動的グループにおけるクラウドデータ共有を実現するための データ所持証明方式の拡張

1215090　多田菜南　【 セキュリティシステム研究室 】

Extension of Provable Data Possession method for Cloud Data Sharing in Dynamic Group

1215090　Nana TADA　【 Security Systems Lab. 】

1　はじめに

コールドデータと呼ばれる頻繁なアクセスは無いが，長期的な保存が必要なデータに注目が集まっている．コールドデータの具体例としては，アーカイブのような重要な記録が挙げられ，株主総会議事録や決算書，請求書等は法律によって記録が義務付けられている．また，記録管理の標準規格 ISO/IEC15489-1 では記録の責任は記録管理者だけでなく組織内の複数人に割り当てることが望ましいとしており，これら全員に管理する責任がある．アーカイブ等を電子的に保存する流れは広まっており，2020 年までにパブリッククラウドにはコンシューマデバイスよりも多くのデータが保存されることが予想されている [1].

クラウドストレージ (CS) は安価なストレージを提供するが，利用者はデータを完全に管理することができなくなるため，そのデータのセキュリティは CS に依存する．コールドデータを CS に委託する場合，これらのデータを完全に CS が所持していることを確認する必要がある．S-PDP というデータ所持証明方式は CS 上のデータに破損がないかデータサイズに関係なく規定回数内であれば一定の計算量で効率的に検証できる．S-PDP は対称鍵暗号を用いており，許可のないデータ削除等を検知できるがデータ検証を行えるのはそのデータの所有者 1 人である．そこで，CS 上の大量データが正しく保存されているかグループで効率的に検証可能な方式へ S-PDP を拡張する．そのために，S-PDP の特徴とセキュリティ要件に合ったグループ鍵管理方式を提案する．

2　グループ鍵管理要件

グループで S-PDP を実現するための要件を述べる．

【信頼エンティティの最小限化】 S-PDP は CS を信頼できないエンティティとしており，グループ鍵管理においても信頼できるエンティティはデータ所有者 (DO) と DO に認められたグループユーザだけとする．

【動的グループでの効率的な鍵更新】 ユーザの入退出がある動的グループでは，メンバ変更の度にグループ鍵を新しくする必要がある．

【失効ユーザの不正防止】 S-PDP は検証できる回数が予め決められている．失効されたユーザは信頼できるエンティティではないため，失効ユーザが検証できると不正に検証回数を消費される可能性がある．

3　前提知識

3.1　双線形写像

写像 $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ が以下の三つの条件を満たす時，e を双線形写像という．

(1) $\mathbb{G}_1$ と $\mathbb{G}_2$ は位数が同じ素数 q の群
(2) $\forall a, b \in Z_q$，$g \in \mathbb{G}_1$ に対して，$e(g^a, g^b) = e(g, g)^{ab}$ は効率的に計算可能
(3) $e(g, g) \neq 1$ （非退化性）

3.2　プロキシ再暗号化（Proxy Re-encryption:PRE）

プロキシ再暗号化はプロキシが平文の情報を得ずに PRE 鍵 $rk_{A\to B}$ を用いてユーザ A 宛の暗号文をユーザ B の暗号文に変換可能な暗号方式である．プロキシ再暗号化は双線形写像によって実現され，公開パラメータを $g \in \mathbb{G}_1$，$\mathbb{Z} = e(g, g) \in \mathbb{G}_2$ とする．$\alpha, \beta \in Z_q$，A の鍵ペア $(sk_A, pk_A) = (\alpha, g^\alpha)$，$B$ の鍵ペア $(sk_B, pk_B) = (\beta, g^\beta)$ とすると，PRE 鍵は $rk_{A\to B} = g^{\frac{\beta}{\alpha}}$ となる．

暗号化： A が平文 m を暗号化する時，乱数 k を選び暗号文 $C^1 = (\mathbb{Z}^{\alpha k}, m\mathbb{Z}^k)$ を生成する．C^1 は A のみ復号できる第一レベル暗号文とする．また，この時の第二レベル暗号文を $C^2 = (g^{\alpha k}, m\mathbb{Z}^k)$ と表現する．

再暗号化： $C^2 = (g^{\alpha k}, m\mathbb{Z}^k)$ を $rk_{A\to B} = g^{\frac{\beta}{\alpha}}$ で C^1 へ再暗号化する．

$$\begin{aligned}(e(rk_{A\to B}, g^{\alpha k}), m\mathbb{Z}^k) &= (e(g^{\frac{\beta}{\alpha}}, g^{\alpha k}), m\mathbb{Z}^k) \\ &= (\mathbb{Z}^{\beta k}, m\mathbb{Z}^k) = C^1\end{aligned}$$

復号： B は C^1 と sk_B より $m = m\mathbb{Z}^k / \mathbb{Z}^{\beta k \frac{1}{\beta}}$ を復号する．

3.3　定義

Basic Diffie-Hellman Problem（BDHP）仮定 [3]

代数曲線上の点を P とし，$r \in Z_q$ に対して $r \cdot P$ を計算することは容易であるが，P，$r \cdot P$ を与えられた時，r を効率的に計算するアルゴリズムは存在しない仮定

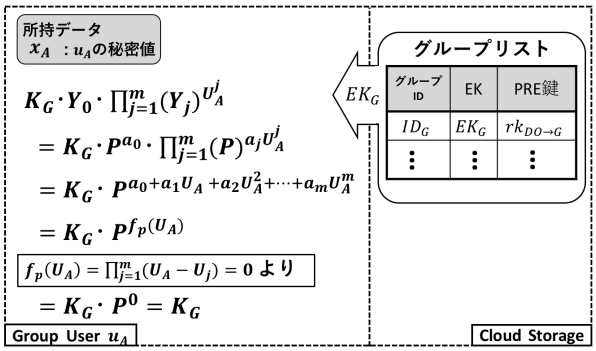

図 1　グループ鍵の取得

4　提案方式

提案方式はクラウドストレージ CS，データ所有者 DO, グループユーザで構成される．CS は DO のデータを保存しデータ削除等の不正が想定されるサーバである．DO は CS 上にデータを保存する際に検証データを生成し，グループユーザの入退出も管理する．グループユーザ u_A は DO にデータ検証が認められているグループ G のユーザとする．

S-PDP は対称鍵暗号の鍵を用いて検証データを作成・検証するため，検証できるユーザは鍵を所持する DO のみである．提案方式では S-PDP の検証に使用する検証鍵を S とした時，S を暗号化して CS 上で保存し，検証のリクエストがあった場合グループ鍵 K_G を持つユーザのみ復号可能な暗号文へ再暗号化される．これにより，グループでの S-PDP の検証を実現する．提案方式では，グループ鍵配布に多項式関数，検証鍵配布にプロキシ再暗号化を使用し，グループ鍵管理を実現する．グループ鍵と検証鍵のユーザへの配布を説明する．

グループ鍵配布：　DO はグループ G のためのグループ鍵 K_G を生成し，グループ G の鍵関数 EK_G と PRE 鍵 $rk_{DO\to G}$ を CS へ登録する．グループ G に所属するユーザ ID を ID_j，ID_j の秘密値 x_j とする．ハッシュ関数を h とし $U_j = h(ID_j, x_j)$ を求め，グループユーザ数 m の多項式関数 $f_p(x)$ を求める．

$$f_p(x) = \prod_{j=1}^{m}(x - U_j) = \sum_{i=0}^{m} a_i x^i \ (mod\, q) \qquad (1)$$

加法巡回群の生成元 $P \in \mathbb{G}_{add}$ と式 1 より，$\{Y_0, ..., Y_m\} = \{P^{a_0}, ..., P^{a_m}\}$ を求め，$EK_G = \{K_G \cdot Y_0, Y_1, \cdots, Y_m\}$ とする．DO の秘密鍵 $sk_{DO} = \pi_0$ とした時，グループ G の PRE 鍵 $rk_{DO\to G} = g^{\frac{K_G}{\pi_0}}$ である．EK_G と PRE 鍵 $rk_{DO\to G}$ を CS へ登録する．図 1 にグループ G のユーザ u_A が K_G を取得する流れを示す．グループメンバの変更があれば DO は新しいグループ鍵，鍵関数，PRE 鍵を作り CS へ再登録する．

検証鍵の取得：　検証者 u_A が検証する時，検証リクエストを受けた CS は検証データ $\sigma = \{V, C^2\}$ から PRE 鍵 $rk_{DO\to G} = g^{\frac{K_G}{\pi_0}}$ を用いて $C^1 = (\mathbb{Z}^{K_G k},\ S\mathbb{Z}^k)$ を計算し，$\{V, C^1\}$ を u_A へ返す．u_A はグループ鍵 K_G を用いて式 2 より検証鍵 S を取り出す．

$$S = S\mathbb{Z}^k / \mathbb{Z}^{\frac{K_G k}{K_G}} = S\mathbb{Z}^k / \mathbb{Z}^k \qquad (2)$$

表 1　ストレージ・通信コストの比較

		S-PDP	提案方式
ストレージコスト		$t\|V\|$	$t(\|V\| + \|\mathbb{G}_1\| + \|S\| \cdot \|\mathbb{G}_2\|)$
通信コスト	データ登録	$\|D\| + t\|V\|$	$\|D\| + t(\|V\| + \|\mathbb{G}_1\| + \|S\| \cdot \|\mathbb{G}_2\|)$
	検証	$\|V\|$	$\|S\|,\ \|V\|$

5　評価

5.1　グループ鍵の安全性

CS が保存している鍵関数 EK_G からグループ鍵 K_G を得ることが困難なことを示す．鍵関数 EK_G から K_G を得るためには $K_G \cdot P^{a_0}$ から K_G を求める．しかし，$P^{a_0} \in \mathbb{G}_{add}$ より BDHP 仮定に矛盾している．よって CS は鍵関数 EK_G からグループ鍵 K_G を得ることが困難である．しかし，失効ユーザの持つ古いグループ鍵とそのグループ鍵に対応する PRE 鍵を CS が使用すると失効ユーザは検証鍵 S を得られる．そのため，提案方式では失効ユーザと結託がないことを前提とする．

5.2　ストレージ・通信コスト

提案方式と S-PDP の CS のストレージコストと通信コストについて評価したものを表 1 に示す．$|V|$ は検証データ V，$|\mathbb{G}_1|$ と $|\mathbb{G}_2|$ は巡回群 $\mathbb{G}_1$，$\mathbb{G}_2$，$|S|$ は検証鍵 S のサイズをそれぞれ示している．提案方式では検証データに加えて検証用の鍵データ C^2 も保存する必要があるため，S-PDP よりもストレージコストがかかる．しかし，S-PDP と同様に，データファイルサイズに関係なく固定サイズのストレージコストと通信コストになることが分かる．また，検証時の通信回数に関しては S-PDP が 1 回に対して，提案方式では 2 回発生する．

6　まとめ

本稿では，S-PDP の要件に合ったグループ鍵管理方式を提案し，S-PDP の効率性を維持したままデータ検証をグループで実現した．提案方式は効率的な鍵管理のためにプロキシ再暗号化と多項式関数を用いた．これにより動的グループに対応できる．

参考文献

[1] D. Reinsel, J. Gantz, J. Rydning, ”Data Age 2025”, IDC White Paper, November 2018.

[2] G. Ateniese, RD. Pietro, et al., ”Scalable and efficient Provable data possession”, Proc. 4th ACM Conf. SecureComm., 2008.

[3] Z. Zhu and R. Jiang, “A secure anti-collusion data sharing scheme for dynamic groups in the cloud,” IEEE TPDS, vol.27, pp.40–50, 2016.