループ鍵を生成する．1^λ 及び κ を入力に取り，グループ公開鍵 gpk，発行鍵 ik 及び開封マスター鍵 omk を返す．
- OKG(gpk, omk, j, X)→ ok[j]．この確率的多項式時間アルゴリズムは，開封鍵を生成する．gpk, omk, 開封者指数 j 及び開封者属性 X を入力に取り，開封鍵 ok[j]を返す．ok[j]は X のデータを含むとする．
- UKG(1^λ)→ (upk, usk)．この確率的多項式時間アルゴリズムは，ユーザー鍵を生成する．1^λ を入力に取り，ユーザー公開鍵 upk 及びユーザー秘密鍵 usk を返す．
- Join, Iss．これらの対話型確率的多項式時間アルゴリズムは，図 1の通りシンタックスが定義される．また，図 1の通りグループメンバー個別秘密鍵 gsk[i]及び参加登録テーブル reg が生成される．
- GSign(gpk, gsk[i], Y, m)→(Y, σ_0)．この確率的多項式時間アルゴリズムは，グループ署名を生成する．gpk, gsk[i]，アクセス構造 Y 及びメッセージ m を入力に取り，グループ署名(Y, σ_0)を返す．
- GVrfy(gpk, m, (Y, σ_0))→ d．この確定的多項式時間アルゴリズムは，グループ署名を検証する．gpk, m 及び(Y, σ_0)を入力に取り，ブール値 d=0 or 1 を返す．
- Open(gpk, ok[j], reg, m, (Y, σ_0))→(i, τ)．この確率的多項式時間アルゴリズムは，グループ署名を開封する．gpk, ok[j], reg, m 及び(Y, σ_0)を入力に取り，ユーザーアイデンティティ指数 i 及び証明 τ を返す．
- Judge(gpk, i, upk[i], m, (Y, σ_0), τ)→ d．この確定的多項式時間アルゴリズムは，グループ署名を検証する．gpk, i，ユーザー公開鍵 upk[i], m, (Y, σ_0) 及び τ を入力に取り，ブール値 d=0 or 1 を返す．

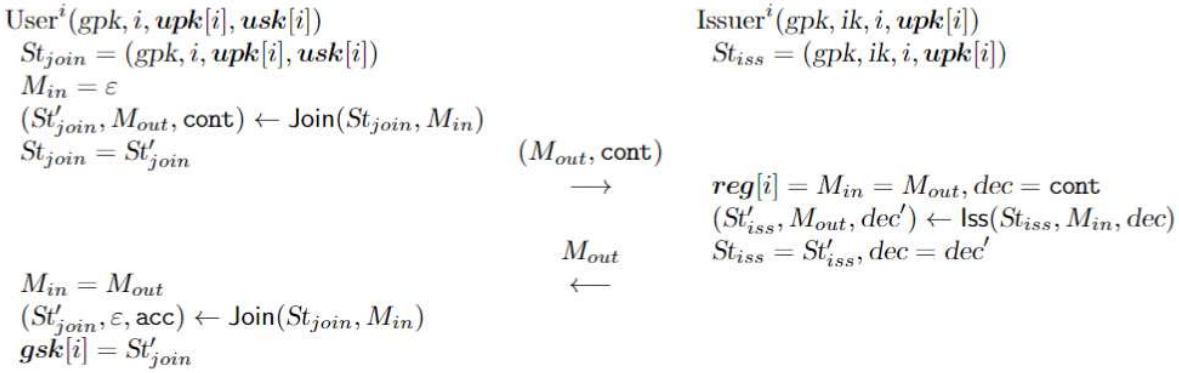

図 1　Join と Iss のシンタックス

3-2 安全性定義

スキーム GSdT に対し，四つの安全性を定義する．はじめにオラクルを図 2及び図 3の通り導入する．ここで，AddOO は開封者追加オラクルである．AddUO はユーザー追加オラクルである．CrptOO は開封者堕落オラクルである．CrptUO はユーザー堕落オラクルである．StoUO はユーザーへの送信オラクルである．StoUI は発行者への送信オラクルである．USKO はユーザー鍵生成オラクルである．GSignO はグループ署名生成オラクルである．OpenO は開封オラクルである．RRegO は参加者登録テーブル読み出しオラクルである．WRegO は参加者登録テーブル書き込みオラクルである．ChaO_b は b-チャレンジオラクルである．HU は正直なユーザーの集合である．CU は堕落したユーザーの集合である．OP は開封者の集合である．MS はクエリされたメッセージと返答されたグループ署名の対の集合である．CO は堕落した開封者の集合である．参考文献[12]と比較すると，AddOO 及び CruptOO が新しく導入されている．

留意点として，本稿では，OpenO へのクエリは，(j,m,(Y, σ_0))の形，ただし R(X,Y)=1 なる X で開封者 j に対し発行された ok[j]が存在するもの，のみとしている．この制約は，通常のグループ署名の開封オラクルとは異なる，GSdT に固有のものと考えている．そして，この制約により，第 4 節の一般的構成で部品となる ABE には適応的選択平文攻撃に対する識別不可能性（adaptive IND-CPA 安全性）で十分となる（adaptive IND-CCA 安全性でなく）．

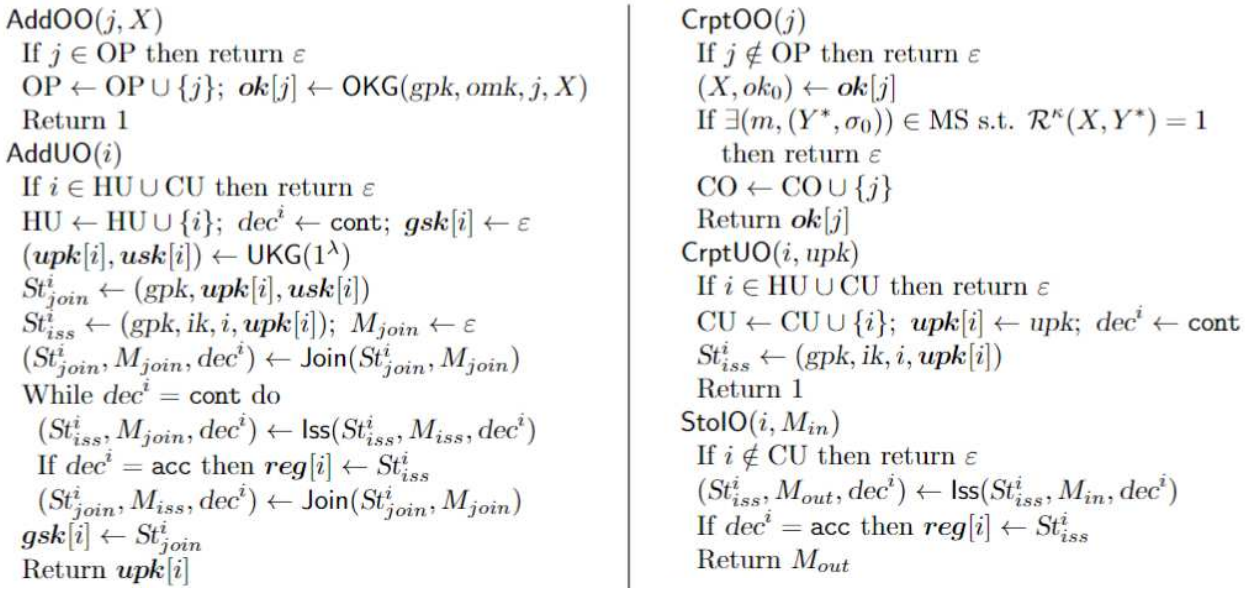

図 2　オラクルの定義

$\mathsf{StoUO}(i, M_{in})$
If $i \notin \mathrm{HU}$ then
$\mathrm{HU} \leftarrow \mathrm{HU} \cup \{i\}$; $(\boldsymbol{upk}[i], \boldsymbol{usk}[i]) \leftarrow \mathsf{UKG}(1^\lambda)$
$\boldsymbol{gsk}[i] \leftarrow \varepsilon$; $M_{in} \leftarrow \varepsilon$;
$St^i_{join} \leftarrow (gpk, \boldsymbol{upk}[i], \boldsymbol{usk}[i])$
$(St^i_{join}, M_{out}, dec) \leftarrow \mathsf{Join}(St^i_{join}, M_{in})$
If $dec = \mathsf{acc}$ then $\boldsymbol{gsk}[i] \leftarrow St^i_{join}$
Return (M_{out}, dec)
$\mathsf{USKO}(i)$ Return $(\boldsymbol{gsk}[i], \boldsymbol{usk}[i])$
$\mathsf{GSignO}(i, Y^*, m)$
If $i \notin \mathrm{HU}$ then return $\perp$
If $\boldsymbol{gsk}[i] = \varepsilon$ then return $\perp$
Else return $\mathsf{GSign}(gpk, \boldsymbol{gsk}[i], Y^*, m)$

$\mathsf{OpenO}(j, m, (Y, \sigma_0))$
If $(m, (Y, \sigma_0)) \in \mathrm{MS}$ then return $\perp$
Return $\mathsf{Open}(gpk, \boldsymbol{ok}[j], \boldsymbol{reg}, m, (Y, \sigma_0))$
$\mathsf{RRegO}(i)$ Return $\boldsymbol{reg}[i]$
$\mathsf{WRegO}(i, \rho)$ $\boldsymbol{reg}[i] \leftarrow \rho$; Return 1
$\mathsf{ChaO}_b(i_0, i_1, m, Y^*)$
If $i_0 \notin \mathrm{HU}$ or $i_1 \notin \mathrm{HU}$ then return $\perp$
If $\boldsymbol{gsk}[i_0] = \varepsilon$ or $\boldsymbol{gsk}[i_1] = \varepsilon$ then return $\perp$
If $\exists j \in \mathrm{CO}$ s.t.
$\mathcal{R}^\kappa(X, Y^*) = 1$ for $(X, ok_0) \leftarrow \boldsymbol{ok}[j]$
then return $\perp$
$\sigma = (Y^*, \sigma_0) \leftarrow \mathsf{GSign}(gpk, \boldsymbol{gsk}[i_b], Y^*, m)$
$MS \leftarrow \mathrm{MS} \cup \{(m, (Y^*, \sigma_0))\}$
Return σ

図 3　オラクルの定義（続き）

- 正当性．GSdT の正当性は，次の実験アルゴリズム Exp^{corr}_{GSdT, A}を用いて定義される．ここで，A は（攻撃）アルゴリズムである．

$\mathsf{Exp}^{\mathrm{corr}}_{\mathsf{GSdT},\mathbf{A}}(1^\lambda, \kappa)$
$(gpk, ik, omk) \leftarrow \mathsf{GKG}(1^\lambda, \kappa)$, $\mathrm{CU} \leftarrow \emptyset, \mathrm{HU} \leftarrow \emptyset, \mathrm{OP} \leftarrow \emptyset$
$(i, m, Y) \leftarrow \mathbf{A}(gpk : \mathsf{AddOO}(\cdot,\cdot), \mathsf{AddUO}(\cdot), \mathsf{RRegO}(\cdot))$
If $i \notin \mathrm{HU}$ then return 0; If $\boldsymbol{gsk}[i] = \varepsilon$ then return 0
$\sigma \leftarrow \mathsf{GSign}(gpk, \boldsymbol{gsk}[i], Y, m)$
If $\mathsf{GVrfy}(gpk, m, \sigma) = 0$ return 1
$\mathrm{OS}_Y \leftarrow \{j \in \mathrm{OP} \mid \mathcal{R}^\kappa(X, Y) = 1 \text{ for } (X, ok_0) \leftarrow \boldsymbol{ok}[j]\}$
For $j \in \mathrm{OS}_Y$ do
$(i', \tau) \leftarrow \mathsf{Open}(gpk, \boldsymbol{ok}[j], \boldsymbol{reg}, m, \sigma)$
If $i \neq i'$ or $\mathsf{Judge}(gpk, i, \boldsymbol{upk}[i], m, \sigma, \tau) = 0$ then return 1
Return 0

A の GSdT に対する優位度 Adv^{corr}_{GSdT, A}は次の式で定義される．

$$\mathbf{Adv}^{\mathrm{corr}}_{\mathsf{GSdT},\mathbf{A}}(\lambda) \stackrel{\mathrm{def}}{=} \Pr[\mathsf{Exp}^{\mathrm{corr}}_{\mathsf{GSdT},\mathbf{A}}(1^\lambda, \kappa) = 1].$$

任意の確率的多項式時間アルゴリズム A に対し，Adv^{corr}_{GSdT, A}(λ)が λ の無視可能な関数であるとき，GSdT は正当性を有すると言われる．

- 匿名性．GSdT の匿名性は，次の実験アルゴリズム Exp^{anon-b}_{GSdT, A}を用いて定義される．ここで，A は（攻撃）アルゴリズムである．

$\mathsf{Exp}^{\text{anon-}b}_{\mathsf{GSdT},\mathbf{A}}(1^\lambda, \kappa)$ // $b \in \{0, 1\}$
$(gpk, ik, omk) \leftarrow \mathsf{GKG}(1^\lambda, \kappa)$
$\mathrm{CU} \leftarrow \emptyset, \mathrm{HU} \leftarrow \emptyset, \mathrm{MS} \leftarrow \emptyset, \mathrm{CO} \leftarrow \emptyset, \mathrm{OP} \leftarrow \emptyset$
$d \leftarrow \mathbf{A}(gpk, ik : \mathsf{ChaO}_b(\cdot,\cdot,\cdot,\cdot), \mathsf{AddOO}(\cdot,\cdot), \mathsf{OpenO}(\cdot,\cdot,\cdot), \mathsf{StoUO}(\cdot,\cdot), \mathsf{WRegO}(\cdot,\cdot),$
$\mathsf{USKO}(\cdot), \mathsf{CrptOO}(\cdot), \mathsf{CrptUO}(\cdot,\cdot))$
Return d

A の GSdT に対する優位度 Adv^{anon}_{GSdT, A}は次の式で定義される．

$$\mathbf{Adv}^{\mathrm{anon}}_{\mathsf{GSdT},\mathbf{A}}(\lambda) \stackrel{\mathrm{def}}{=} |\Pr[\mathsf{Exp}^{\text{anon-0}}_{\mathsf{GSdT},\mathbf{A}}(1^\lambda, \kappa) = 1] - \Pr[\mathsf{Exp}^{\text{anon-1}}_{\mathsf{GSdT},\mathbf{A}}(1^\lambda, \kappa) = 1]|.$$

任意の確率的多項式時間アルゴリズム A に対し，Adv^{anon}_{GSdT, A}(λ)が λ の無視可能な関数であるとき，GSdT は匿名性を有すると言われる．

- 追跡可能性．GSdT の追跡可能性は，次の実験アルゴリズム Exp^{trace}_{GSdT, A}を用いて定義される．ここで，A は（攻撃）アルゴリズムである．

$$
\begin{aligned}
&\mathsf{Exp}^{\mathrm{trace}}_{\mathsf{GSdT},\mathbf{A}}(1^\lambda,\kappa)\\
&(gpk, ik, omk) \leftarrow \mathsf{GKG}(1^\lambda,\kappa),\ \mathrm{CU} \leftarrow \emptyset, \mathrm{HU} \leftarrow \emptyset, \mathrm{OP} \leftarrow \emptyset\\
&(m,(Y,\sigma_0)) \leftarrow \mathbf{A}(gpk, omk : \mathsf{StoIO}(\cdot,\cdot), \mathsf{AddUO}(\cdot), \mathsf{RRegO}(\cdot), \mathsf{USKO}(\cdot), \mathsf{CrptUO}(\cdot,\cdot))\\
&\text{If } \mathsf{GVrfy}(gpk, m, (Y,\sigma_0)) = 0 \text{ then return } 0\\
&\text{Find } X \text{ s.t. } \mathcal{R}^\kappa(X,Y) = 1;\ ok \leftarrow \mathsf{OKG}(gpk, omk, 0, X)\\
&(i,\tau) \leftarrow \mathsf{Open}(gpk, ok, \boldsymbol{reg}, m, (Y,\sigma_0))\\
&\text{If } i = 0 \text{ or } \mathsf{Judge}(gpk, i, \boldsymbol{upk}[i], m, (Y,\sigma_0), \tau) = 0 \text{ then return } 1 \text{ else return } 0
\end{aligned}
$$

A の GSdT に対する優位度 Adv^{trace}_{GSdT, A}は次の式で定義される．

$$\mathbf{Adv}^{\mathrm{trace}}_{\mathsf{GSdT},\mathbf{A}}(\lambda) \stackrel{\mathrm{def}}{=} \Pr[\mathsf{Exp}^{\mathrm{trace}}_{\mathsf{GSdT},\mathbf{A}}(1^\lambda,\kappa) = 1].$$

任意の確率的多項式時間アルゴリズム A に対し，Adv^{trace}_{GSdT, A}(λ)が λ の無視可能な関数であるとき，GSdT は追跡可能性を有すると言われる．

- 陥罪不可能性．GSdT の陥罪不可能性は，次の実験アルゴリズム Exp^{nf}_{GSdT, A}を用いて定義される．ここで，A は（攻撃）アルゴリズムである．

$$
\begin{aligned}
&\mathsf{Exp}^{\mathrm{nf}}_{\mathsf{GSdT},\mathbf{A}}(1^\lambda,\kappa)\\
&(gpk, ik, omk) \leftarrow \mathsf{GKG}(1^\lambda,\kappa),\ \mathrm{CU} \leftarrow \emptyset, \mathrm{HU} \leftarrow \emptyset, \mathrm{OP} \leftarrow \emptyset\\
&(m,(Y,\sigma_0),i,\tau) \leftarrow \mathbf{A}(gpk, ik, omk : \mathsf{StoUO}(\cdot,\cdot), \mathsf{WRegO}(\cdot,\cdot), \mathsf{GSignO}(\cdot,\cdot,\cdot,\cdot),\\
&\qquad\qquad \mathsf{USKO}(\cdot), \mathsf{CrptUO}(\cdot,\cdot))\\
&\text{If the following are all true then return } 1 \text{ else return } 0:\\
&\quad - i \in \mathrm{HU} \wedge \boldsymbol{gsk}[i] \neq \varepsilon\\
&\quad - \mathsf{Judge}(gpk, i, \boldsymbol{upk}[i], m, (Y,\sigma_0), \tau) = 1\\
&\quad - A \text{ did not query } \mathsf{USKO}(i) \vee \mathsf{GSignO}(i, m)
\end{aligned}
$$

A の GSdT に対する優位度 Adv^{nf}_{GSdT, A}は次の式で定義される．

$$\mathbf{Adv}^{\mathrm{nf}}_{\mathsf{GSdT},\mathbf{A}}(\lambda) \stackrel{\mathrm{def}}{=} \Pr[\mathsf{Exp}^{\mathrm{nf}}_{\mathsf{GSdT},\mathbf{A}}(1^\lambda,\kappa) = 1].$$

任意の確率的多項式時間アルゴリズム A に対し，Adv^{nf}_{GSdT, A}(λ)が λ の無視可能な関数であるとき，GSdT は陥罪不可能性を有すると言われる．

4 一般的構成

本節では，第 3 節で定義したスキーム GSdT のシンタックスに従い，GSdT の一般的構成について，構成の方針及び構成における留意点を説明する．なお，詳細は文献[13][14]を参照されたい．

4-1 構成の方針

一般的構成は，先行研究[12]に基づく．なお，[12]は“partially dynamic group signature scheme”のシンタックスと一般的構成を与えた研究として知られている．[12]の一般的構成の方針は，“sign, then encrypt, then prove”と簡約することが出来る．即ち，グループメンバーがメッセージに対しデジタル署名を生成する（グループ署名ではない）．次いで，この(i)署名，(ii)アイデンティティ指数，(iii)グループメンバー公開鍵，(iv)(ii)と(iii)に対する証明書の 4 点を公開鍵暗号で暗号化する．そして，暗号化時の乱数を用い，証明書が正しいこと及び 4 点が正しく暗号化されていることを非対話型ゼロ知識証明する．以下の一般的構成は，[12]の一般的構成に対し公開鍵暗号を属性ベース暗号で置き換える方針である．

本稿の一般的構成を図 4及び図 5で与える．グループメンバーがグループ署名を生成する際，アルゴリズム GSign において ABE 暗号化アルゴリズム Enc を用いる．ここで，開封者属性の集合の上のアクセス構造 Y を入力に取り，Y が暗号文属性として扱われる．この点が，グループ署名を生成する者が主体的に追跡可能性の一部分を制御出来る機能としている点である．従って，開封アルゴリズム Open は，開封者属性 X を，開封鍵 ok[j]という形で入力に取っている．その開封鍵 ok[j]は，開封鍵生成アルゴリズム OKG で生成される．

$\mathsf{GKG}(1^\lambda, \kappa)$
$R_1 \leftarrow \{0,1\}^{p_1(\lambda)};\ R_2 \leftarrow \{0,1\}^{p_2(\lambda)}$
$(pk_\mathsf{a}, msk_\mathsf{a}) \leftarrow \mathsf{Setup}_\mathsf{a}(1^\lambda, \kappa);\ (pk_\mathsf{s}, sk_\mathsf{s}) \leftarrow \mathsf{KG}_\mathsf{s}(1^\lambda)$
$gpk = (1^\lambda, R_1, R_2, pk_\mathsf{a}, pk_\mathsf{s});\ omk = msk_\mathsf{a};\ ik = sk_\mathsf{s}$
Return (gpk, ik, omk)
$\mathsf{OKG}(gpk, omk, j, X)$
Parse omk as $msk_\mathsf{a};\ r_{\mathsf{a},j} \leftarrow \{0,1\}^{r(\lambda)}$
$sk_X^j \leftarrow \mathsf{KG}_\mathsf{a}(msk_\mathsf{a}, j, X; r_{\mathsf{a},j});\ \boldsymbol{ok}[j] \leftarrow (sk_X^j, r_{\mathsf{a},j})$
Return $\boldsymbol{ok}[j]$
$\mathsf{UKG}(1^\lambda)$ $(upk, usk) \leftarrow \mathsf{KG}_\mathsf{s}(1^\lambda)$; Return (upk, usk)
$\mathsf{GSign}(gpk, \boldsymbol{gsk}[i], Y, m)$
Parse gpk as $(1^\lambda, R_1, R_2, pk_\mathsf{a}, pk_\mathsf{s})$
Parse $\boldsymbol{gsk}[i]$ as $(i, pk_i, sk_i, cert_i)$
$s \leftarrow \mathsf{Sign}(sk_i, m);\ r \leftarrow_R \{0,1\}^\lambda$
$C = (Y, C_0) \leftarrow \mathsf{Enc}(pk_\mathsf{a}, Y, \langle i, pk_i, cert_i, s\rangle; r)$
$\pi_1 \leftarrow \mathsf{P}_1(1^\lambda, (pk_\mathsf{a}, pk_\mathsf{s}, m, C), (i, pk_i, cert_i, s, r), R_1)$
Return $\sigma = (C, \pi_1)$
$\mathsf{GVrfy}(gpk, (m, \sigma))$
Parse gpk as $(1^\lambda, R_1, R_2, pk_\mathsf{a}, pk_\mathsf{s})$;
Parse σ as (C, π_1)
Return $\mathsf{V}_1(1^\lambda, (pk_\mathsf{a}, pk_\mathsf{s}, m, C), \pi_1, R_1)$

$\mathsf{Open}(gpk, \boldsymbol{ok}[j], \boldsymbol{reg}, m, \sigma)$
Parse gpk as $(1^\lambda, R_1, R_2, pk_\mathsf{a}, pk_\mathsf{s})$
Parse $\boldsymbol{ok}[j]$ as $(sk_X^j, r_{\mathsf{a},j})$; Parse σ as (C, π_1)
$M \leftarrow \mathsf{Dec}(pk_\mathsf{a}, sk_X^j, C)$; Parse M as $\langle i, pk, cert, s\rangle$
If $\boldsymbol{reg}[i] \neq \varepsilon$ then parse $\boldsymbol{reg}[i]$ as (pk_i, sig_i)
Else $pk_i \leftarrow \varepsilon, sig_i \leftarrow \varepsilon$
$\pi_2 \leftarrow \mathsf{P}_2(1^\lambda, (pk_\mathsf{a}, C, i, pk, cert, s), (sk_X^j, r_{\mathsf{a},j}), R_2)$
If $\mathsf{V}_1(1^\lambda, (pk_\mathsf{a}, pk_\mathsf{s}, m, C), \pi_1, R_1) = 0$
then return $(0, \varepsilon)$
If $pk \neq pk_i$ or $\boldsymbol{reg}[i] = \varepsilon$ then return $(0, \varepsilon)$
$\tau = (pk_i, sig_i, i, pk, cert, s, \pi_2)$
Return (i, τ)
$\mathsf{Judge}(gpk, i, \boldsymbol{upk}[i], m, \sigma, \tau)$
Parse gpk as $(1^\lambda, R_1, R_2, pk_\mathsf{a}, pk_\mathsf{s})$;
Parse σ as (C, π_1)
If $(i, \tau) = (0, \varepsilon)$ then
Return $\mathsf{V}_1(1^\lambda, (pk_\mathsf{a}, pk_\mathsf{s}, m, C), \pi_1, R_1)$
Parse τ as $(\overline{pk}, \overline{sig}, i', pk, cert, s, \pi_2)$
If $\mathsf{V}_2(1^\lambda, (pk_\mathsf{a}, C, i', pk, cert, s), \pi_2, R_2) = 0$
then Return 0
If the following are true then return 1
else return 0:
$i = i' \ \wedge\ \mathsf{Vrfy}(\boldsymbol{upk}[i], \overline{pk}, \overline{sig}) = 1 \ \wedge\ \overline{pk} = pk$

図 4　一般的構成

$\mathsf{Join}(St_{join}, M_{in})$
If $M_{in} = \varepsilon$ then
Parse St_{join} as (gpk, i, upk_i, usk_i)
$(pk_i, sk_i) \leftarrow \mathsf{KG}_\mathsf{s}(1^\lambda);\ sig_i \leftarrow \mathsf{Sign}(usk_i, pk_i)$
$St'_{join} = (i, pk_i, sk_i);\ M_{out} = (pk_i, sig_i)$
Return $(St'_{join}, M_{out}, \mathsf{cont})$
Else
Parse St_{join} as (i, pk_i, sk_i); Parse M_{in} as $cert_i$
$St'_{join} = (i, pk_i, sk_i, cert_i)$
Return $(St'_{join}, \varepsilon, \mathsf{acc})$

$\mathsf{Iss}(St_{iss}, M_{in}, dec)$
$M_{out} = \varepsilon;\ dec' = \mathsf{rej}$
If $dec = \mathsf{cont}$ then
Parse St_{iss} as (gpk, ik, i, upk_i)
Parse M_{in} as (pk_i, sig_i)
Parse ik as sk_s
If $\mathsf{Vrfy}(upk_i, pk_i, sig_i) = 1$ then
$cert_i \leftarrow \mathsf{Sign}(sk_\mathsf{s}, \langle i, pk_i\rangle)$
$St'_{iss} = (pk_i, sig_i)$
$M_{out} = cert_i;\ dec' = \mathsf{acc}$
Return $(St'_{iss}, M_{out}, dec')$

図 5　一般的構成（Join, Iss）

4-2 構成における留意点

提案した一般的構成は，属性ベース暗号スキーム ABE を用いた．ただし，構成要素である ABE に対し，暗号文ポリシーであること及び平文のみの秘匿（ペイロード秘匿，payload-hiding）であることを前提としている．ここで，後者は，暗号文においてアクセス構造が陽に見えることを意図している．

5 安全性

本節では，第 3 節で定義したスキーム GSdT の安全性に対し，第 4 節の一般的構成の GSdT が満足する安全性の定理及び留意点を述べる．なお，安全性の証明については文献[14]を参照されたい．

5-1 正当性

定理．Sig が正当性を有し，ABE が正当性を有し，Π_1 が完全性を有し，Π_2 が完全性を有するとする．このとき，GSdT は正当性を有する．より詳しくは，計算能力に制約のない任意のアルゴリズム A に対し，次の式が成り立つ．

$$\mathbf{Adv}^{corr}_{GSdT,\mathbf{A}}(\lambda) = 0.$$

5-2 匿名性

定理．ABE が適応的選択平文攻撃に対する識別不可能性を有し，Π_1 がシミュレーション健全性及び計算量的ゼロ知識性を有し，Π_2 が計算量的ゼロ知識性を有するとする．このとき，GSdT は匿名性を有する．より詳しくは，任意の確率的多項式時間アルゴリズム A に対し，確率的多項式時間アルゴリズム A_0，A_1，A_s，D_1 及び D_2 が存在し，次の式が成り立つ．

$$\begin{aligned}\mathbf{Adv}^{anon}_{GSdT,\mathbf{A}}(\lambda) \leq & \mathbf{Adv}^{ind\text{-}cpa}_{ABE,\mathbf{A}_0}(\lambda) + \mathbf{Adv}^{ind\text{-}cpa}_{ABE,\mathbf{A}_1}(\lambda) \\ & + \mathbf{Adv}^{ss}_{\Pi_1,\mathbf{A}_s}(\lambda) + 2 \cdot (\mathbf{Adv}^{zk}_{P_1,Sim_1,\mathbf{D}_1}(\lambda) + \mathbf{Adv}^{zk}_{P_2,Sim_2,\mathbf{D}_2}(\lambda)).\end{aligned}$$

留意点．本稿では，OpenO へのクエリは，(j,m,(Y,σ_0))の形，ただし R(X,Y)=1 なる X で開封者 j に対し発行された ok[j]が存在するもののみとしている（第 3-2 節）．この制約により， ABE には適応的選択平文攻撃に対する識別不可能性（adaptive IND-CPA 安全性）で十分となる．

5-3 追跡可能性

定理．Sig が選択メッセージ攻撃に対する存在的偽造不可能性を有し，Π_1 が健全性を有し，Π_2 が健全性を有するとする．このとき，GSdT は追跡可能性を有する．より詳しくは，任意の確率的多項式時間アルゴリズム A に対し，確率的多項式時間アルゴリズム F が存在し，次の式が成り立つ．

$$\mathbf{Adv}^{trace}_{GSdT,\mathbf{A}}(\lambda) \leq 2^{-\lambda} + \mathbf{Adv}^{euf\text{-}cma}_{Sig,\mathbf{F}}(\lambda).$$

5-4 陥罪不可能性

定理．Sig が選択メッセージ攻撃に対する存在的偽造不可能性を有し，Π_1 が健全性を有し，Π_2 が健全性を有するとする．このとき，GSdT は陥罪不可能性を有する．より詳しくは，任意の確率的多項式時間アルゴリズム A，ただし A は高々N(λ)の正直なユーザーを生成する，に対し，確率的多項式時間アルゴリズム F_1 及び F_2 が存在し，次の式が成り立つ．

$$\mathbf{Adv}^{nf}_{GSdT,\mathbf{A}}(\lambda) \leq 2^{-\lambda+1} + N(\lambda) \cdot (\mathbf{Adv}^{euf\text{-}cma}_{Sig,\mathbf{F}_1}(\lambda) + \mathbf{Adv}^{euf\text{-}cma}_{Sig,\mathbf{F}_2}(\lambda)).$$

6 双線形群における例示：構成の方針と漸近性能

6-1 構成の方針

本節では，スキーム GSdT の第 4 節の一般的構成に従い，双線形群の代数構造を用いた具体的構成の例について，構成の方針と漸近性能を説明する．なお，詳細は文献[15]を参照されたい．

スキーム GSdT の第 3 節の一般的構成における構成要素は，選択平文攻撃に対し存在的偽造不可な署名スキーム Sig，適応的選択平文攻撃に対し識別不可能でペイロード秘匿な暗号文ポリシー属性ベース暗号スキーム ABE，そして非対話ゼロ知識証明系Π_1，Π_2 である．ただし，Π_1，Π_2 は 2 種類を使い分けてもよく，完全性，健全性，計算量的ゼロ知識性を満たすべきことに加え，Π_1 はシミュレーション健全性，より正確にはワンタイムシミュレーション健全性を満たすことが要求される（第 2.3 節）．

構成要素を踏まえ，具体例を構成する際に留意すべき点は，双線形群における ABE の先行研究はそのほとんどが双線形群のターゲット群において``blinding factor''を乗じることで平文を暗号化する設計であるという制約がある点である．この制約を満たそうとすると，Sig はターゲット群において署名を生成することとなり，このためソース群において署名を生成する``structure-preserving signatures (SPS)''等とは相

容れない．そこで，一例として，ABE として pairing-free なもの[16]を用いる方針を取る．即ち，Sig として SPS を用いることを優先し，ソース群（という単独の群）において属性ベース暗号化する．ただし，[16]の ABE には，ユーザ数の上限が ABE のセットアップ時に固定されなければならないという別の制約がある．この制約は，開封者の数の上限を GSdT のセットアップ時に固定することに相当する．

以上の理由から，一例の構成要素として次の三つを用いることが出来る．Sig は，``compact structure-preserving signatures with almost tight security'' [17]，ABE は，``pairing-free CP-ABE with limited number of users''[16]，Π_1 は，``one-time simulation-sound Groth-Sahai NIZK''[18]，Π_2 は，``Groth-Sahai NIZK''[19]である．これらの選択に拠り，GSdT の安全性要件である正当性，匿名性，追跡可能性そして陥罪不可能性は，Type-III の双線形群に対する SXDH 仮定に帰着されることとなる．

6-2 漸近性能

上述の具体的構成例で，スキームセットアップ時に固定される開封者（追跡者）の上限を L と記す．また，開封者属性の数を N と記す．また，グループ署名 σ = (Y, σ_0)のアクセス構造 Y に含まれる属性の数を n と記す．λはセキュリティパラメータである．表 1は，上述の具体的構成例の漸近性能を，グループメンバー個別秘密鍵 gsk[i]及びグループ署名 σ のビット長，また，グループ署名生成アルゴリズム GSign 及びグループ署名検証アルゴリズム GVrfy の計算量を，ランダウの記号で示したものである．

結果として，σ のビット長，GSign 及び GVrfy の計算量は，(L+2N)に比例することが分かった．これは，ABE として pairing-free なものを用いたことに起因する，改善すべき性質である．

表 1　具体的構成例の漸近性能

data	bit length
$\boldsymbol{gsk}$[i]	$O(\lambda)$
σ	$O(\lambda n(L+2N))$

algorithm	amount
GSign	$O(\lambda n(L+2N))$
GVrfy	$O(\lambda n(L+2N))$

7 むすび：振り返りと今後の課題

本稿では，研究題目「匿名性・追跡可能性・説明責任性を両立するデジタル署名とプライバシ保護の枠組の設計」の研究成果として，暗号学のアプローチによる提案方式「指定された追跡可能性を有するグループ署名」GSdT を説明した．GSdT は，グループ署名の署名者が，追跡者の属性の全体集合に対するアクセス構造を能動的に選択しグループ署名に付す．これにより，追跡者はアクセスを許可された者のみ匿名を開封できる．この点において，追跡者は説明責任を果たす根拠を持つことが出来る．

本研究では，提案方式のアルゴリズムのシンタックス及び安全性定義を与えた．また，参考文献に基づき一般的構成を与えた．更に，双線形群の構造を用いた具体的構成の例を示した．

今後の課題としては次のように考える．一般的構成の着想は，参考文献の“partially dynamic group signature scheme”において，その一般的構成の部品である公開鍵暗号を属性ベース暗号に置き換えるものであった．従って，副産物の狙いとして，公開鍵暗号を別の高機能暗号に置き換える研究がありうる．この方向性について既に着手している（文献[20]）．また，一般的構成として別の方針もありうる．即ち，“sign, then encrypt, then prove”とは異なる設計方針を，先行研究を参考に検討することは課題である．更に，本研究で示した具体的構成例は漸近性能が良くないことから，性能を改善することは課題である．また，（双線形群の構造を用いる他）格子構造[21]を用いる等，耐量子計算機暗号としての具体的構成例を与えることも重要な課題である．

【参考文献】

[1] D. Chaum and E. van Heyst: “Group Signatures”, in Proc. of EUROCRYPT ’91, 1991

[2] R. Rivest, A. Shamir and Y. T. Kalai: “How to leak a secret”, ASIACRYPT 2001

[3] H. K. Maji, M. Prabhakaran and M. Rosulek: “Attribute-Based Signatures”, in Proc. of CT-RSA 2011

[4] Y. Sakai, K. Emura, G. Hanaoka, Y. Kawai, T. Matsuda and K. Omote: “Group Signatures with Message-Dependent Opening”, in Proc. Pairing 2012
[5] M. Kohlweiss and I. Miers: “Accountable Metadata-Hiding Escrow: A Group Signature Case Study”, in Proc. Priv. Enhancing Technol. 2015
[6] J. Bootle, A. Cerulli, P. Chaidos, E. Ghadafi, J. Groth and C. Petit: “Short Accountable Ring Signatures Based on DDH”, in Proc. of ESORICS 2015
[7] B. Libert, K. Nguyen, T. Peters and M. Yung: “Bifurcated Signatures: Folding the Accountability vs. Anonymity Dilemma into a Single Private Signing Scheme”, EUROCRYPT 2021
[8] S. D. Galbraith, K. G. Paterson and N. P. Smart: “Pairings for cryptographers”, Discrete Applied Mathematics, 156(16), pp.3113-3121, 2008.
[9] S. Goldwasser, S. Micali and R. L. Rivest: “A Digital Signature Scheme Secure Against Adaptive Chosen-Message Attacks”, SIAM J. Comput. 17(2), pp.281-308, 1988.
[10] A. Sahai and B. Waters: “Fuzzy Identity-Based Encryption”, in Proc. EUROCRYPT 2005, 2005.
[11] A. Sahai: “Non-malleable non-interactive zero-knowledge and adaptive chosen-ciphertext security”, in Proc. FOCS 2001
[12] M. Bellare, H. Shi and C. Zhang: “Foundations of Group Signatures: The Case of Dynamic Groups”, in Proc. CT-RSA 2005
[13] H. Anada, M. Fukumitsu and S. Hasegawa: “Group Signatures with Designated Traceability”, CANDAR 2021
[14] H. Anada, M. Fukumitsu and S. Hasegawa: “Group Signatures with Designated Traceability over Openers’ Attributes”, to appear in Int. J. Network and Computing.
[15] 穴田啓晃, 福光正幸, 長谷川真吾:「指定された追跡可能性を有するグループ署名の双線形群における例示」, 2022 年暗号と情報セキュリティシンポジウム予稿論文集, 2022 年
[16] J. Herranz: “Attribute-based versions of Schnorr and ElGamal”, Appl. Algebra Eng. Commun. Comput. 27(1), pp.17-57, 2016
[17] M. Abe, D. Hofheinz, R. Nishimaki, M. Ohkubo and J. Pan: “Compact Structure-Preserving Signatures with Almost Tight Security”, CRYPTO 2017
[18] B. Libert and M. Yung: “Non-interactive CCA-Secure Threshold Cryptosystems with Adaptive Security: New Framework and Constructions”, in Proc. TCC 2012
[19] J. Groth and A. Sahai: “Efficient Non-interactive Proof Systems for Bilinear Groups”, EUROCRYPT ’08, 2008
[20] 穴田啓晃, 安在恭弥:「署名者に対する等検査付きグループ署名の検討」, 電子情報通信学会情報セキュリティ研究会技術研究報告集, 2022 年
[21] S. Ling, K. Nguyen, H. Wang and Y. Xu: “Accountable Tracing Signatures from Lattices”, CT-RSA 2019

〈発 表 資 料〉

題 名	掲載誌・学会名等	発表年月
Group Signatures with Designated Traceability	Proceedings of CANDAR2021	2021 年 11 月
指定された追跡可能性を有するグループ署名の双線形群における例示	2022 年暗号と情報セキュリティシンポジウム予稿論文集	2022 年 1 月
署名者に対する等検査付きグループ署名の検討	電子情報通信学会情報セキュリティ研究会技術研究報告集	2022 年 3 月