CL-003

鍵集約型 ID ベースプロキシ再暗号化方式と個人データ管理システム

Key Aggregate Identity-based Proxy Re-Encryption Scheme and Data Management Provision System

梶田 海成† 大竹 剛†
Kaisei Kajita Go Ohtake

1. 導入

1.1 背景

近年，パーソナルデータストア（PDS）やデータ取引市場といった個人情報の管理・提供をユーザ自らの意思に基づいて行うシステムが注目されている．PDS では，スマートフォンの位置情報や，オンラインショッピングでの購入履歴などの個人情報をユーザ自身が管理し，サービス事業者等の第三者に，ユーザが自らの意思でデータを提供することで，ユーザはその提供したデータに基づいてサービスを横断的に享受することが可能になる．

ユーザが自身のデータを管理するとき，利便性の観点から，クラウドを利用することが多い．クラウド上で位置情報や購入履歴といったセンシティブなデータを管理するとき，プライバシー保護の観点から，データを暗号化してクラウドに保存する必要がある．しかし，現状では適切な暗号化を用いた PDS システムは実用化されていない．例えば，現在 W3C で議論が進められている Solid [1], [2] では，安全性の面では通信路の保護とアクセス制御のみを扱い，PDS に保存されているデータ自体の暗号化は考慮されていない．また，別の PDS 方式である Personal Life Repository (PLR) [3] では，個人主導の Digital Rights Management (DRM)を用いた暗号化とアクセス制御を採用しているが，DRM は主に著作権保護に用いられる暗号技術であり，ライセンスサーバの導入コストや後述する秘密鍵管理のコストなどがかかる．

PDS を実現する上で，適切な暗号技術を用いることでシステムの安全性や利便性を高めることができるが，以下の理由により，公開鍵暗号（PKE）や共通鍵暗号（SKE）のような一般に広く用いられる暗号プリミティブは PDS に適さない．まず AES などの SKE では，データ所有者であるユーザとデータ提供先であるサービス事業者が共通の鍵を用いるため，全ての事業者とユーザが同じ鍵を共有しなければならない．したがって，ユーザが複数のサービス事業者にデータを提供するとき，もしある事業者の持つ鍵が漏洩すると，クラウド上にあるデータも含めてユーザの全てのデータ漏洩する恐れがある．従って，データ所有者であるユーザはデータ提供先毎に異なる鍵を保持する必要があるため鍵管理コストが高くなり，さらにサービス事業者毎の暗号化データを生成する必要があるためストレージコストが高くなる，といった課題が生じてしまう．一方 RSA などの PKE を用いた場合では，公開鍵を用いるため鍵管理コストは削減できるが，SKE の場合と同様，サービス事業者毎に暗号化データを生成する必要があるため，ストレージコストの課題が生じてしまう．また，PDS では複数あるサービス事業者に応じて提供するデータを選択可能であることがシステム要件の一つである．サービス事業者毎に渡すデータを選択して暗号化するとき，クラウドに蓄積・管理されている暗号化データは，一般的に，一度復号して再び暗号化する必要がある．したがって，クラウド上のデータベースが不正アクセスを受けた場合，復号したデータが漏洩する恐れがある．このため，クラウド上にある全てのデータは一度も復号されることなく，再暗号化されることが望ましいが，SKE や PKE では，クラウド上で一度暗号文を復号しない限り，クラウド上の暗号化データをサービス事業者毎に選ぶことはできない．従って，PDS の利便性を損なわずに安全性を保証可能な暗号化手法が必要である．

†NHK 放送技術研究所　NHK Science and Technology Research Laboratories

1.2 関連研究

Blaze らはプロキシ再暗号化方式（proxy re-encryption (PRE) [4] を提案した．PRE は，プロキシサーバ（クラウド）上でデータを暗号化したまま再暗号化可能な暗号方式である．PRE を用いると，プロキシサーバはユーザの秘密鍵や平文を用いずに，ユーザの公開鍵に対応する暗号文を他のユーザの暗号文に効率的に変換できる．2007 年には，Green と Ateniese が ID ベース暗号（IBE）[5] のメカニズムをプロキシ再暗号化方式に導入し，ID ベースプロキシ再暗号化方式（identity-based proxy re-encryption: IB-PRE）を提案した[6]．IB-PRE では，ユーザの公開鍵はメールアドレスや電話番号などの一意の識別子を用いることが可能であるため，公開鍵の管理や配布の負荷を抑えることができる．IB-PRE が提案されて以来，多くの方式が改良・提案されてきた．例えば，再暗号化の正当性を検証可能な方式[13]，安全性証明においてランダムオラクルを仮定せずに証明を行う標準モデル方式[7]，量子コンピュータに対しても安全な耐量子方式[8][9]，属性ベース暗号と組み合わせた方式[10]，鍵集約可能な方式[11] などがある．鍵集約可能なプロキシ再暗号化方式（key-aggregate proxy re-encryption: KA-PRE）[11] は，プロキシ再暗号化方式 (PRE) に鍵集約暗号 (key-aggregate cryptosystem: KAC）[12]の技術を組み込んだ暗号方式であり，2021 年に Pateek と Purushothama によって提案された．KAC は，公開鍵暗号の一種で，集約鍵を用いてデータ所有者が自分のデータに対するアクセス権を他のユーザに安全かつ効率的に委譲することを可能にする．KA-PRE では，KAC を用いてデータのアクセス権を指定して再暗号化することで，任意のデータのみ安全に再暗号化することができる．

Pateek と Purushothama が提案した KA-PRE のシステムモデルでは，まずデータ所有者が各ユーザからデータを集めてクラウド上に保存する．各ユーザはクラウド上にある元々の自分のデータにはアクセスでき，その他のデータはデータ所有者が再暗号化して別のユーザに配布する．従って，自分のデータを自分で管理するという PDS のサービス

モデルとは異なるため，KA-PRE 方式をそのまま PDS システムに適用することはできない．また，鍵の配布方法についても別途セキュアチャネルを確保しなければならない．Kajita らは，IB-PRE[6][13]を用いて PDS に適用可能なシステムを構築した[14]．彼らは ID ベース暗号の仕組みによって効率的な鍵管理を実現し，クラウド上に保存した暗号化データをサービス事業者毎に再暗号化している．しかし，IB-PRE をそのまま適用すると，再暗号化されたデータの内，任意のデータを選んで再暗号化することができないため，彼らはメッセージインデックスを導入し，暗号文と共にデータベースに記録することで，任意のデータを再暗号化可能な PDS システム構築した．しかし，メッセージインデックスの導入により，どの暗号化データが選択されて再暗号化されるのか，クラウド側が分かってしまうという脆弱性がある．これは，クラウドがプロトコルには従う semi-honest なエンティティであっても有効な攻撃手法であり，例えば毎回同じデータを再暗号化することが分かると，データの中身は分からなくとも，そのデータが重要であることから，そのデータを意図的に破損させることでサービス低下を狙うような攻撃が考えられる．

1.3 貢献

そこで本稿では，鍵集約機能を持つプロキシ再暗号化方式（KA-PRE）と，ID ベースプロキシ再暗号化方式(IB-PRE) を組み合わせ，鍵集約機能を持つ ID ベースプロキシ再暗号化方式(KA-IB-PRE) を開発した．これにより，従来の ID ベースプロキシ再暗号化の性質に加え，クラウドにはどのデータを再暗号化するかという情報を秘匿したまま，鍵集約機能によって任意のデータを選択して再暗号化することが可能となる．具体的には，後の章で記述する構成において，データ所有者からクラウドにデータクラス集合 S_B を送るのではなく，集約鍵K_{S_B}を送ることで再暗号化データの対象の秘匿を実現している．ここで，データクラスとは，IB-PRE システム[14]のメッセージインデックスに対応し，再暗号化する対象を示し，データクラス集合は，再暗号化する対象となるデータクラスの集合を示す．

また，KA-IB-PRE を応用し，PDS に適用可能なプライバシー保護データ管理・提供システムを提案する．提案システムでは，PDS の要件である，クラウドに保存された暗号化データを，管理するユーザ本人の意思に基づいて事業者へ提供することが可能であり，従来の PDS システムよりも高い安全性を実現する．

2. 想定サービスモデル

本稿では図 1 に示す PDS サービスモデルを考える．データ所有者（DO），サービス事業者（SP），クラウド（CL）の 3 種類のエンティティが存在し，次のステップによって実現する．

Step 1. DO が SP へ提供可能なデータを暗号化して CL の暗号化 PDS へデータを保存する．
Step 2. DO がどの SP へデータを提供するか選択する．
Step 3. SP は受けとりたいデータクラス集合を DO へ通知する．ここでは個別のデータの指定はされないことに注意されたい．
Step 4. CL は指定されたデータクラスの暗号化データを再暗号化する．
Step 5. 再暗号化されたデータは SP へ提供される．
Step 6. SP へ提供されたデータに基づいて，DO は SP からサービスを享受する．

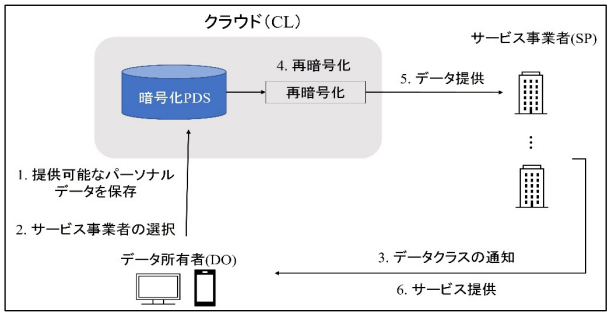

図 1. サービスモデル

3. 準備

本章では，提案する KA-IB-PRE 方式の構成に必要となるいくつかの定義を紹介する．

3.1.1 定義（双線形写像）

素数位数pと生成元$g \in \mathbb{G}_1$を持つ巡回群$\mathbb{G}_1$と，$\mathbb{G}_1$と同じ位数を持つ巡回群$\mathbb{G}_2$において，効率的に計算可能な双線形写像$e: \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$は以下の性質を満たす．ただし，$\forall g \in \mathbb{G}_1, l, k \in \mathbb{Z}_p$とする．

- （双線形性）$e(g^l, g^k) = e(g,g)^{lk} = e(g^k, g^l) = e(g,g)^{kl}$
- （非退化性）$e(g,g) \neq 1$.

3.1.2 定義（判定n-BDHE 問題）

$e(\cdot,\cdot)$が効率的に計算可能な双線形写像で，$h, g \in \mathbb{G}_1, g_i = g^{a^i} \in \mathbb{G}_1$（$a \in \mathbb{Z}_p$と$i = 1,2,\dots,n,n+2,\dots,2n$）において，入力$(h, P = (g_1,\dots,g_n,g_{n+2},\dots,g_{2n}), Z \in \mathbb{G}_2)$が与えられたとき，判定$n$-BDHE 問題は，$Z = e(h, g_{n+1})$が成り立つかどうかを判定する．

上記の入力をとるτ-時間アルゴリズムを A とする．このとき A の判定n-BDHE 問題を解く成功確率ϵは以下となる．

$$\left|\Pr\left[A\left(h, P, e(h, g_{n+1})\right) = 0\right] - \Pr[A(h, P, Z) = 0]\right| \geq \epsilon$$

3.1.3 定義（判定(τ, ϵ, n)-BDHE 仮定）

$(\mathbb{G}_1, \mathbb{G}_2)$において成功確率$\epsilon$で判定$n$-BDHE 問題を解く$\tau$-時間アルゴリズム A が存在しないとき，$(\mathbb{G}_1, \mathbb{G}_2)$において判定$(\tau, \epsilon, n)$-BDHE 仮定が成り立つという．

4. KA-IB-PRE 方式

IB-PRE と KA-PRE を組み合わせて，鍵集約型 ID ベースプロキシ再暗号化 (key-aggregate identity-based proxy re-encryption: KA-IB-PRE)を提案する．本章では，KA-IB-PRE のモデルと安全性を定義する．

4.1 定義

KA-IB-PRE は 7 つのアルゴリズム(Setup, KeyGen, Encrypt, Decrypt, ExReKeyGen, ReEncrypt, Decrypt$_R$)から構成される．以下に KA-IB-PRE のシンタックスを示す．

- $(params, msk) \leftarrow \text{Setup}(1^\lambda, n)$;

Setupアルゴリズムは，セキュリティパラメータλとデータクラスの最大値nを入力とし，公開セキュリティパラメータ$params$とマスター秘密鍵mskを出力するアルゴリズムである．ただし，公開セキュリティパラメータ$params$は各アルゴリズムの入力に取るものとして，本稿では明示的な表記は省略する．

- $sk_{id} \leftarrow \mathrm{KeyGen}(msk, \mathrm{id})$;

KeyGenは，マスター秘密鍵msk，ユーザの識別子idを入力とし，秘密鍵sk_{id}を出力する．

- $C_{id_1} \leftarrow \mathrm{Encrypt}(M, \mathrm{id}_1)$;

Encryptは，メッセージM，あるユーザの識別子id_1を入力とし，暗号文C_{id_1}を出力する．

- $M = \mathrm{Decrypt}(sk_{id_1}, C_{id_1}, \mathrm{id}_1)$;

Decryptは，あるユーザの識別子id_1に基づく秘密鍵sk_{id_1}，暗号文C_{id_1}，ユーザの識別子id_1を入力とし，メッセージMを出力する．

- $(rk_{id_1 \to id_2}, K_{S_B}) \leftarrow \mathrm{ExReKeyGen}(sk_{id_1}, S_B, \mathrm{id}_1, \mathrm{id}_2)$

ExReKeyGenアルゴリズムは，データを保持するユーザの秘密鍵sk_{id_1}とそのユーザの識別子id_1，データクラス集合S_B，データを提供するユーザの識別子id_2を入力とし，再暗号化鍵$rk_{id_1 \to id_2}$と集約鍵K_{S_B}を出力する．ただし，データクラス集合$S_B \in \{1, \dots, n\}$とする．

- $\tilde{C}_{id_2} \leftarrow \mathrm{ReEncrypt}(rk_{id_1 \to id_2}, C_{id_1} K_{S_B}, \mathrm{id}_1)$;

ReEncryptは，再暗号化鍵$rk_{id_1 \to id_2}$，暗号文C_{id_1}，集約鍵K_{S_B}，識別子id_1を入力とし，再暗号文$\tilde{C}_{id_2}$を出力する．

- $M = \mathrm{Decrypt}_R(sk_{id_2}, \tilde{C}_{id_2}, K_{S_B}, S_B, \mathrm{id}_2)$;

$\mathrm{Decrypt}_R$は，復号するユーザの秘密鍵sk_{id_2}，再暗号文$\tilde{C}_{id_2}$，集約鍵K_{S_B}，データクラス集合S_B，識別子id_2を入力とし，元のメッセージMを出力する．

4.1.1 正当性

任意のメッセージ$M \in \mathcal{M}$，データクラス$i \in \{1, \dots, n\}$，$S_A, S_B \subseteq \{1, \dots, n\}$において，次が成り立つ．

$$\Pr\left[M = \mathrm{Decrypt}(sk_{id_1}, C_{id_1}, \mathrm{id}_1) \middle| \begin{array}{c} sk_{id_1} \leftarrow \mathrm{KeyGen}(msk, \mathrm{id}_1); \\ C_{id_1} \leftarrow \mathrm{Encrypt}(M, \mathrm{id}_1); \\ i \in S_A \end{array}\right] = 1.$$

$$\Pr\left[M = Decrypt_R(sk_{id_2}, \tilde{C}_{id_2}, K_{S_B}, S_B, id_2) \middle| \begin{array}{c} sk_{id_2} \leftarrow KeyGen(msk, id_2) \\ (rk_{id_1 \to id_2}, K_{S_B}) \leftarrow ExReKeyGen(sk_{id_1}, S_B, id_1, id_2) \\ C_{id_1} \leftarrow \mathrm{Encrypt}(M, \mathrm{id}_1) \\ \tilde{C}_{id_2} \leftarrow ReEncrypt(rk_{id_1 \to id_2}, C_{id_1} K_{S_B}, id_1) \\ i \in S_B \end{array}\right] = 1.$$

4.1.2 安全性定義

我々は，Pareek らの鍵集約型プロキシ再暗号化方式の安全性モデル[11]に対して，Green らの ID ベースプロキシ再暗号化の安全性モデル[6]を組み合わせた KA-IB-PRE の安全性の定義を示す．集合Sに含まれていないデータクラスの集合$\bar{S} = \{1,2, \dots, n\} \setminus S$とする．ATK $\in (CPA, CCA)$において，チャレンジャーB と確率的多項式時間（PPT）の敵対者 A において以下のゲームを考える．

1. Init: 敵対者 A はターゲットデータクラス集合$S_B \subseteq \{1, \dots, n\}$ を出力し，チャレンジャーB はターゲットデータ$b^* \in S_B$を無作為に選ぶ．
2. Setup: B は Setup を実行し，$params$を A へ公開し，mskを安全に保管する．
3. Query-phase-1: A は B に対して以下のクエリを行う．ただし，各クエリ名はアルゴリズムと区別するため斜体で表現されることに注意されたい．
   - *ID-Extract*: A はあるidに対する秘密鍵$sk_{id} \leftarrow \mathrm{KeyGen}(msk, \mathrm{id})$を B から得る．
   - *KS-Extract*: A はデータクラス$S \in \bar{S}_B$に対する集約鍵K_Sを B から得る．
   - *Decrypt*: A はid_1における暗号文の復号クエリ$q_1, q_2, \dots, q_u$を B へ送る．$ATK = CCA$のとき，B は$M_i = \mathrm{Decrypt}(sk_{id_1}, \mathrm{Encrypt}(M_i, \mathrm{id}_1), \mathrm{id}_1)$ $(1 \le i \le u)$を返す．ただし，$C_i = \mathrm{Encrypt}(M_i, \mathrm{id}_1) \neq C_{b^*}$とする．$ATK = CPA$のとき，$B$ は⊥を返す．
   - *ReKeyGen*: A はid_1, id_2（$id_1 \neq id_2$）において，再暗号化鍵$rk_{id_1 \to id_2}$を B から得る．
   - *ReEncrypt*: $ATK = CCA$のとき，A はid_1において暗号化された任意の$C_{id_1} \leftarrow \mathrm{Encrypt}(M, \mathrm{id}_1)$において，$K_S$と$rk_{id_1 \to id_2}$を用いて$\tilde{C}_{id_2}$を B から得る．$ATK = CPA$のとき，B は⊥を返す．
   - *Decrypt*$_R$: A はid_2における再暗号文の復号クエリ$q_1, q_2, \dots, q_v$を B へ送る．$ATK = CCA$のとき，B は$M_j = \mathrm{Decrypt}_R(sk_{id_2}, \tilde{C}_j, K_{S_B}, S_B, \mathrm{id}_2)$ $(1 \le j \le v)$ を返す．$ATK = CPA$のとき，B は⊥を返す．
4. Choice and Challenge: A はメッセージスペースから$(M_0, M_1) \leftarrow \mathcal{M}$と$id^*$を$B$へ渡す．$B$は$d \leftarrow \{0,1\}$において，$C^* \leftarrow \mathrm{Encrypt}(M_d, \mathrm{id}^*)$を実行して A へ返す．
5. Guess: Aはd'を出力し，もし$d = d'$であればAの勝利とする．このときの成功確率は以下となる．

$$Adv_{A,n} = \left|\Pr[d = d'] - \frac{1}{2}\right|.$$

定義（CCA・CPA 安全性）

τ時間 PPT アルゴリズム A がデータクラスnにおいて，d_1回の Decrypt クエリとd_2回の$\mathrm{Decrypt_R}$クエリを実行し，$Adv_{A,n} < \epsilon$ であるとき，KA-IB-PRE 方式は$(\tau, \epsilon, n, d_1, d_2)$-CCA 安全という．また，$(\tau, \epsilon, n, 0, 0)$-CCA 安全であるとき，KA-IB-PRE は$(\tau, \epsilon, n)$-CPA 安全という．

5. 具体的構成

4.1 章で定義された KA-IB-PRE を実現するための具体的な構成例を示す．

- $(params, msk) \leftarrow \mathrm{Setup}(1^\lambda, n)$;
- $\mathbb{G}_1, \mathbb{G}_2$を素数位数$p$を持つ巡回群とする．
- $e(\mathbb{G}_1, \mathbb{G}_1) \to \mathbb{G}_2$を双線形写像とする．
- $g \in \mathbb{G}_1$を生成元とする．
- 無作為に$\alpha \leftarrow \mathbb{Z}_p$を選び，任意の$i \in \{1, \dots, 2n\}$において，$g_i \coloneqq g^{\alpha^i}$とする．
- ハッシュ関数$H_1, H_2, H_3, H_4, H_5, H_6$を次のように定義する．

$$H_1 \colon \mathbb{G}_2 \to \{0,1\}^\lambda,$$
$$H_2 \colon \mathbb{G}_1 \times \mathbb{G}_1 \times \mathbb{G}_2 \times \mathbb{G}_1 \times \{0,1\}^\lambda \to \mathbb{G}_1,$$
$$H_3 \colon \{0,1\}^\lambda \times \mathbb{G}_2 \to \mathbb{Z}_p,$$
$$H_4 \colon \{0,1\}^\lambda \to \mathbb{G}_1,$$
$$H_5 \colon \mathbb{G}_2 \to \mathbb{G}_1,$$
$$H_6 \colon \{0,1\}^\lambda \to \mathbb{Z}_p.$$

- 公開パラメータ$params$とマスター秘密鍵mskを出力する．

$$params = (g, g_1, \dots, g_{2n}, g^\alpha, H_1, \dots, H_6)$$
$$msk = \alpha$$

- $sk_{id} \leftarrow \mathrm{KeyGen}(msk, \mathrm{id})$;
- ユーザ識別子$id \in \{0,1\}^*$において，秘密鍵sk_{id}を計算する．

$$sk_{id} = H_4(id)^\alpha \in \mathbb{G}_1$$

- $C_{id_1} \leftarrow \mathrm{Encrypt}(M, \mathrm{id}_1)$;
- $M \in \{0,1\}^\lambda$，$\mathrm{R} \leftarrow \mathbb{G}_2$から，以下を計算する．

$$t = H_3(M, R) \in \mathbb{Z}_p$$

- $C_{id_1} = (C_1, C_2, C_3, C_4, C_5, C_6, C_7)$を出力する．

$$C_1 = g^t,$$
$$C_2 = (H_4(id)g_n)^t,$$
$$C_3 = R \cdot e(g, g_n)^t,$$
$$C_4 = H_4(id)^t,$$
$$C_5 = (C_4)^t,$$
$$C_6 = M \oplus H_1(R),$$
$$C_7 = H_2(C_1, C_2, C_3, C_4 C_5)^t$$

- $M = \mathrm{Decrypt}(sk_{id_1}, C_{id_1}, \mathrm{id}_1)$;
- 次の式を計算し，成立しない場合は処理を中止する．

$$\begin{aligned} e(C_1, H_4(id)g_n) &= e(g^t, H_4(id)g_n) \\ &= e(g, (H_4(id)g_n)^t) \\ &= e(g, C_2) \end{aligned} \quad (1)$$

$$\begin{aligned} e(C_1, C_4) &= e(g^t, H_4(id)^t) \\ &= e\left(g, H_4(id)^{t^2}\right) \\ &= e(g, C_5) \end{aligned} \quad (2)$$

$$\begin{aligned} e\left(C_1, H_2(C_1, C_2, C_3, C_5, C_6)\right) &= e\left(g^t, H_2(C_1, C_2, C_3, C_5, C_6)\right) \\ &= e(g, H_2(C_1, C_2, C_3, C_5, C_6)^t) \\ &= e(g, C_7) \end{aligned} \quad (3)$$

- 次の式を計算し，Rを求める．

$$C_3 \frac{e\left(sk_{id_1}(g^\alpha)^{n+1}(g_n)^{-1}, C_1\right)}{e(C_2, g^\alpha)} = R \quad (4)$$

- 得られたRから以下を計算し，平文Mを入手する．

$$M = C_6 \oplus H_1(R)$$

- $(rk_{id_1 \to id_2}, K_{S_B}) \leftarrow \mathrm{ExReKeyGen}(sk_{id_1}, S_B, \mathrm{id}_1, \mathrm{id}_2)$
- 再暗号化の対象となるデータクラス集合をS_Bとする．ただし，$S_B \subseteq \{1, \ldots, n\}$とする．
- 乱数$\sigma' \leftarrow \{0,1\}^\lambda$，生成元$R' \leftarrow \mathbb{G}_2$を無作為に選び，

$$r = H_3(\sigma', R')$$

を計算する．

- 集約鍵K_{S_B}を以下とする．

$$K_{S_B} = \left(\prod_{b \in S_B} g_{n+1-b}^r\right)$$

- $rk_{id_1 \to id_2} = (rk_0, rk_1, rk_2, rk_3, rk_4, rk_5, rk_6)$を以下のように計算する．ただし，乱数$s \leftarrow \mathbb{Z}_p$とする．

$$rk_0 = sk_{id_1} \cdot H_4(id_1)^s,$$
$$rk_1 = g^r,$$
$$rk_2 = \left(H_4(id_2)K_{S_B}\right)^r,$$
$$rk_3 = R' e(g, g_n)^r$$
$$rk_4 = g^s H_4(\sigma'),$$
$$rk_5 = \sigma' \oplus H_1(R'),$$
$$rk_6 = H_2(rk_1, rk_2, rk_3, rk_4, rk_5)^r.$$

- $\tilde{C}_{id_2} \leftarrow \mathrm{ReEncrypt}(rk_{id_1 \to id_2}, C_{id_1} K_{S_B}, \mathrm{id}_1)$;
- 再暗号文$\tilde{C}_{id_2} = \left(\tilde{C}_0, \tilde{C}_1, \tilde{C}_2, \tilde{C}_3, \tilde{C}_4, \tilde{C}_5, \tilde{C}_6, \tilde{C}_7, \tilde{C}_8\right)$を以下のように計算する．

$$\tilde{C}_0 = K_{S_B} C_3 \frac{e(rk_0(g^\alpha)^{n+1}(g_n)^{-1}, C_1)}{e(C_2, g^\alpha)},$$

$$\tilde{C}_1 = rk_1 = g^r$$
$$\tilde{C}_2 = rk_2 = \left(H_4(id_2)K_{S_B}\right)^r,$$
$$\tilde{C}_3 = rk_3 = R' e\left(g, g_n\right)^r$$
$$\tilde{C}_4 = C_4 = H_4(id_1)^t$$
$$\tilde{C}_5 = rk_5 = \sigma' \oplus H_1(R'),$$
$$\tilde{C}_6 = rk_4 = g^s H_4(\sigma'),$$
$$\tilde{C}_7 = C_6 = M \oplus H_1(R)$$
$$\tilde{C}_8 = rk_6 = H_2(rk_1, rk_2, rk_3, rk_4, rk_5)^r.$$

- $M = \mathrm{Decrypt}_R\left(sk_{id_2}, \tilde{C}_{id_2}, K_{S_B}, S_B, \mathrm{id}_2\right)$;
- 以下を計算し，成立しない場合は処理を中止する．

$$e\left(\left(\tilde{C}_1\right)^2, H_4(id_2)\left(\prod_{b \in S_B} g_{n+1-b}\right)\right) = e\left((g^r)^2, H_4(id_2)\left(\prod_{b \in S_B} g_{n+1-b}\right)\right)$$
$$= \left(g, H_4(id_2)\left(\prod_{b \in S_B} g_{n+1-b}\right)^{r^2}\right)$$
$$= e\left(g, \left(H_4(id_2)K_{S_B}\right)^r\right) = e(g, \tilde{C}_2). \quad (5)$$

$$e\left(\tilde{C}_1, H_2\left(\tilde{C}_1, \tilde{C}_2, \tilde{C}_3, \tilde{C}_6, \tilde{C}_5\right)\right) = e\left(g^r, H_2(rk_1, rk_2, rk_3, rk_4, rk_5)\right)$$
$$= e(g, H_2(rk_1, rk_2, rk_3, rk_4, rk_5)^r) = e\left(g, \tilde{C}_8\right). \quad (6)$$

- 上記(5)(6)式が成立するとき，任意の$j \in S_B$において以下を計算する．

$$\tilde{C}_3 \frac{e\left(K_{S_B} \cdot sk_{id_2} \cdot \prod_{b \in S_B, b \neq j} g_{n+1-b+j}, \tilde{C}_1\right)}{e\left(\tilde{C}_2, g^\alpha\right) e\left(\prod_{b \in S_B} g_{n+1-b+j}, \tilde{C}_1\right)} = R' \quad (7)$$

- 得られたR'を用いてσ'を計算する．

$$\tilde{C}_5 \oplus H_1(R') = \sigma' \quad (8)$$

- 次に得られたσ'を用いてg^sを計算する．

$$g^s = \frac{\tilde{C}_6}{H_4(\sigma')} \quad (9)$$

- $r = H_3(\sigma', R')$より，Rを計算する．

$$R = \tilde{C}_0 \cdot \left(\left(\prod_{b \in S_B} g_{n+1-b}\right)^r e\left(g^s, \tilde{C}_4\right)\right)^{-1} \quad (10)$$

- 最後に，Rを用いてMを計算する．

$$M = \tilde{C}_7 \oplus H_1(R)$$

5.1.1 正当性

- (1)-(3)式が成立するとき，(4)式が成立することを示す．

$$\begin{aligned} & C_3 \frac{e\left(sk_{id_1}(g^\alpha)^{n+1}(g_n)^{-1}, C_1\right)}{e(C_2, g^\alpha)} \\ &= Re(g, g_n)^t \frac{e(H_4(id_1)^\alpha (g^\alpha)^{n+1}(g_n)^{-1}, g^t)}{e((H_4(id_1)g_n)^t, g^\alpha)} \\ &= R \frac{e(g, g_n)^t \cdot e(H_4(id_1)^\alpha, g^t) \cdot e((g^\alpha)^{n+1}, g^t) \cdot e(g_n, g)^{-t}}{e\left(\left(H_4(id_1)\right)^t, g^\alpha\right) \cdot e((g_n)^t, g^\alpha)} \\ &= R \frac{e(H_4(id_1), g)^{\alpha t} \cdot e((g^\alpha)^{n+1}, g^t)}{e(H_4(id_1), g)^{\alpha t} \cdot e(g_n, g^\alpha)^t} = R \frac{e(g, g)^{\alpha^{n+1} t}}{e(g, g)^{\alpha^{n+1} t}} = R. \end{aligned}$$

- (5)(6)式が成立するとき，(7)式が成立することを示す．

$$\begin{aligned} & \tilde{C}_3 \frac{e\left(K_{S_B} \cdot sk_{id_2} \cdot \prod_{b \in S_B, b \neq j} g_{n+1-b+j}, \tilde{C}_1\right)}{e\left(\tilde{C}_2, g^\alpha\right) e\left(\prod_{b \in S_B} g_{n+1-b+j}, \tilde{C}_1\right)} \\ &= R' e(g_1, g_n)^r \frac{e\left(\prod_{b \in S_B} g_{n+1-b}^r \cdot H_4(id_2)^\alpha \prod_{b \in S_B, b \neq j} g_{n+1-b+j}, g^r\right)}{e\left(\left(H_4(id_2) \prod_{b \in S_B} g_{n+1-b}^r\right)^r, g^\alpha\right) \cdot e\left(\prod_{b \in S_B} g_{n+1-b+j}^r, g^r\right)} \\ &= R' e(g_1, g_n)^r \frac{e\left(\prod_{b \in S_B} g_{n+1-b}^r \cdot H_4(id_2)^\alpha, g^r\right) \cdot e\left(\prod_{b \in S_B, b \neq j} g_{n+1-b+j}, g^r\right)}{e\left(H_4(id_2) \prod_{b \in S_B} g_{n+1-b}^r, g\right)^{\alpha r} \cdot e\left(\prod_{b \in S_B} g_{n+1-b+j}^r, g^r\right)} \\ &= R' e(g_1, g_n)^r \frac{e\left(H_4(id_2) \prod_{b \in S_B} g_{n+1-b}^r, g\right)^{\alpha r} \cdot e\left(\prod_{b \in S_B} g_{n+1-b+j}, g^r\right) e\left((g_{n+1})^{-1}, g^r\right)}{e\left(H_4(id_2) \prod_{b \in S_B} g_{n+1-b}^r, g\right)^{\alpha r} \cdot e\left(\prod_{b \in S_B} g_{n+1-b+j}^r, g^r\right)} \\ &= R' \frac{e(g_1, g_n)^r}{e(g_{n+1}, g)^r}. \end{aligned} \quad (7')$$

ここで

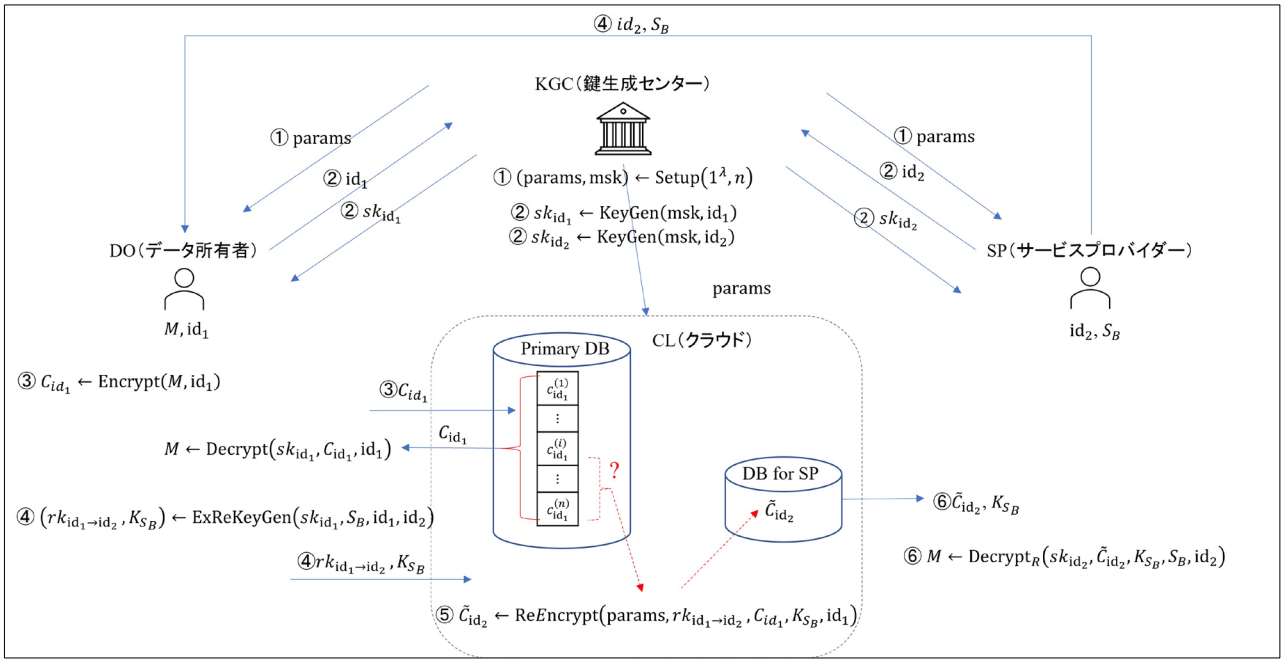

図 2　提案システムアーキテクチャ

$$e(g_1, g_n)^r = e(g, g_n)^r = e(g^\alpha, (g^\alpha)^n)^r = e\left(g, g^{\alpha^n \cdot \alpha}\right)^r$$
$$= e\left(g, g^{\alpha^{n+1}}\right)^r = e(g, g_{n+1})^r$$

より，(7')式は以下となる．

$$R' \frac{e(g_1, g_n)^r}{e(g_{n+1}, g)^r} = R'.$$

- (7)-(9)式より，(10)式が成立することを示す．

$$\tilde{C}_0 \cdot \left(\left(\prod_{b \in S_B} g_{n+1-b} \right)^r e(g^s, \tilde{C}_4) \right)^{-1}$$

$$= K_{S_B} C_3 \frac{e(rk_0 (g^\alpha)^{n+1} (g_n)^{-1}, C_1)}{e(C_2, g^\alpha) \left(\prod_{b \in S_B} g_{n+1-b}\right)^r e(g^s, \tilde{C}_4)}$$

$$= \frac{\prod_{b \in S_B} g_{n+1-b}^r \cdot R \cdot e(g, g_n)^t \cdot e(H_4(id_1)^\alpha H_4(id_1)^s (g^\alpha)^{n+1} (g_n)^{-1}, g^t)}{e\left(\left(H_4(id) g_n\right)^t, g^\alpha\right) \cdot \left(\prod_{b \in S_B} g_{n+1-b}\right)^r \cdot e(g^s, H_4(id_1)^t)}$$

$$= \frac{R \cdot e(g, g_n)^t \cdot e(H_4(id_1)^\alpha, g^t) \cdot e(H_4(id_1)^s, g^t) \cdot e((g^\alpha)^{n+1}, g^t) \cdot e(g_n, g^t)^{-1}}{e(H_4(id)^t, g^\alpha) \cdot e(g_n^t, g^\alpha) \cdot e(g^s, H_4(id_1)^t)}$$

$$= R \cdot \frac{e(g, g_n)^t}{e(g, g_n)^t} \cdot \frac{e(H_4(id_1), g)^{\alpha t}}{e(H_4(id_1), g)^{\alpha t}} \cdot \frac{e(H_4(id_1), g)^{st}}{e(H_4(id_1), g)^{st}} \cdot \frac{e(g, g)^{\alpha^{(n+1)} t}}{e(g, g)^{\alpha^{(n+1)} t}} = R.$$

定理 1. 提案 KA-IB-PRE 方式は，(τ, ϵ, n)-BDHE 仮定が $(\mathbb{G}_1, \mathbb{G}_2)$において成立するとき，ランダムオラクル仮定の下で$(\tau, \epsilon, n, d_1, d_2)$-CCA 安全である．

6. データ管理・提供システム

KA-IB-PRE を用いた PDS に適用可能なデータ管理・提供システムの構成例を図 2 に示す．提案システムでは，鍵生成センター（KGC），データ所有者（DO），サービス事業者（SP），クラウド（CL）の 4 つのエンティティによって構成される．KGC は信頼できる第三者機関であり，DO と SP それぞれの ID に対して秘密鍵を生成する．DO は，SP へデータを提供するエンティティであり，データを暗号化して CL に保存する．SP は，CL を経由して DO からデータを受け取るエンティティであり，DO によって暗号化されたデータを管理し，SP の ID に基づいて，指定されたデータクラスの再暗号化を行い，SP へデータを提供する．提案システムは次のステップによって実現する．ただし，本構成では簡単のため DO と SP はそれぞれ一つずつとしたが，複数でも構成可能である．また，Step 4 で DO はデータクラス集合S_Bを SP から受け取るものとするが，DO がS_Bを選択しても構わない．その場合はS_Bを SP へ共有する．

Step 1. KGC は Setup を行い，params を各エンティティに公開し，msk を安全に保管する．

Step 2. KGC は，DO と SP からそれぞれid_1，id_2を受け取り，KeyGen によって各 ID に対応する秘密鍵sk_{id_1}，sk_{id_2}を出力し，それぞれ DO と SP へ返す．

Step 3. DO は，Encrypt によって平文 M を暗号化し，暗号文C_{id_1}を CL へ送信する．ここで，CL に保存されたデータは Decrypt によって復号することができる．

Step 4. DO は，SP から識別子id_2とデータクラス集合S_Bを受け取り，ExReKeyGen によって再暗号化鍵$rk_{id_1 \to id_2}$と集約鍵K_{S_B}を計算し，CL へ送信する．

Step 5. CL は，再暗号化鍵$rk_{id_1 \to id_2}$と集約鍵K_{S_B}によって暗号文C_{id_1}を再暗号化し，再暗号文$\tilde{C}_{id_2}$を集約鍵と共に SP へ送信する．

Step 6. SP は，SP のid_2に対応する秘密鍵sk_{id_2}を用いて，$\mathrm{Decrypt}_R$によって元の平文 M を入手する．

6.1 システム評価

KA-IB-PRE による提案システムは，表 1 に示す 3 つの性質を満たす．

表 1. 比較．各暗号方式を用いて，PDS システムを構築したときに満たす性質．
③再暗号化データの選択可能性について，(*) IB-PRE を用いたシステム[14]ではメッセージインデックスの導入が必要であり，(**) 提案 KA-IB-PRE を用いたシステムでは，DO と SP が再暗号化データの対象を共有する必要がある．

要件		SKE	PKE	IB-PRE [14]	KA-IB-PRE
① 完全プライバシー保護	データの暗号化	✓	✓	✓	✓
	データ選択の秘匿	-	-	-	✓
② スケーラビリティ	秘密鍵のスケーラビリティ	-	✓	✓	✓
	クラウドストレージのスケーラビリティ	-	-	✓	✓
	IDベース鍵管理	-	-	✓	✓
③ 選択可能性	復号者の選択可能性	-	-	✓	✓
	再暗号化データの選択可能性	-	-	✓*	✓**

- **完全プライバシー保護．** PDS にあるデータは全て暗号化され SP へ提供されるデータは復号することなく再暗号化されている．さらに，従来の KA-PRE 方式[11]では再暗号化アルゴリズムReEncryptにデータクラス集合を直接入力していたが，KA-IB-PRE では再暗号化の際に集約鍵を入力に取るため，提案システムではどの暗号文を再暗号化するかについても秘匿されている．このため，CL は DO のデータに関連するいかなる情報も得られない．
- **スケーラビリティ．** DO と SP は互いに秘密鍵を共有する必要がなく，ID ベースによる効率的な鍵管理を可能とする．また，CL は暗号化データに対応するストレージと再暗号化データを一時的に保存するためのメモリー領域のみを必要とする．従って，DO と SP の数が増加しても各エンティティが持つ鍵の数および CL において保存されるデータ量は無関係であり，鍵管理と CL のストレージにおいて提案システムはスケーラブルである．
- **選択可能性．** ExReKeyGenアルゴリズムによって，データ提供先である SP の ID を用いて再暗号化鍵を生成することが可能であるため，提案システムではDOによって選択された SP のみが再暗号化データを復号することができる．ただし，DO と SP が互いに再暗号化の対象となるデータクラスを共有する必要がある点に注意されたい．

7. まとめ

鍵集約機能を持つプロキシ再暗号化方式（KA-PRE）と，ID ベースプロキシ再暗号化方式(IB-PRE) を組み合わせ，鍵集約機能を持つ ID ベースプロキシ再暗号化方式(KA-IB-PRE) を開発した．これにより，従来の ID ベースプロキシ再暗号化の性質に加え，鍵集約機能によって任意のデータを選択して再暗号化することが可能となる．また，KA-IB-PRE を応用することで，サーバーに保存された暗号化データを，管理するユーザ本人の意思に基づいてデータを再暗号化して提供するシステムを構築し，PDS への適用可能性を示した．

参考文献

[1] GitHub - solid/community-server: Community Solid Server: an open and modular implementation of the Solid specifications. Retrieved March 7, 2022 from https://github.com/solid/community-server
[2] Home Solid. Retrieved March 7, 2022 from https://solidproject.org/.
[3] Hasida, K., “Personal life repository as a distributed PDS and its dissemination strategy for healthcare services”, In 2014 AAAI Spring Symposium Series. (2014).
[4] Blaze M, Bleumer G, Strauss M. “Divertible protocols and atomic proxy cryptography.” In Eurocrypt. LNCS, vol 1403, pp 127–144, (1998).
[5] Boneh, D., and Franklin, M. “Identity-based encryption from the Weil pairing.” In CRYPTO. Santa Barbara, California, USA, August 19–23, 2001 Proceedings (pp. 213-229). Berlin, Heidelberg: Springer Berlin Heidelberg, (2001).
[6] Green, Matthew, and Giuseppe Ateniese. "Identity-based proxy re-encryption." International Conference on Applied Cryptography and Network Security. Springer, Berlin, Heidelberg, (2007).
[7] Chu, C. K., and Tzeng, W. G. “Identity-based proxy re-encryption without random oracles.” In ISC, Vol. 7, pp. 189-202, (2007).
[8] Singh, K., Rangan, C. P., and Banerjee, A. K. “Lattice Based Identity Based Proxy Re-Encryption Scheme.” J. Internet Serv. Inf. Secur., 3(3/4), 38-51. (2013).
[9] Dutta, P., Susilo, W., Duong, D. H., and Roy, P. S. “Collusion-resistant identity-based proxy re-encryption: lattice-based constructions in standard model.” Theoretical Computer Science, Vol. 871, pp. 16-29, (2021).
[10] Luo, S., Hu, J., and Chen, Z. “Ciphertext policy attribute-based proxy reencryption.” In ICISS, pp. 401-415. Springer Berlin Heidelberg, (2010).
[11] Pareek, G., and Purushothama, B. R. “KAPRE: Key-aggregate proxy reencryption for secure and flexible data sharing in cloud storage.” Journal of Information Security and Applications, 63, 103009, (2021).
[12] Chu CK, Chow SS, Tzeng WG, Zhou J, Deng RH. Key-aggregate cryptosystem for scalable data sharing in cloud storage. IEEE Trans Parallel Distrib Syst 2013;25(2), pp.468–77, (2013).
[13] Li-qiang, W., Xiao-yuan, Y., Min-qing, Z., and Xu-an, W. “IB-VPRE: adaptively secure identity-based proxy re-encryption scheme from LWE with re-encryption verifiability.” In Journal of Ambient Intelligence and Humanized Computing, 1-14, (2021).
[14] Kajita. K., Matsumura K.,Ohtake G., “Privacy-Preserving Data Management and Provision System for Personal Data Store.” In HCII 2023, Part III, CCIS 1834, to be appeared. (2023).