属性による指定追跡者グループ署名の格子からの構成

穴田 啓晃[1,a)]　福光 正幸[2,b)]　長谷川 真吾[3,c)]

概要：指定追跡者グループ署名 (GSdT) は，署名者が追跡者を属性上のアクセス構造で指定可能なグループ署名である．本稿では GSdT の具体的な構成について，格子ベースのものをはじめて提案する．

Group Signatures with Designated Traceability over Openers' Attributes from Lattices

Hiroaki Anada[1,a)]　Masayuki Fukumitsu[2,b)]　Shingo Hasegawa[3,c)]

Abstract: The *group signature with designated traceability* (GSdT) is a kind of group signatures (GS) that the actual signer can control openers by setting an access structure over openers' attributes. In this paper, we give a lattice-based GSdT scheme for the first time.

1. はじめに

グループ署名（GS） [1] はグループメンバにグループとしての署名を許可する署名技術である．グループ署名に要求される代表的な性質として匿名性（anonymity）と追跡性（traceability）が挙げられる．匿名性は実署名者が誰か署名からはわからないことを保証し，追跡性はグループ管理者がトラップドアにより署名から実署名者を特定できることを表す．

グループ管理者は全ての署名を開封し実署名者を追跡できるため，システムによってはその権限が強すぎると見られる可能性がある．実際，グループ管理者の追跡権限を適切に制限するための研究が行われている．メッセージ依存開封型グループ署名（Group Signature with Message-Dependent Opening, GS-MDO）[2] は追跡権限を開封者と許可者に分割している．説明可能追跡性（accountable tracing）[3], [4] は，グループを追跡可能ユーザと追跡不可能ユーザの 2 種に分割するが，追跡権限をコントロールすることは署名者にはできない．二分岐匿名署名（bifurcated anonymous signature）[5] は，署名者に対して署名生成時に追跡可能な署名かどうかの選択を許可する．説明可能リング署名（accountable ring signature）[6] では，署名者に開封者の選択権限が与えられる．すなわち，指定された開封者は実署名者を特定可能であるが，その他の開封者には署名の匿名性が保たれる．この点で，説明可能リング署名は匿名性と追跡性をバランスする技術と考えられるが，指定できる開封者は 1 人のみである．

指定追跡者グループ署名 (Group Signature with designated Traceability, GSdT) [7, 8] はより柔軟な開封者の選択を目指して提案された．署名者は署名生成時に開封者が持つ属性へのアクセス構造を指定することにより，開封者の選択をコントロール可能である．指定追跡者グループ署名の構成例については，文献 [7], [8] において暗号文ポリシー属性ベース暗号（CP-ABE），署名，非対話型ゼロ知識証明（NIZK）からの一般的構成が与えられた．具体的な構成については [9] にてペアリングからの構成が，[10] で耐量子計算機性のため対象鍵要素からの構成が示された．ただし，[10] における匿名性は [8] での定義よりも弱いものとなっていた．

[1] 明治学院大学
Meiji Gakuin University
[2] 長崎県立大学
University of Nagasaki
[3] 福島大学
Fukushima University
[a)] hiroaki.anada@mi.meijigakuin.ac.jp
[b)] fukumitsu@sun.ac.jp
[c)] hasegawa@sss.fukushima-u.ac.jp

1.1 貢献

本論文では文献 [8] の意味での匿名性と耐量子計算機性を持つ指定追跡者グループ署名として格子からの構成を提案する．指定追跡者グループ署名には既に一般的構成 [7,8] が知られており，それは通常のグループ署名 [11] のように sign-then-encrypt-then-prove 構成となっている．ここで，いくつかの格子ベースグループ署名はより簡易な構成である encrypt-then-prove 構成となっている [3,12–14]．これは，ビルディングブロックとして使用されるプリミティブの相性の良さを利用している．そこで，我々は同様の戦略を採用し，既存の一般的構成を格子ベースのプリミティブで組み上げる構成よりも簡易な構成を試みる．

構成のアイディアは Tsabary [15] による 格子ベース CP-ABE と Libert らの格子ベースグループ署名 [16]（LLMNW GS）の組み合わせである．この 2 つの方式は Regev 暗号 [17] を利用しているという共通項を持つ．Tsabary の CP-ABE は Regev 暗号の CP-ABE への拡張であり，LLMNW GS は Regev 暗号による暗号化処理の正しさを NIZK で証明している．この特徴を利用し，指定追跡者グループ署名を encrypt-then-prove 構成にて構成する．我々の構成は部品として採用するプリミティブの特徴を利用し指定追跡者グループ署名の新たな構成方法を与えるものである．

提案方式の有効性検証として，同じプリミティブを使用して [8] の一般的構成により構成した方式との比較を行う．漸近的評価の結果として，各種鍵サイズや署名サイズを一般的構成よりも大幅に削減できることがわかった．

指定追跡者グループ署名では署名作成時にアクセス構造を指定するが，提案方式で利用可能な構造は t-CNF に限定されている．より広いクラスのアクセス構造を利用可能な方式の開発は今後の課題である．

2. 準備

$\mathbb{N}$，$\mathbb{Z}$，$\mathbb{R}$ をそれぞれ自然数，整数，実数の集合とする．任意の整数 $a \le b$ に対し，$[a,b] \subseteq \mathbb{Z}$ を $a \le x \le b$ である整数 x の集合とする．任意の整数 $a \in \mathbb{Z}$ と正の奇数 N に対し，$a \bmod^{\pm} N$ は $x = a \bmod N$ を表すとする．ここで，$-(N-1)/2 \le x \le (N-1)/2$ である．

$\boldsymbol{b} \in \mathbb{Z}^n$ を n 次元ベクトルとし，行ベクトルで表されるとする．$\|\boldsymbol{b}\|_2$ と $\|\boldsymbol{b}\|$ はそれぞれ $\boldsymbol{b}$ のユークリッドノルムと無限大ノルムである．$\boldsymbol{b}^T$ で $\boldsymbol{b}$ の転置ベクトルを，$\mathsf{bin}(\boldsymbol{b})$ で $\boldsymbol{b}$ の 2 進表現をそれぞれ表す．任意の自然数 $a \in \mathbb{N}$ について，$\boldsymbol{a}^n$ を $\begin{bmatrix} a & a & \cdots & a \end{bmatrix}^T \in \mathbb{Z}^n$ とする．任意の文字列 $s \in \{0,1\}^n$ について，$s[i]$ を s の i 番目のビットとする．

任意のベクトル $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{Z}^n$ について，$[\boldsymbol{a}|\boldsymbol{b}] \in \mathbb{Z}^{n\times 2}$ を $\boldsymbol{a}$ と $\boldsymbol{b}$ の水平方向の連結ベクトルとする．また，$\begin{bmatrix} \boldsymbol{a} \\ \hline \boldsymbol{b} \end{bmatrix} \in \mathbb{Z}^{2n}$ を垂直方向の連結ベクトルとする．行列についても同様の記法を採用する．$\boldsymbol{B} \in \mathbb{R}^{n\times m}$ をフルランク行列とするとき，$\tilde{\boldsymbol{B}}$ をグラムシュミット直交行列とする．

集合 X 上の確率分布 $\mathcal{D}$ に対し，$x \leftarrow\!\$\ \mathcal{D}$ は分布 $\mathcal{D}$ に従って X を取る操作を表す．特に，$\mathcal{D}$ が X 上の一様分布であるとき，$x \leftarrow\!\$\ X$ と書く．実数 $\epsilon \ge 0$，X_λ 上のパラメタライズされたアンサンブル $(\mathcal{D}_{1,\lambda})_{\lambda\in\mathbb{N}}$，$(\mathcal{D}_{2,\lambda})_{\lambda\in\mathbb{N}}$ について，$(\mathcal{D}_{1,\lambda})_{\lambda\in\mathbb{N}}$ が $(\mathcal{D}_{2,\lambda})_{\lambda\in\mathbb{N}}$ に **ϵ-近接**するとは，統計的距離 $(1/2)\sum_{x\in X_\lambda}|\mathcal{D}_{1,\lambda}(x) - \mathcal{D}_{2,\lambda}(x)|$ が十分大きい λ について $\epsilon(\lambda)$ となることを言う．関数 ϵ が λ **において無視できる**とは，任意の多項式 p に対し $\lambda_0 \in \mathbb{N}$ が存在し，$\lambda \ge \lambda_0$ となる λ に対し $\epsilon(\lambda) < 1/p(\lambda)$ となることを言う．$(\mathcal{D}_{1,\lambda})_{\lambda\in\mathbb{N}}$ が無視できる関数 ϵ について $(\mathcal{D}_{2,\lambda})_{\lambda\in\mathbb{N}}$ に ϵ-近接するとき，$(\mathcal{D}_{1,\lambda})_{\lambda\in\mathbb{N}}$ は $(\mathcal{D}_{2,\lambda})_{\lambda\in\mathbb{N}}$ に **統計的近接** と言う．PPT と DPT で確率的多項式時間と決定的多項式時間をそれぞれ表す．

2.1 格子

$m \ge n \ge 1$ を整数，q を素数とする．格子 $\mathcal{L} \subseteq \mathbb{R}^n$ は基底 $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m \in \mathbb{Z}^n$ の整数係数による線形結合として定義される．行列 $\boldsymbol{A} \in \mathbb{Z}_q^{n\times m}$ とベクトル $\boldsymbol{u} \in \mathbb{Z}_q^n$ について，以下の集合を定義する:

$$\Lambda_q(\boldsymbol{A}) = \{\boldsymbol{e} \in \mathbb{Z}^m \mid \exists \boldsymbol{s} \in \mathbb{Z}_q^n \ \textbf{s.t.}\ \boldsymbol{A}^T\boldsymbol{s} = \boldsymbol{e} \bmod q\},$$
$$\Lambda_q^{\perp}(\boldsymbol{A}) = \{\boldsymbol{e} \in \mathbb{Z}^m \mid \boldsymbol{A}\boldsymbol{e} = \boldsymbol{0} \bmod q\},$$
$$\Lambda_q^{\boldsymbol{u}}(\boldsymbol{A}) = \{\boldsymbol{e} \in \mathbb{Z}^m \mid \boldsymbol{A}\boldsymbol{e} = \boldsymbol{u} \bmod q\}.$$

$\mathcal{L} \subseteq \mathbb{R}^m$ を格子，$\boldsymbol{c} \in \mathbb{R}^n$ をベクトル，$\sigma > 0$ を実数とする．$\rho_{\sigma,\boldsymbol{c}}(\boldsymbol{x}) = \exp(-\pi\|\boldsymbol{x}-\boldsymbol{c}\|^2/\sigma^2)$ とする．標準偏差 σ の $\boldsymbol{c}$ を中心とした $\mathcal{L}$ 上の離散ガウス分布 $D_{\mathcal{L},\sigma,\boldsymbol{c}}$ は $\rho_{\sigma,\boldsymbol{c}}(\boldsymbol{y})/\rho_{\sigma,\boldsymbol{c}}(\mathcal{L})$ $(\boldsymbol{y} \in \mathcal{L})$ で定義される．$\boldsymbol{c} = \boldsymbol{0}^n$ のとき，単に $D_{\mathcal{L},\sigma}$ と書く．また，$\boldsymbol{x} \leftarrow\!\$\ D_{\mathcal{L},\sigma}$ の無限大ノルムが $\sigma\sqrt{m}$ 以下となる確率は $1 - 2^{\Omega(m)}$ より大きいことが知られている [18].

提案方式で使用する種々のアルゴリズムを導入する．

- $\mathsf{TrapGen}(1^n, 1^m, q)$ [19]: 入力 1^n，1^m，$q > 2$ $(m \ge \Omega(n\log q))$ に対し，行列 $\boldsymbol{A} \in \mathbb{Z}_q^{n\times m}$ と $\Lambda_q^{\perp}(\boldsymbol{A})$ の基底 $\boldsymbol{T}_{\boldsymbol{A}}$ を出力する．ただし，$\boldsymbol{A}$ の分布は $\mathbb{Z}_q^{n\times m}$ 上の一様分布に $2^{-\Omega(n)}$-近接 であり，$\left\|\tilde{\boldsymbol{T}_{\boldsymbol{A}}}\right\| \le O(\sqrt{n\log q})$ である．
- $\mathsf{ExtBasis}(\overline{\boldsymbol{A}}, \boldsymbol{T}_{\boldsymbol{A}})$ [20]: 行列 $\overline{\boldsymbol{A}} = [\boldsymbol{A}|\boldsymbol{A}'] \in \mathbb{Z}^{n\times\overline{m}}$，$\Lambda_q^{\perp}(\boldsymbol{A})$ の基底 $\boldsymbol{T}_{\boldsymbol{A}}$ を入力とし，$\left\|\boldsymbol{T}_{\overline{\boldsymbol{A}}}\right\| \le \|\boldsymbol{T}_{\boldsymbol{A}}\|$ を満たす $\Lambda_q^{\perp}(\overline{\boldsymbol{A}})$ の基底 $\boldsymbol{T}_{\overline{\boldsymbol{A}}}$ を出力する．
- $\mathsf{SamplePre}(\boldsymbol{A}, \boldsymbol{T}_{\boldsymbol{A}}, \boldsymbol{u}, \sigma)$ [21]: 行列 $\boldsymbol{A} \in \mathbb{Z}_q^{n\times m}$, $\Lambda_q^{\perp}(\boldsymbol{A})$ の基底 $\boldsymbol{T}_{\boldsymbol{A}}$，$\sigma \ge \left\|\tilde{\boldsymbol{T}_{\boldsymbol{A}}}\right\| \cdot \omega(\sqrt{\log m})$，$\boldsymbol{u} \in \mathbb{Z}^n$ を入力とし，$\boldsymbol{A}\boldsymbol{e} = \boldsymbol{u} \bmod q$ である $\boldsymbol{e} \leftarrow\!\$\ D_{\mathbb{Z}^m,\sigma}$ を出力する．また，$\mathsf{SamplePre}$ への入力としてベクトル $\boldsymbol{u} \in \mathbb{Z}^n$ の代わりに行列 $\boldsymbol{U} = [\boldsymbol{u}_1 \mid \cdots \mid \boldsymbol{u}_m] \in \mathbb{Z}_q^{n\times m}$

を許す．このとき，SamplePre は ベクトル $\boldsymbol{e}_j \leftarrow\!\$\ \mathsf{SamplePre}(\boldsymbol{A}, \boldsymbol{T}_{\boldsymbol{A}}, \boldsymbol{u}_j, \sigma)$ $(j \in [1, m])$ を計算し，行列 $\boldsymbol{E} = [\boldsymbol{e}_1 \mid \cdots \mid \boldsymbol{e}_m]$ を出力する．

本論文で使用する暗号学的仮定を定義する．

- Short Integer Solution ($\mathsf{SIS}_{n,m,q,\beta}$) 仮定: n, m, q, β を $\lambda \in \mathbb{N}$ の関数とする．$\mathsf{SIS}_{n,m,q,\beta}$ 仮定は，任意の PPT アルゴリズム $\mathcal{A}$ が行列 $\boldsymbol{A} \leftarrow\!\$\ \mathbb{Z}_q^{n\times m}$ を与えられたとき，$\|\boldsymbol{x}\| \le \beta$ である非ゼロベクトル $\boldsymbol{x} \in \Lambda_q^{\perp}(\boldsymbol{A})$ を見つける確率が無視できることをいう．
- Decisional Lerning with Errors ($\mathsf{LWE}_{n,q,\chi}$) 仮定: n と q を $\lambda \in \mathbb{N}$ の関数とし，χ を $\mathbb{Z}$ 上の確率分布とする．$\mathsf{LWE}_{n,q,\chi}$ 仮定は，任意の PPT アルゴリズム $\mathcal{A}$ が以下の 2 つの確率分布により生成されたベクトル $(\boldsymbol{A}, \boldsymbol{t})$ を判別できないことをいう:
  - $\boldsymbol{A} \leftarrow\!\$\ \mathbb{Z}_q^{n\times m}; \boldsymbol{t} \leftarrow\!\$\ \mathbb{Z}_q^m$
  - $\boldsymbol{A} \leftarrow\!\$\ \mathbb{Z}_q^{n\times m}; \boldsymbol{s} \leftarrow\!\$\ \mathbb{Z}_q^n; \boldsymbol{e} \leftarrow\!\$\ \chi^m; \boldsymbol{t} \leftarrow \boldsymbol{A}^T\boldsymbol{s} + \boldsymbol{e}$.

χ を B-bounded とする．すなわち，χ からサンプリングされるベクトルの無限ノルムは B 以下である．また，$\tilde{B}$-bounded ($B \ge \sqrt{n}\omega(\log n)$) な $\tilde{\chi}$ について，$\tilde{B}(\lambda) = B(\lambda) \cdot \lambda^{\omega(1)}$ である．具体例については [15] を参照されたい．

3. 指定追跡者グループ署名

指定追跡者グループ署名 (Group Signature with designated Traceability, GSdT) [8] に関わる定義を導入する．$\mathbb{U}$ を属性空間とする．$\mathcal{R}(X, Y) = 1$ または $Y(X) = 1$ で，属性 X がアクセスポリシー Y を満たすとする．ここで $\mathcal{R}$ は Y に関連する二項関係である．

3.1 シンタックス

GSdT のエンティティは発行者 $\mathcal{I}$，マスター開封者 $\mathcal{OM}$，開封者 $\mathcal{OP}_j$，ユーザ $\mathcal{U}_i$ である．GSdT は以下のアルゴリズムとプロトコルから構成される．

- $\mathsf{GKG}(1^\lambda, \mathbb{U})$: PPT 鍵生成アルゴリズム GKG は，セキュリティパラメータ 1^λ と属性空間 $\mathbb{U}$ を入力とし，グループ公開鍵 gpk，発行者鍵 ik，マスター開封者鍵 omk を出力する．ik と omk は $\mathcal{I}$ と $\mathcal{OM}$ がそれぞれ所有する．また，テーブル **reg** を初期化する．
- $\mathsf{OKG}(\mathsf{gpk}, \mathsf{omk}, j, X)$: PPT 開封者鍵生成アルゴリズム OKG は $\mathcal{OM}$ によって実行される．グループ公開鍵 gpk，マスター開封者鍵 omk，開封者 $\mathcal{OP}_j$ のインデックス j と属性 X を入力とし，$\mathcal{OP}_j$ の X における開封者鍵 ok_j を出力する．
- $\mathsf{UKG}(1^\lambda)$: PPT ユーザ鍵生成アルゴリズム UKG はユーザ $\mathcal{U}_i$ のグループ参加の際に実行される．セキュリティパラメータ 1^λ を入力とし，ユーザ公開鍵 upk とユーザ秘密鍵 usk を出力する．
- グループ参加プロトコル: ユーザ $\mathcal{U}_i$ がグループに参加するときに発行者 $\mathcal{I}$ との間で実行される．プロトコルの内容は 図 1 に示す．プロトコルの実行後，$\mathcal{U}_i$ はユーザ署名鍵 gsk_i を入手し，$\mathcal{I}$ はユーザテーブル **reg** を更新する．

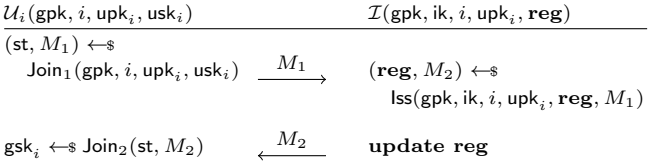

図 1 グループ参加プロトコル
Fig. 1 Joining Protocol

- $\mathsf{GSig}(\mathsf{gpk}, \mathsf{gsk}_i, Y, \mu)$: PPT 署名アルゴリズム GSig は $\mathcal{U}_i$ によって実行される．グループ公開鍵 gpk，ユーザ署名鍵 gsk_i，アクセスポリシー Y，メッセージ μ を入力とし，署名 $\Sigma = (Y, \Sigma_0)$ を出力する．
- $\mathsf{GVf}(\mathsf{gpk}, \mu, (Y, \Sigma_0))$: DPT 検証アルゴリズム GVf は，グループ公開鍵 gpk，メッセージ μ，署名 (Y, Σ_0) を入力とし，Σ が μ の gpk における 正当な署名であるとき 1 を出力する．
- $\mathsf{Open}(\mathsf{gpk}, \mathsf{ok}_j, \mathbf{reg}, \mu, (Y, \Sigma_0))$: PPT 開封アルゴリズム Open は $\mathcal{OP}_j$ によって実行される．グループ公開鍵 gpk，開封者鍵 ok_j，ユーザテーブル **reg**，メッセージ μ，署名 (Y, Σ_0) を入力とし，署名者を表すインデックス i と開封プロセスの正当性を保証する証明 τ を出力する．
- $\mathsf{Judge}(\mathsf{gpk}, i, \mathsf{upk}_i, \mu, (Y, \Sigma_0), \tau)$: DPT 判定アルゴリズム Judge はグループ公開鍵 gpk，インデックス i，ユーザ公開鍵 upk_i，メッセージ μ，署名 (Y, Σ_0)，証明 τ を入力とし，τ が (Y, Σ_0) と (i, upk_i) について正当であるとき 1 を出力する．

3.2 安全性

まず，安全性ゲームの中で使用するオラクルを導入する．

3.2.1 オラクル

オラクルが使用するリスト，テーブルは以下のとおりである．HO: 正当開封者リスト，HU: 正当ユーザリスト，CO: コラプト開封者リスト，CU: コラプトユーザリスト，**upk**: ユーザ公開鍵テーブル，**usk**: ユーザ秘密鍵テーブル，**gsk**: ユーザ署名鍵テーブル，**ok**: 開封者鍵テーブル，**reg**: ユーザテーブル，MS: チャレンジ集合，$\mathbf{st}_{\mathsf{Join}}$，$\mathbf{st}_{\mathsf{Iss}}$: 状態リスト．

- $\mathsf{AddOO}(j, X)$: 属性 X を持つ開封者 $\mathcal{OP}_j$ を正当開封者リストに追加する: $HO \leftarrow HO \cup \{j\}$, $\mathsf{ok}[j] \leftarrow \mathsf{OKG}(\mathsf{gpk}, \mathsf{omk}, j, X)$.
- $\mathsf{AddUO}(i)$: ユーザ $\mathcal{U}_i$ $(i \notin HU \cup CU)$ を正当ユーザリストに追加する: $HU \leftarrow HU \cup \{i\}$, $(\mathbf{upk}[i], \mathbf{usk}[i]) \leftarrow\!\$\ \mathsf{UKG}(1^\lambda)$. また，グループ参加プロトコルを実行し，$\mathbf{upk}[i]$ を出力

する: $(\mathsf{st}, M_1) \leftarrow\!\$\ \mathsf{Join}_1(\mathsf{gpk}, i, \mathbf{upk}[i], \mathbf{usk}[i])$, $(\mathbf{reg}, M_2) \leftarrow\!\$\ \mathsf{Iss}(\mathsf{gpk}, \mathsf{ik}, i, \mathbf{upk}[i], \mathbf{reg}, M_1)$, $\mathbf{gsk}[i] \leftarrow\!\$\ \mathsf{Join}_2(\mathsf{st}, M_2)$, $\mathbf{st}_{\mathsf{Join}}[i] \leftarrow (\mathsf{gpk}, i, \mathbf{upk}[i], \mathbf{usk}[i])$.

- $\mathsf{StoUO}(i, M_{in})$: グループ参加プロトコルにおけるユーザ $\mathcal{U}_i$ の動作を行い M_{out} を出力する．$HU \leftarrow HU \cup \{i\}$, $(\mathbf{upk}[i], \mathbf{usk}[i]) \leftarrow\!\$\ \mathsf{UKG}(1^\lambda)$, $\mathbf{st}_{\mathsf{Join}}[i] \leftarrow (\mathsf{gpk}, i, \mathbf{upk}[i], \mathbf{usk}[i])$. $M_{in} = \epsilon$ のとき $(\mathsf{st}, M_{out}) \leftarrow\!\$\ \mathsf{Join}_1(\mathsf{gpk}, i, \mathbf{upk}[i], \mathbf{usk}[i])$, $\mathbf{st}_{\mathsf{Join}}[i] \leftarrow \mathsf{st}$，そうでないとき $M_{out} \leftarrow\!\$\ \mathsf{Join}_2(\mathbf{st}_{\mathsf{Join}}[i], M_{in})$, $\mathbf{gsk}[i] \leftarrow M_{out}$, $\mathbf{st}_{\mathsf{Join}}[i] \leftarrow (\mathsf{gpk}, i, \mathbf{upk}[i], \mathbf{usk}[i])$.
- $\mathsf{StoIO}(i, M_{in})$: グループ参加プロトコルにおける Iss の動作を行い M_{out} を出力する．ただし，$i \in CU$ とする: $(\mathbf{reg}, M_{out}) \leftarrow\!\$\ \mathsf{Iss}(\mathsf{gpk}, \mathsf{ik}, i, \mathbf{upk}[i], \mathbf{reg}, M_{in})$.
- $\mathsf{CrptOO}(j)$: 開封者 $\mathcal{OP}_j$ の開封者鍵 $\mathbf{ok}[j]$ を出力する: $CO \leftarrow CO \cup \{j\}$. ただし，任意の $(m, (Y, \Sigma_0)) \in MS$ について $R(X, Y) \neq 1$ $((X, \mathsf{ok}_0) \leftarrow \mathbf{ok}[j])$ である．
- $\mathsf{CrptUO}(i, \mathsf{upk})$: ユーザ $\mathcal{U}_i$ $(i \notin HU \cup CU)$ をコラプトユーザリストに追加する: $CU \leftarrow CU \cup \{i\}$, $\mathbf{upk}[i] \leftarrow \mathsf{upk}$, $\mathbf{st}_{\mathsf{Iss}}[i] \leftarrow (\mathsf{gpk}, \mathsf{ik}, i, \mathsf{upk})$.
- $\mathsf{USKO}(i)$: ユーザ $\mathcal{U}_i$ の秘密鍵 $(\mathbf{usk}[i], \mathbf{gsk}[i])$ を出力する．
- $\mathsf{GSignO}(i, Y, \mu)$: メッセージ μ のポリシー Y における署名 (Y, Σ_0) を出力する: $(Y, \Sigma_0) \leftarrow\!\$\ \mathsf{GSig}(\mathsf{gpk}, \mathbf{gsk}[i], Y, \mu)$.
- $\mathsf{OpenO}(j, \mu, (Y, \Sigma_0))$: 署名 (Y, Σ_0) の開封結果 $\mathsf{Open}(\mathsf{gpk}, \mathsf{ok}[j], \mu, (Y, \Sigma_0))$ を出力する．ただし，$(\mu, (Y, \Sigma_0)) \notin MS$.
- $\mathsf{RRegO}(i)$: ユーザテーブルの内容 $\mathbf{reg}[i]$ を出力する．
- $\mathsf{WRegO}(i, \rho)$: ユーザテーブルを更新する: $\mathbf{reg}[i] \leftarrow \rho$.
- $\mathsf{ChaO}_b(i_0, i_1, \mu, Y)$ $(b \in \{0, 1\})$: チャレンジ $\Sigma \leftarrow\!\$\ \mathsf{GSig}(\mathsf{gpk}, \mathbf{gsk}[i_b], \mu)$ を出力する: $MS \leftarrow MS \cup \{(\mu, \Sigma)\}$.

GSdT の安全性を定義する [8]．各性質の安全性ゲームは図 2 で与えられる．

Definition 1 (正当性)．GSdT が正当であるとは，任意の PPT アルゴリズム $\mathcal{A}$ に対し，$\mathsf{Exp}^{\mathrm{corr}}_{\mathsf{GSdT},\mathcal{A},\mathbb{U}}(\lambda) = 1$ となる確率が無視できることをいう．

Definition 2 (匿名性)．GSdT が匿名性をを持つとは，任意の PPT アルゴリズム $\mathcal{A}$ に対し，$\left|\mathsf{Exp}^{\text{anom-0}}_{\mathsf{GSdT},\mathcal{A},\mathbb{U}}(\lambda) - \mathsf{Exp}^{\text{anom-1}}_{\mathsf{GSdT},\mathcal{A},\mathbb{U}}(\lambda)\right|$ が無視できることをいう．

Definition 3 (追跡可能性)．GSdT が追跡可能とは，任意の PPT アルゴリズム $\mathcal{A}$ に対し，$\mathsf{Exp}^{\mathrm{trac}}_{\mathsf{GSdT},\mathcal{A},\mathbb{U}}(\lambda) = 1$ となる確率が無視できることをいう．

Definition 4 (陥罪不可能性)．GSdT が陥罪不可能であるとは，任意の PPT アルゴリズム $\mathcal{A}$ に対し，$\mathsf{Exp}^{\mathrm{nf}}_{\mathsf{GSdT},\mathcal{A},\mathbb{U}}(\lambda) = 1$ となる確率が無視できることをいう．

$\mathsf{Exp}^{\mathrm{corr}}_{\mathsf{GSdT},\mathcal{A},\mathbb{U}}$

$(\mathsf{gpk}, \mathsf{ik}, \mathsf{omk}) \leftarrow\!\$\ \mathsf{GKG}(1^\lambda, \mathbb{U});\ HO \leftarrow \emptyset;\ HU \leftarrow \emptyset;\ CO \leftarrow \emptyset$
$\mathbf{upk} \leftarrow \emptyset;\ \mathbf{usk} \leftarrow \emptyset;\ \mathbf{gsk} \leftarrow \emptyset;\ \mathbf{ok} \leftarrow \emptyset;\ \mathbf{reg} \leftarrow \emptyset;\ \mathbf{st}_{\mathsf{Join}} \leftarrow \emptyset;\ \mathbf{st}_{\mathsf{Iss}} \leftarrow \emptyset$
$(i, \mu, Y) \leftarrow\!\$\ \mathcal{A}^{\mathsf{AddOO},\mathsf{AddUO},\mathsf{RRegO}}(\mathsf{gpk})$
return 0 **if** $i \notin HU \vee \mathbf{gsk}[i] = \epsilon$
$\Sigma \leftarrow\!\$\ \mathsf{GSig}(\mathsf{gpk}, \mathbf{gsk}[i], Y, \mu)$
return 1 **if** $\mathsf{GVf}(\mathsf{gpk}, \mu, \Sigma) \neq 1$
$OS_Y \leftarrow \{j \in HO \mid R(X, Y) = 1$ **for** $(X, \mathsf{ok}) \leftarrow \mathbf{ok}[j]\}$
for $j \in OS_Y$:
  $(i', \tau) \leftarrow\!\$\ \mathsf{Open}(\mathsf{gpk}, \mathbf{ok}[j], \mathbf{reg}, \mu, \Sigma)$
  return 1 **if** $i \neq i' \vee \mathsf{Judge}(\mathsf{gpk}, i, \mathbf{upk}[i], \mu, \Sigma, \mu) \neq 1$
return 0

$\mathsf{Exp}^{\text{anom-}b}_{\mathsf{GSdT},\mathcal{A},\mathbb{U}}$

$(\mathsf{gpk}, \mathsf{ik}, \mathsf{omk}) \leftarrow\!\$\ \mathsf{GKG}(1^\lambda, \mathbb{U});\ HO \leftarrow \emptyset;\ HU \leftarrow \emptyset;\ CO \leftarrow \emptyset;\ CU \leftarrow \emptyset$
$\mathbf{upk} \leftarrow \emptyset;\ \mathbf{usk} \leftarrow \emptyset;\ \mathbf{gsk} \leftarrow \emptyset;\ \mathbf{ok} \leftarrow \emptyset;\ \mathbf{reg} \leftarrow \emptyset;\ MS \leftarrow \emptyset$
$\mathbf{st}_{\mathsf{Join}} \leftarrow \emptyset;\ \mathbf{st}_{\mathsf{Iss}} \leftarrow \emptyset$
$d \leftarrow\!\$\ \mathcal{A}^{\mathsf{ChaO}_b,\mathsf{AddOO},\mathsf{OpenO},\mathsf{StoUO},\mathsf{WRegO},\mathsf{USKO},\mathsf{CrptOO},\mathsf{CrptUO}}(\mathsf{gpk}, \mathsf{ik})$
return d

$\mathsf{Exp}^{\mathrm{trac}}_{\mathsf{GSdT},\mathcal{A},\mathbb{U}}$

$(\mathsf{gpk}, \mathsf{ik}, \mathsf{omk}) \leftarrow\!\$\ \mathsf{GKG}(1^\lambda, \mathbb{U});\ HO \leftarrow \emptyset;\ HU \leftarrow \emptyset;\ CO \leftarrow \emptyset$
$\mathbf{upk} \leftarrow \emptyset;\ \mathbf{usk} \leftarrow \emptyset;\ \mathbf{gsk} \leftarrow \emptyset;\ \mathbf{ok} \leftarrow \emptyset;\ \mathbf{reg} \leftarrow \emptyset;\ \mathbf{st}_{\mathsf{Join}} \leftarrow \emptyset;\ \mathbf{st}_{\mathsf{Iss}} \leftarrow \emptyset$
$(\mu, (Y, \Sigma_0)) \leftarrow\!\$\ \mathcal{A}^{\mathsf{StoIO},\mathsf{AddUO},\mathsf{RRegO},\mathsf{USKO},\mathsf{CrptUO}}(\mathsf{gpk}, \mathsf{omk})$
return 0 **if** $\mathsf{GVf}(\mathsf{gpk}, \mu, (Y, \Sigma_0)) \neq 1$
find X **s.t.** $\mathcal{R}(X, Y) = 1;\ \mathsf{ok} \leftarrow\!\$\ \mathsf{OKG}(\mathsf{gpk}, \mathsf{omk}, 0, X)$
$(i, \tau) \leftarrow \mathsf{Open}(\mathsf{gpk}, \mathsf{ok}, \mathbf{reg}, \mu, (Y, \Sigma_0))$
return 1 **if** $i = 0 \vee \mathsf{Judge}(\mathsf{gpk}, i, \mathbf{upk}[i], \mu, (Y, \Sigma_0), \tau) \neq 1$
else return 0

$\mathsf{Exp}^{\mathrm{nf}}_{\mathsf{GSdT},\mathcal{A},\mathbb{U}}$

$(\mathsf{gpk}, \mathsf{ik}, \mathsf{omk}) \leftarrow\!\$\ \mathsf{GKG}(1^\lambda, \mathbb{U});\ HO \leftarrow \emptyset;\ HU \leftarrow \emptyset;\ CO \leftarrow \emptyset$
$\mathbf{upk} \leftarrow \emptyset;\ \mathbf{usk} \leftarrow \emptyset;\ \mathbf{gsk} \leftarrow \emptyset;\ \mathbf{ok} \leftarrow \emptyset;\ \mathbf{reg} \leftarrow \emptyset;\ \mathbf{st}_{\mathsf{Join}} \leftarrow \emptyset;\ \mathbf{st}_{\mathsf{Iss}} \leftarrow \emptyset$
$(\mu, (Y, \Sigma_0), i, \tau) \leftarrow\!\$\ \mathcal{A}^{\mathsf{StoUO},\mathsf{WRegO},\mathsf{GSignO},\mathsf{USKO},\mathsf{CrptUO}}(\mathsf{gpk}, \mathsf{ik}, \mathsf{omk})$
return 1 **if** $i \in HU \wedge \mathbf{gsk}[i] \neq \epsilon \wedge \mathsf{Judge}(\mathsf{gpk}, i, \mathbf{upk}[i], \mu, (Y, \Sigma_0), \tau) = 1$
  $\wedge\ i$ is not queried to $\mathsf{USKO} \wedge (i, \mu)$ is not queried to GSignO
else return 0

図 2 GSdT の安全性ゲーム
Fig. 2 Security Games on GSdT

4. 提案方式

本節では格子ベース GSdT 方式を提案する．提案方式で使用するパラメータを表 1 に示す．まず方式内で使用するサブアルゴリズムを導入する．

4.1 サブアルゴリズム: DS

サブアルゴリズム $\mathsf{DS} = (\mathsf{SKGen}, \mathsf{Sign}, \mathsf{Vf})$ を図 3 に示す．ここでメッセージ μ の全体空間は $\{0, 1\}^{2m}$ である．

表 1 提案方式のパラメータ
Table 1 Parameters

N	メンバー数	$poly(\lambda)$
ξ	属性の長さ	$poly(\lambda)$
n	行数	$O(\lambda)$
q	法の大きさ	$\tilde{O}(\ell n^3)$
m	DS に関する列数	$2n\lceil \log n \rceil$
$\tilde{m}$	ABE の $\boldsymbol{C}$ の列数	$n\lceil \log n \rceil$
$\tilde{m}'$	ABE の $\boldsymbol{B}$ の列 数	$(n+1)\log q + 2\lambda$
ℓ	τ の長さ	$N = 2^\ell$
σ	$\boldsymbol{d}$ の標準偏差	$\Omega(\sqrt{n \log q} \log n)$
σ_1	$\boldsymbol{s}$ の標準偏差	$\sqrt{(4\sqrt{2}\sigma m^{3/2})^2 + \sigma^2}$
β	DS の無限ノルム	$\sigma\omega(\sqrt{m})$
κ	NIZK の反復回数	$\omega(\log n)$
l	ABE の平文長	$2m$
ϵ	効率パラメータ	$0 < \epsilon < 1$
d	回路の深さ	$poly(\lambda)$, $(2n^2)^{2d+4} \leq 2^{n^\epsilon}$
s	ABE の標準偏差	$\max\{O(\sqrt{n \log q \log n}), O(\lambda, (2\tilde{m})^{d+3})\}$
B	χ の無限ノルム上限	$q/B > 2^{n^\epsilon}$
$\tilde{B}$	$\tilde{\chi}$ の無限ノルム上限	$O((\tilde{m}+\tilde{m}')\lambda B(2m)^d, \lambda)$
ι	ek_Y の長さ	$poly(\lambda)$

$\mathsf{SKGen}(1^\lambda)$

$(\boldsymbol{A}, \boldsymbol{T}_{\boldsymbol{A}}) \leftarrow\!\$\ \mathsf{TrapGen}(1^n, 1^m, q)$
for $t \in [1, \ell]$: $\boldsymbol{A}_t \leftarrow\!\$\ \mathbb{Z}_q^{n \times m}$
$\boldsymbol{u} \leftarrow\!\$\ \mathbb{Z}_q^n$; $\boldsymbol{D} \leftarrow\!\$\ \mathbb{Z}_q^{n \times m}$
$\boldsymbol{D}_0, \boldsymbol{D}_1 \leftarrow\!\$\ \mathbb{Z}_q^{2n \times 2m}$
$\mathsf{pk} \leftarrow (\boldsymbol{A}, \{\boldsymbol{A}_t\}_{t \in [1,\ell]}, \boldsymbol{D}, \boldsymbol{D}_0, \boldsymbol{D}_1, \boldsymbol{u})$
$\mathsf{sk} \leftarrow \boldsymbol{T}_{\boldsymbol{A}}$
return $(\mathsf{pk}, \mathsf{sk})$

$\mathsf{Sign}(\mathsf{sk}, \mu)$

$\tau = (\tau[1], \tau[2], \ldots, \tau[\ell]) \leftarrow\!\$\ \{0,1\}^\ell$
$\boldsymbol{A}_\tau \leftarrow [\ \boldsymbol{A}\ \middle|\ \boldsymbol{A}_0 + \sum_{t=1}^{\ell} \tau[t]\boldsymbol{A}_t\ ]$
$\boldsymbol{T}_\tau \leftarrow\!\$\ \mathsf{ExtBasis}(\boldsymbol{A}_\tau, \boldsymbol{T}_{\boldsymbol{A}})$
$\boldsymbol{s} \leftarrow\!\$\ D_{\mathbb{Z}^{2m}, \sigma_1}$; $\boldsymbol{c} \leftarrow \boldsymbol{D}_0\boldsymbol{s} + \boldsymbol{D}_1\mu$
$\boldsymbol{\gamma} \leftarrow \mathsf{bin}(\boldsymbol{c})$; $\boldsymbol{u}_\mu \leftarrow \boldsymbol{u} + \boldsymbol{D} \cdot \boldsymbol{\gamma}$
$\boldsymbol{d} \leftarrow\!\$\ \mathsf{SamplePre}(\boldsymbol{A}_\tau, \boldsymbol{T}_\tau, \boldsymbol{u}_\mu, \sigma)$
return $\boldsymbol{\Sigma} \leftarrow (\tau, \boldsymbol{d}, \boldsymbol{s})$

$\mathsf{Vf}(\mathsf{pk}, \mu, \boldsymbol{\Sigma})$

$\boldsymbol{u}_\mu \leftarrow \boldsymbol{u} + \boldsymbol{D} \cdot \mathsf{bin}(\boldsymbol{D}_0\boldsymbol{s} + \boldsymbol{D}_1\mu)$
return 1 **if** $\|\boldsymbol{d}\| < \sigma\sqrt{2m} \wedge \|\boldsymbol{s}\| < \sigma_1\sqrt{2m} \wedge \boldsymbol{A}_\tau \boldsymbol{d} = \boldsymbol{u}_\mu \bmod q$

図 3 サブアルゴリズム DS
Fig. 3 Subalgorithm DS

4.2 サブアルゴリズム: NIZK

4.2.1 二項関係

$T_\pi : \{-1,0,1\}^L \to \{-1,0,1\}^L$ を $\pi \in \mathcal{S}$ でパラメタライズされた置換とし，NIZK の証拠集合 $\mathsf{W} \subseteq \{-1,0,1\}^L$ を

- 任意の $\pi \in \mathcal{S}$ について $\boldsymbol{x} \in \mathsf{W} \Leftrightarrow T_\pi(\boldsymbol{x}) \in \mathsf{W}$,
- $\boldsymbol{x} \in \mathsf{W} \wedge \pi \leftarrow\!\$\ \mathcal{S}$ ならば $T_\pi(\boldsymbol{x})$ は W 上に一様分布する,

を満たすものとする．また，一方向性関係を次で与える．

$$R_{\mathsf{NIZK}} = \left\{((\boldsymbol{P}, \boldsymbol{v}), \boldsymbol{x}) \in \mathbb{Z}_q^{D \times L} \times \mathbb{Z}_q^D \times \mathsf{W} : \boldsymbol{P}\boldsymbol{x} = \boldsymbol{v} \bmod q\right\}.$$

4.2.2 プロトコル

サブアルゴリズム $\mathsf{NIZK} = (P, V)$ を図 4 に示す．ここで COM は [22] のコミットメント，$H : \{0,1\}^* \to \{1,2,3\}$ はハッシュ関数，κ は反復回数である．

$P((\boldsymbol{P}, \boldsymbol{v}), \boldsymbol{x}, \mathrm{str})$

for $j \in [1, \kappa]$:
$\boldsymbol{r}_j \leftarrow\!\$\ \mathbb{Z}_q^L$; $\boldsymbol{y}_j \leftarrow \boldsymbol{x} + \boldsymbol{r}_j$; $\pi_j \leftarrow\!\$\ \mathcal{S}$; $\rho_{j,1}, \rho_{j,2}, \rho_{j,3} \leftarrow\!\$\ \{0,1\}^\eta$

$$\mathsf{cmt}_j = \begin{bmatrix} C_{j,1} \\ C_{j,2} \\ C_{j,3} \end{bmatrix} \leftarrow \begin{bmatrix} \mathsf{COM}(\pi_j, \boldsymbol{P}\boldsymbol{r}_j; \rho_{j,1}) \\ \mathsf{COM}(T_{\pi_j}(\boldsymbol{r}_j); \rho_{j,2}) \\ \mathsf{COM}(T_{\pi_j}(\boldsymbol{y}_j); \rho_{j,3}) \end{bmatrix}$$

$\{\mathsf{cha}_j\}_{j \in [1,\kappa]} \leftarrow H(\{\mathsf{cmt}_j\}_{j \in [1,\kappa]}, (\boldsymbol{P}, \boldsymbol{v}), \mathrm{str})$

for $j \in [1, \kappa]$:

$$\mathsf{res}_j = (R_j, R'_j, \rho_j, \rho'_j) \leftarrow \begin{cases} (T_{\pi_j}(\boldsymbol{x}), T_{\pi_j}(\boldsymbol{r}_j), \rho_{j,2}, \rho_{j,3}) & \mathsf{cha}_j = 1 \\ (\pi_j, \boldsymbol{y}_j, \rho_{j,1}, \rho_{j,3}) & \mathsf{cha}_j = 2 \\ (\pi_j, \boldsymbol{r}_j, \rho_{j,1}, \rho_{j,2}) & \mathsf{cha}_j = 3 \end{cases}$$

return $\pi = \{(\mathsf{cmt}_j, \mathsf{res}_j)\}_{j \in [1,\kappa]}$

$V((\boldsymbol{P}, \boldsymbol{v}), \{(\mathsf{cmt}_j, \mathsf{res}_j)\}_{j \in [1,\kappa]}, \mathrm{str})$

$\left\{((C_{j,1}, C_{j,2}, C_{j,3}), (r_j, r'_j, \rho_j, \rho'_j))\right\} \leftarrow \{(\mathsf{cmt}_j, \mathsf{res}_j)\}_{j \in [1,\kappa]}$

for $j \in [1, \kappa]$:
return 0 **if**

$$\begin{cases} r_j \notin \mathsf{W} \vee C_{j,2} \neq \mathsf{COM}(r'_j; \rho_j) \vee C_{j,3} \neq \mathsf{COM}(r_j + r'_j; \rho'_j) & \mathsf{cha}_j = 1 \\ C_{j,1} \neq \mathsf{COM}(T_{r_j}, \boldsymbol{P}r'_j - \boldsymbol{v}; \rho_j) \wedge C_{j,3} \neq \mathsf{COM}(T_{r_j}(r'_j); \rho'_j) & \mathsf{cha}_j = 2 \\ C_{j,1} \neq \mathsf{COM}(T_{r_j}, \boldsymbol{P}r'_j; \rho_j) \wedge C_{j,2} \neq \mathsf{COM}(T_{r_j}(r'_j); \rho'_j) & \mathsf{cha}_j = 3 \end{cases}$$

return 1

図 4 サブアルゴリズム NIZK
Fig. 4 Subalgorithm NIZK

4.2.3 インスタンスと証拠の表現

[16] に従い，以下の 3 つのタイプの文字列について，W に属する $\boldsymbol{x}$ への変換が可能である．

(1) $\boldsymbol{x} \in \{0,1\}^m$,
(2) $\boldsymbol{x} \in [-B, B]^m$,
(3) $\begin{bmatrix} \boldsymbol{d} \cdot \boldsymbol{b}[1] \\ \vdots \\ \boldsymbol{d} \cdot \boldsymbol{b}[n] \end{bmatrix} \in [-\beta, \beta]^{mn}$ for $(\boldsymbol{d}, \boldsymbol{b}) \in [-\beta, \beta]^m \times \{0,1\}^n$.

4.3 サブアルゴリズム: ABE

$t \leq \xi$ とする．任意の属性 X について，ξ ビットの文字列で表されるとする．また，アクセスポリシー Y は t-CNF とする．

4.3.1 適合制約付き擬似ランダム関数

適合制約付き擬似ランダム関数 (conforming constrained Pseudo-Random Function, ccPRF) [15] を導入する．ccPRF ccPRF は以下のアルゴリズムから構成される，

- $\mathsf{Pgen}(1^\lambda)$: PPT パラメータ生成アルゴリズム Pgen は，セキュリティパラメータ 1^λ を入力とし，パブリックパラメータ pp，マスター評価鍵 $\mathsf{mek} \in \{0,1\}^\lambda$ を出力する．
- $\mathsf{Eval}(\mathsf{pp}, \mathsf{mek}, X)$: DPT 評価アルゴリズム Eval は，パブリックパラメータ pp，マスター評価鍵 mek，文字列 $X \in \{0,1\}^\xi$ を入力とし，$\rho_X \in \{0,1\}^\lambda$ を出力する．

- Constrain$(\mathsf{pp}, \mathsf{mek}, Y)$: DPT 制約鍵生成アルゴリズム Constrain は，パブリックパラメータ pp，マスター評価鍵 mek，ブール関数 Y を入力とし，制約鍵 $\mathsf{ek}_Y \in \{0,1\}^\iota$ を出力する．
- CEval$(\mathsf{pp}, \mathsf{ek}_Y, X)$: DPT 評価アルゴリズム CEval は，パブリックパラメータ pp，制約鍵 ek_Y，文字列 $X \in \{0,1\}^\xi$ を入力とし，$\rho'_X \in \{0,1\}^\lambda$ または $\perp$ を出力する．
- KeySim(pp, Y): PPT 擬似鍵生成アルゴリズム KeySim は，パブリックパラメータ pp，ブール関数 Y を入力とし，擬似鍵 $\mathsf{ek}_Y \in \{0,1\}^\iota$ を出力する．

ccPRF の正当性は次の通りである: 任意の $X \in \{0,1\}^\xi$ と $Y : \{0,1\}^\xi \to \{0,1\}$, $(\mathsf{pp}, \mathsf{mek}) \leftarrow\!\$\ \mathsf{Pgen}(1^\lambda)$, $\mathsf{ek}_Y \leftarrow \mathsf{Constrain}(\mathsf{pp}, \mathsf{mek}, Y)$ に対し，

$$\mathsf{CEval}(\mathsf{pp}, \mathsf{ek}_Y, X) = \begin{cases} \mathsf{Eval}(\mathsf{pp}, \mathsf{mek}, X) & Y(X) = 1, \\ \perp & Y(X) = 0. \end{cases}$$

が成り立つ．また，ccPRF の擬似ランダム性については通常の PRF と同様に考える．

ccPRF は漸次評価可能，すなわち，任意の $(\mathsf{pp}, \mathsf{mek}) \leftarrow\!\$\ \mathsf{Pgen}(1^\lambda)$, $X \in \{0,1\}^\xi$, $Y : \{0,1\}^\xi \to \{0,1\}$ について以下を満たす回路 $U_{\eta\to X}, U_{\eta\to Y}, U_{Y\to X}$ が存在する:

$$U_{\eta\to X}(\mathsf{mek}) = \mathsf{Eval}(\mathsf{pp}, \mathsf{mek}, X),$$
$$U_{\eta\to Y}(\mathsf{mek}) = \mathsf{Constrain}(\mathsf{pp}, \mathsf{mek}, Y),$$
$$U_{Y\to X}(\mathsf{ek}_Y) = \mathsf{CEval}(\mathsf{pp}, \mathsf{ek}_Y, X).$$

$U_{\eta\to X}$ は $U_{Y\to X}$ と $U_{\eta\to Y}$ の連結で表現可能である．また，ccPRF の鍵模倣性は，同一のアクセスポリシー Y に対する Constrain で生成された制限鍵と KeySim による擬似鍵が，識別不可能であることをいう．ただし，Y を満たす属性に対する ccPRF の評価値を知らない状況を前提とする．最後に，次の補題を導入する．

Lemma 1 ([15])**.** 属性 $X \in \{0,1\}^\xi$, アクセスポリシー Y, $(\mathsf{mek}, \mathsf{pp}) \leftarrow\!\$\ \mathsf{Pgen}(1^\lambda)$, 擬似鍵 $\mathsf{ek}_Y \leftarrow\!\$\ \mathsf{KeySim}(\mathsf{pp}, Y)$ について，$Y(X) = 1$ のとき，無視できる確率を除いて $\mathsf{CEval}(\mathsf{pp}, \mathsf{ek}_Y, X)$ が $\perp$ でも $\mathsf{Eval}(\mathsf{pp}, \mathsf{mek}, X)$ でもない．

4.3.2 評価回路の変換

評価回路を格子で表現する [15]. $m = n\lceil \log q \rceil$, $f : \{0,1\}^{\mathsf{in}} \to \{0,1\}^{\mathsf{out}}$ とし，$g : \{0,1\}^{\mathsf{out}} \to \{0,1\}^{\mathsf{out}'}$ を深さ d のブール回路，$x \in \{0,1\}^{\mathsf{in}}$, $\boldsymbol{C} \in \mathbb{Z}_q^{n\times m\cdot\mathsf{in}}$ とする．

入力 $(f, \boldsymbol{C})$ について，DPT アルゴリズム EvalF は $\boldsymbol{H} \in \mathbb{Z}_q^{m\cdot\mathsf{in}\times m\cdot\mathsf{out}}$ を出力する．また，入力 $(f, x, \boldsymbol{C})$ について，DPT アルゴリズム EvalFx は $\hat{\boldsymbol{H}} \in \mathbb{Z}_q^{m\cdot\mathsf{in}\times m\cdot\mathsf{out}}$ を出力する．$\boldsymbol{H}$ と $\hat{\boldsymbol{H}}$ は次を満たす: $\|\boldsymbol{H}\|, \left\|\hat{\boldsymbol{H}}\right\| \le (2m)^d$, $\left[\boldsymbol{C} - x \otimes \boldsymbol{G}\right] \hat{\boldsymbol{H}} = \boldsymbol{C}\boldsymbol{H} - f(x) \otimes \boldsymbol{G} \bmod q$. ただし，$\boldsymbol{G} = \begin{bmatrix} 1 & 2 & 4 & \cdots & 2^{\lceil \log q \rceil - 1} \end{bmatrix} \otimes \boldsymbol{I}_n \in \mathbb{Z}_q^{n\times m}$. $\boldsymbol{H}_f \leftarrow \mathsf{EvalF}(f, \boldsymbol{C})$, $\boldsymbol{H}_g \leftarrow \mathsf{EvalF}(g, \boldsymbol{C}\boldsymbol{H}_f)$, $\boldsymbol{H}_{g\circ f} \leftarrow \mathsf{EvalF}(g \circ f, \boldsymbol{C})$ について，$\boldsymbol{H}_f\boldsymbol{H}_g = \boldsymbol{H}_{g\circ f}$ が成り立つ．

APgen$(1^n, 1^{\bar{m}}, q, \mathbb{U})$

$(\eta, \mathsf{pp}) \leftarrow\!\$\ \mathsf{CPgen}(1^\lambda)$
$(\boldsymbol{B}, \boldsymbol{T_B}) \leftarrow\!\$\ \mathsf{TrapGen}(1^n, 1^{\bar{m}'}, q)$
$\boldsymbol{C} \leftarrow\!\$\ \mathbb{Z}_q^{n\times\bar{m}\cdot\lambda}; \boldsymbol{U} \leftarrow\!\$\ \mathbb{Z}_q^{n\times l}$
$msk \leftarrow (\boldsymbol{T_B}, \eta)$
$\mathsf{pk} \leftarrow (\boldsymbol{B}, \boldsymbol{C}, \boldsymbol{U}, \mathsf{pp})$
return (msk, pk)

AKGen(msk, X)

$\boldsymbol{H}_{\eta\to X} \leftarrow \mathsf{EvalF}(U_{\eta\to X}, \boldsymbol{C})$
$\boldsymbol{C}_X \leftarrow \boldsymbol{C}\boldsymbol{H}_{\eta\to X}$
$\rho \leftarrow \mathsf{Eval}(\mathsf{pp}, \eta, X)$
Create a circuit I_ρ :
$\{0,1\}^\lambda \to \{0,1\}$ **s.t.**
  $I_\rho(\rho') \mapsto 1$ **if and only if** $\rho = \rho'$
$\boldsymbol{H}_\rho \leftarrow \mathsf{EvalF}(I_\rho, \boldsymbol{C}_X)$
$\boldsymbol{C}_{X,\rho} \leftarrow \boldsymbol{C}_X\boldsymbol{H}_\rho$
$\overline{\boldsymbol{B}} \leftarrow \left[\boldsymbol{B} \mid \boldsymbol{C}_{X,\rho}\right]$
$\boldsymbol{T}_{\overline{\boldsymbol{B}}} \leftarrow\!\$\ \mathsf{ExtBasis}(\overline{\boldsymbol{B}}, \boldsymbol{T_B})$
$\boldsymbol{K} \leftarrow\!\$\ \mathsf{SamplePre}(\overline{\boldsymbol{B}}, \boldsymbol{T}_{\overline{\boldsymbol{B}}}, \boldsymbol{U}, s)$
return $\mathsf{sk}_X \leftarrow (X, \rho, \boldsymbol{K})$

$dec(\boldsymbol{u} = (\boldsymbol{u}[1], \ldots, \boldsymbol{u}[l]))$

for $k \in [1, l]$:
$$\mu[k] \leftarrow \begin{cases} 1 & |\boldsymbol{u}[k]| \le q/4 \\ 0 & |\boldsymbol{u}[k]| > q/4 \end{cases}$$
return μ

Enc$(\mathsf{pk}, Y, \mu \in \{0,1\}^l)$

$s_Y \leftarrow\!\$\ \mathsf{KeySim}(\mathsf{pp}, Y)$
$\boldsymbol{t} \leftarrow\!\$\ \chi^n$; $\boldsymbol{e}_0 \leftarrow\!\$\ \chi^{\bar{m}'}$
$\boldsymbol{e}_1 \leftarrow\!\$\ \tilde{\chi}^{\bar{m}\cdot\iota}$; $\boldsymbol{e}_2 \leftarrow\!\$\ \chi^l$
$\boldsymbol{H}_{\eta\to Y} \leftarrow \mathsf{EvalF}(U_{\eta\to Y}, \boldsymbol{C})$
$\boldsymbol{C}_Y \leftarrow \boldsymbol{C}\boldsymbol{H}_{\eta\to Y}$
$\boldsymbol{u}_0 \leftarrow \boldsymbol{B}^T\boldsymbol{t} + \boldsymbol{e}_0$
$\boldsymbol{u}_1 \leftarrow \left[\boldsymbol{C}_Y - s_Y \otimes \boldsymbol{G}\right]^T\boldsymbol{t} + \boldsymbol{e}_1$
$\boldsymbol{u}_2 \leftarrow \boldsymbol{U}^T\boldsymbol{t} + \boldsymbol{e}_2 + \mu \cdot \lceil q/2 \rfloor$
$\mathsf{cp} \leftarrow (s_Y, \boldsymbol{u}_0, \boldsymbol{u}_1, \boldsymbol{u}_2)$
return (Y, cp)

Dec$(\mathsf{sk}_X, (Y, \mathsf{cp}))$

$\rho' \leftarrow U_{Y\to X}(s_Y)$
return $\perp$ **if if** $Y(X) \ne 1 \vee \rho = \rho'$
$\boldsymbol{H}_{\eta\to Y} \leftarrow \mathsf{EvalF}(U_{\eta\to Y}, \boldsymbol{C})$
$\boldsymbol{H}_{\eta\to X} \leftarrow \mathsf{EvalF}(U_{\eta\to X}, \boldsymbol{C})$
$\boldsymbol{C}_Y \leftarrow \boldsymbol{C}\boldsymbol{H}_{\eta\to Y}$; $\boldsymbol{C}_X \leftarrow \boldsymbol{C}\boldsymbol{H}_{\eta\to X}$
$\hat{\boldsymbol{H}}_{s_Y\to\rho'} \leftarrow \mathsf{EvalFx}(U_{Y\to X}, s_Y, \boldsymbol{C}_Y)$
$\hat{\boldsymbol{H}}_{\rho,\rho'} \leftarrow \mathsf{EvalFx}(I_\rho, \rho', \boldsymbol{C}_X)$
$\hat{\boldsymbol{H}}_{s_Y\to\ne\rho'} \leftarrow \hat{\boldsymbol{H}}_{s_Y\to\rho'}\hat{\boldsymbol{H}}_{\rho,\rho'}$
$\overline{\boldsymbol{u}}_1 \leftarrow \hat{\boldsymbol{H}}^T_{s_Y\to\ne\rho'}\boldsymbol{u}_1$
return $dec(\boldsymbol{u}_2 - \boldsymbol{K}^T\begin{bmatrix}\boldsymbol{u}_0 \\ \hline \overline{\boldsymbol{u}}_1\end{bmatrix})$

図 5 サブアルゴリズム ABE
Fig. 5 Subalgorithm ABE

4.3.3 サブアルゴリズム ABE の構成

ABE $= (\mathsf{APgen}, \mathsf{AKGen}, \mathsf{Enc}, \mathsf{Dec})$，および補助アルゴリズム dec を図 5 に示す．

4.4 提案方式

提案する格子ベース GSdT では次のように署名を生成する．グループ参加プロトコルにて作成された署名者の ID ベクトル $\boldsymbol{\zeta}_i$ をサブアルゴリズム ABE で暗号化する．そして，署名者がグループに所属していることと暗号文 $(Y, \mathsf{cp}_{\boldsymbol{\zeta}_i})$ が $\boldsymbol{\zeta}_i$ の正当な暗号化であることの証明 π_E をサブアルゴリズム NIZK で作成し，$\Sigma = (Y, \mathsf{cp}_{\boldsymbol{\zeta}_i}, \pi_E)$ を最終的な署名とする．提案方式の各アルゴリズムを図 6 に示す．GSig および Open にて使用される証拠は 4.2.3 節で示した形を取るものとする．

4.5 提案方式の安全性

提案方式が各安全性を満たすことを示す．証明の詳細は full paper にて記述する．

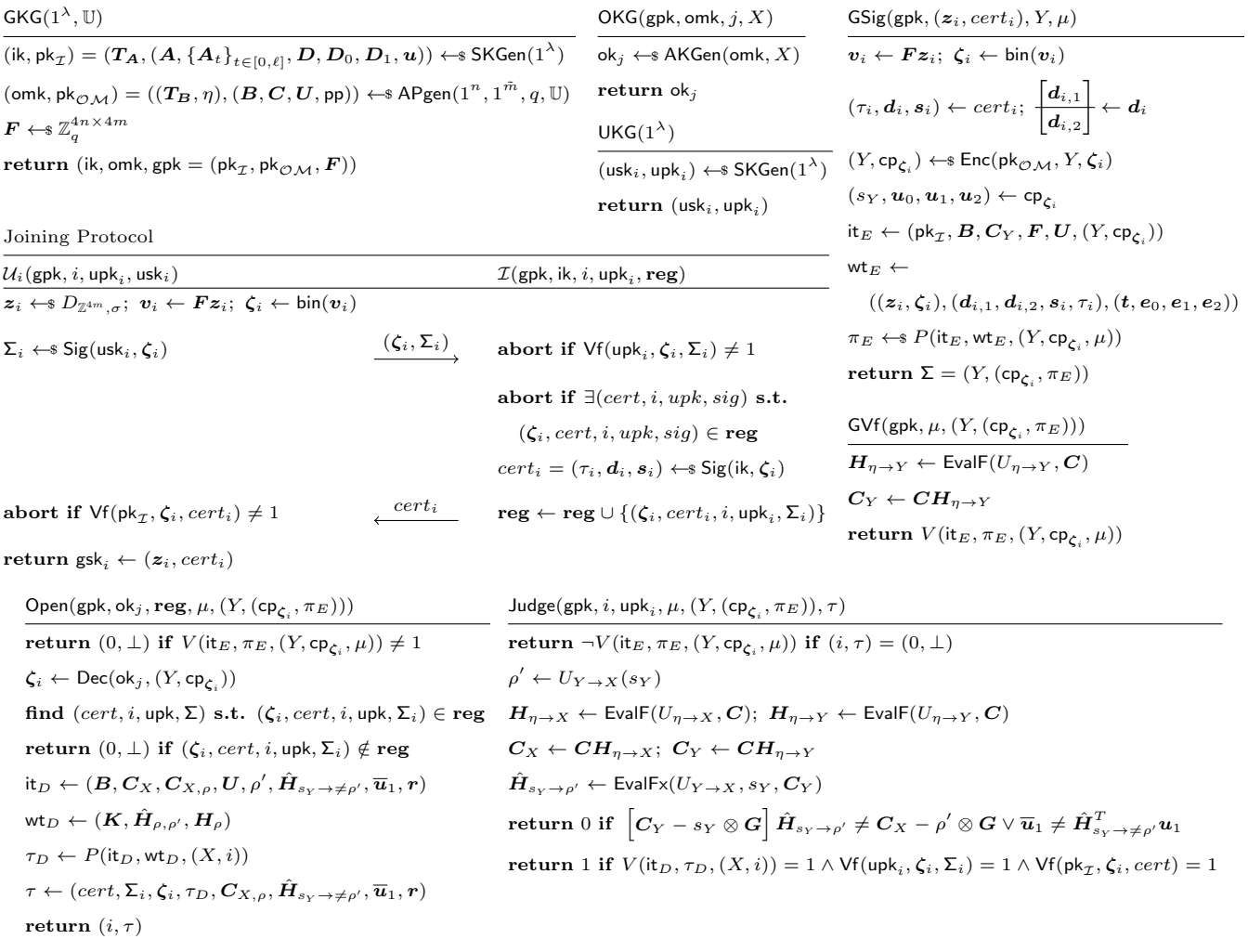

図 6 提案方式
Fig. 6 Proposed GSdT

Theorem 1 (正当性)．提案方式は正当である．
Theorem 2 (匿名性)．$\mathsf{LWE}_{n,q,\chi}$ 仮定の下で，提案方式はランダムオラクルモデルにおいて匿名性を持つ．
Theorem 3 (追跡可能性)．$\mathsf{SIS}_{n,m,q,\beta}$ 仮定の下で，提案方式は追跡可能である．
Theorem 4 (陥罪不可能性)．$\mathsf{SIS}_{4n,4m,q,4\sigma\sqrt{m}}$ 仮定の下で，提案方式はランダムオラクルモデルにおいて陥罪不可能である．

5. 比較

提案方式の効率を [8] の一般的構成において同じプリミティブを使用した場合の構成と比較する．結果を表 2 に示す．なお，スペースの都合によりサイズ効率のみを比較する．提案方式では，gpk, ok, gsk, Σ のサイズが一般的構成よりも大幅に小さくなっている．これは暗号化された ID $\boldsymbol{\zeta}$ のサイズ (表 2 中の id) が圧倒的に減少したためである．これは提案方式の ID が $\mathbb{Z}_q$ 上の $4n$ 次元のベクトル $\boldsymbol{v}$ を文字化したものであるのに対し，一般的構成では DS の公開鍵やその署名を暗号化したものになるからである．この ID サイズの減少により，計算コスト面においても改善が可能である．

謝辞 本研究は JSPS 科研費 JP23K11105, JP23K11106, JP22K12023 の助成を受けたものです．

参考文献

[1] D. Chaum and E. Van Heyst, "Group signatures," in *Proceedings of the 10th Annual International Conference on Theory and Application of Cryptographic Techniques*, ser. EUROCRYPT'91. Berlin, Heidelberg: Springer-Verlag, 1991, p. 257–265.
[2] Y. Sakai, K. Emura, G. Hanaoka, Y. Kawai, T. Matsuda, and K. Omote, "Group signatures with message-dependent opening," in *Pairing-Based Cryptography – Pairing 2012*, M. Abdalla and T. Lange, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 270–294.
[3] S. Ling, K. Nguyen, H. Wang, and Y. Xu, "Accountable tracing signatures from lattices," in *Topics in Cryptology - CT-RSA 2019 - The Cryptographers' Track at the RSA Conference 2019, San Francisco, CA, USA, March 4-8, 2019, Proceedings*, ser. Lecture Notes in Computer Science, M. Matsui, Ed., vol. 11405. Springer,

表 2　サイズ効率の比較

Table 2　Comparisions of size efficiency

[ours]		[8]
$(\mathcal{O}(m^2\lvert\sqrt{m}\rvert), \mathcal{O}(m^2\lvert m\rvert))$	$(\lvert\mathsf{ik}\rvert, \lvert\mathsf{omk}\rvert)$	$(\mathcal{O}(m^2\lvert\sqrt{m}\rvert), \mathcal{O}(m^2\lvert m\rvert))$
$\mathcal{O}(m^2\lvert N\rvert)$	$\lvert\mathsf{gpk}\rvert$	$\mathcal{O}((m^2\lvert N\rvert + m\lvert\mu\rvert)(m\lvert\sigma'\rvert + \lvert m^2\lvert N\rvert + m\lvert\mu\rvert\rvert))$
$\xi + \mathcal{O}(m^2\lvert\tilde{\sigma}\rvert)$	$\lvert\mathsf{ok}\rvert$	$\xi + \mathcal{O}(m\lvert\tilde{\sigma}\rvert(m^2\lvert N\rvert + m\lvert\mu\rvert)(\lvert\sigma'\rvert + \lvert m^2\lvert N\rvert + m\lvert\mu\rvert\rvert))$
$(\mathcal{O}(m^2\lvert\sqrt{m}\rvert), \mathcal{O}(m^2\lvert N\rvert))$	$(\lvert\mathsf{usk}\rvert, \lvert\mathsf{upk}\rvert)$	$(\mathcal{O}(m^2\lvert\sqrt{m}\rvert), \mathcal{O}(m^3\lvert N\rvert + m^2\lvert\mu\rvert))$
$\lvert N\rvert + \mathcal{O}(m\lvert\sigma'\rvert)$	$\lvert\mathsf{gsk}\rvert$	$\mathcal{O}((m^2\lvert N\rvert + m\lvert\mu\rvert)(\lvert\sigma'\rvert + \lvert m^2\lvert N\rvert + m\lvert\mu\rvert\rvert))$
$\lvert Y\rvert + \mathcal{O}(\kappa(\eta + m\iota\lvert B'\rvert + \lvert N\rvert + m\lvert\sigma'\rvert + \lvert\beta\rvert))$	$\lvert\mathbf{\Sigma}\rvert$	$\lvert Y\rvert + \mathcal{O}(\kappa(\eta + m\iota\lvert B'\rvert + \lvert B\rvert(m^2\lvert N\rvert + m\lvert\mu\rvert)(\lvert\sigma'\rvert + \lvert m^2\lvert N\rvert + m\lvert\mu\rvert\rvert)))$
$\mathcal{O}(\lvert N\rvert + m\lvert\sigma'\rvert + m^3\iota\lvert q\rvert + \kappa(\eta + nm\lvert\tilde{\sigma}\rvert + m^2\iota d\lvert m\rvert))$	$\lvert\tau\rvert$	$\mathcal{O}(\kappa(\xi + m\lvert\tilde{\sigma}\rvert(m^2\lvert N\rvert + m\lvert\mu\rvert)(\lvert\sigma'\rvert + \lvert m^2\lvert N\rvert + m\lvert\mu\rvert\rvert)))$
$2m$	$\lvert\mathsf{id}\rvert$	$\mathcal{O}((m^2\lvert N\rvert + m\lvert\mu\rvert)(\lvert\sigma'\rvert + \lvert m^2\lvert N\rvert + m\lvert\mu\rvert\rvert))$
$\lvert N\rvert + \mathcal{O}(m(\lvert\sigma'\rvert + \iota\lvert B'\rvert) + \lvert\beta\rvert)$	$\lvert\mathsf{wt}_E\rvert$	$\mathcal{O}(\lvert B\rvert(m^2\lvert N\rvert + m\lvert\mu\rvert)(\lvert\sigma'\rvert + \lvert m^2\lvert N\rvert + m\lvert\mu\rvert\rvert) + m\iota\lvert B'\rvert)$
$\mathcal{O}(nm\lvert\tilde{\sigma}\rvert + m^2\iota d\lvert m\rvert)$	$\lvert\mathsf{wt}_D\rvert$	$\xi + \mathcal{O}(m\lvert\tilde{\sigma}\rvert(m^2\lvert N\rvert + m\lvert\mu\rvert)(\lvert\sigma'\rvert + \lvert m^2\lvert N\rvert + m\lvert\mu\rvert\rvert))$

2019, pp. 556–576.

[4] M. Kohlweiss and I. Miers, "Accountable metadata-hiding escrow: A group signature case study," *Proc. Priv. Enhancing Technol.*, vol. 2015, no. 2, pp. 206–221, 2015.

[5] B. Libert, K. Nguyen, T. Peters, and M. Yung, "Bifurcated signatures: Folding the accountability vs. anonymity dilemma into a single private signing scheme," in *Advances in Cryptology - EUROCRYPT 2021 - 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, October 17-21, 2021, Proceedings, Part III*, ser. Lecture Notes in Computer Science, A. Canteaut and F. Standaert, Eds., vol. 12698. Springer, 2021, pp. 521–552.

[6] S. Xu and M. Yung, "Accountable ring signatures: A smart card approach," in *Smart Card Research and Advanced Applications VI, IFIP 18th World Computer Congress, TC8/WG8.8 & TC11/WG11.2 Sixth International Conference on Smart Card Research and Advanced Applications (CARDIS), 22-27 August 2004, Toulouse, France*, ser. IFIP, J. Quisquater, P. Paradinas, Y. Deswarte, and A. A. E. Kalam, Eds., vol. 153. Kluwer/Springer, 2004, pp. 271–286.

[7] H. Anada, M. Fukumitsu, and S. Hasegawa, "Group signatures with designated traceability," in *The 9th International Symposium on Computing and Networking (CANDAR2021)*, November 2021, pp. 74–80.

[8] ——, "Group signatures with designated traceability over openers' attributes," *International Journal of Networking and Computing*, vol. 12, no. 2, pp. 493–508, July 2022.

[9] ——, "Group signatures with designated traceability over openers' attributes in bilinear groups," in *The 23rd World Conference on Information Security Applications (WISA 2022)*, I. You and T.-Y. Youn, Eds. Cham: Springer Nature Switzerland, August 2022, pp. 29–43.

[10] ——, "Group signatures with designated traceability over openers' attributes from symmetric-key primitives," in *21st Annual International Conference on Privacy, Security, and Trust (PST2024)*, August 2024, pp. 1–9.

[11] M. Bellare, H. Shi, and C. Zhang, "Foundations of group signatures: The case of dynamic groups," in *Topics in Cryptology – CT-RSA 2005*, A. Menezes, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 136–153.

[12] J. Bootle, A. Cerulli, P. Chaidos, E. Ghadafi, J. Groth, and C. Petit, "Short accountable ring signatures based on ddh," in *Computer Security – ESORICS 2015*, G. Pernul, P. Y A Ryan, and E. Weippl, Eds. Cham: Springer International Publishing, 2015, pp. 243–265.

[13] A. Langlois, S. Ling, K. Nguyen, and H. Wang, "Lattice-based group signature scheme with verifier-local revocation," in *Public-Key Cryptography – PKC 2014*, H. Krawczyk, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 345–361.

[14] W. Beullens, S. Dobson, S. Katsumata, Y.-F. Lai, and F. Pintore, "Group signatures and more from isogenies and lattices: Generic, simple, and efficient," in *Advances in Cryptology – EUROCRYPT 2022*, O. Dunkelman and S. Dziembowski, Eds. Cham: Springer International Publishing, 2022, pp. 95–126.

[15] R. Tsabary, "Fully secure attribute-based encryption for t-cnf from lwe," in *Advances in Cryptology – CRYPTO 2019*, A. Boldyreva and D. Micciancio, Eds. Cham: Springer International Publishing, 2019, pp. 62–85.

[16] B. Libert, S. Ling, F. Mouhartem, K. Nguyen, and H. Wang, "Signature schemes with efficient protocols and dynamic group signatures from lattice assumptions," in *Advances in Cryptology – ASIACRYPT 2016*, J. H. Cheon and T. Takagi, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2016, pp. 373–403.

[17] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," vol. 56, no. 6, 2009.

[18] W. Banaszczyk, "New bounds in some transference theorems in the geometry of numbers," *Mathematische Annalen*, vol. 296, no. 1, pp. 625–635, 1993.

[19] J. Alwen and C. Peikert, "Generating shorter bases for hard random lattices," *Theory of Computing Systems*, vol. 48, no. 3, pp. 535–553, 2011.

[20] D. Cash, D. Hofheinz, E. Kiltz, and C. Peikert, "Bonsai trees, or how to delegate a lattice basis," in *Advances in Cryptology – EUROCRYPT 2010*, H. Gilbert, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 523–552.

[21] C. Gentry, C. Peikert, and V. Vaikuntanathan, "Trapdoors for hard lattices and new cryptographic constructions." New York, NY, USA: Association for Computing Machinery, 2008.

[22] A. Kawachi, K. Tanaka, and K. Xagawa, "Concurrently secure identification schemes based on the worst-case hardness of lattice problems," in *Advances in Cryptology - ASIACRYPT 2008*, J. Pieprzyk, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, pp. 372–389.