7ZD-03

複数組織対応属性ベース暗号を用いたファイル共有システムのアップロードマネージャーの実装と評価

鈴木 智也　小松 蒼樹　石橋 拓哉　柿崎 淑郎　大東 俊博 †
東海大学 †
土田 光 ‡　金岡 晃 §　相原 玲二 ¶
日本電気株式会社 ‡　東邦大学 §　広島大学 ¶

1 はじめに

クラウド技術の発展により，オンラインストレージの利用が増加している．それに伴い，セキュリティと属性によるアクセスコントロールを同時に満たすことができる属性ベース暗号（Attribute-Based Encryption, ABE）という暗号化手法が注目されている．石橋らは，複数組織対応属性ベース暗号（Multi-Authority Attribute-Based Encryption, MA-ABE）を用いて共同研究などに利用可能なファイル共有システム [1] を提案した．ファイル共有システムの詳細設計は文献 [2] で行われており，実際にシステムを実装することが課題として挙げられている．本稿では特に，MA-ABE のユーザ秘密鍵（属性鍵）や公開パラメータが適切に配布されている前提で，ファイル共有システムとオンラインストレージ間の処理を実装する．また，提案システムでは複数の鍵発行センタ（Key Generation Center, KGC）の公開パラメータを暗号化時に取得する必要があるため，その取得方法の検討および取得時間の評価を行う．

2 実装

本研究の実装では，単一組織用の属性ベース暗号（Ciphertext-Policy Attribute-Based Encryption, CP-ABE）を利用したファイル共有システム [3] を参考に MA-ABE 用に拡張する．

Implementation and Evaluation of Upload Manager of a File Sharing System using MA-ABE
† Suzuki Tomoya, Komatsu Soju, Ishibashi Takuya, Kakizaki Yoshio, Ohigashi Toshihiro, Tokai University
‡ Hikaru Tsuchida, NEC
§ Akira Kanaoka, Toho University
¶ Reiji Aibara, Hiroshima University

MA-ABE は C 言語で実装をし，ペアリングライブラリは PBC を利用している．アップロード時には，Dropbox などのオンラインストレージにアップロードマネージャーと呼ばれるファイルアップロードシステムを介して暗号化したデータを送信する．また，ファイルデータ以外にディレクトリ構造も暗号化対象にし，その管理にはリストファイルと呼ばれる情報を用いる．ダウンロード時には，権限を持つユーザがリストファイルを介してファイルを直接ダウンロードし，復号する．以下では，本研究における各処理の実装について概説する（図 1）．

2.1 リストファイル

リストファイルのフォーマットは，大東らの研究 [3] を参考にし作成した（図 2）．リストファイルでは復号できる権限であるアクセス権ごとに識別文字，ファイル名，ファイルの公開用 URL，属性をまとめて暗号化する．同じディレクトリ下の全アクセス権の暗号化データを結合し，リストファイルとする．ヘッダ情報に暗号化時のデータサイズを書き込むことによって，対応する暗号文データを取得できるようにしている．

2.2 システム・ストレージ間の処理

システムにおけるデータの送受信は HTTPS 通信を前提にしている．ユーザ・アップロードマネージャー間およびユーザ・Dropbox 間の通信は curl により，Dropbox との通信は Droobox API v2 でアクセストークンを利用して実装している（図 1）．ユーザのダウンロード時には，リストファイル内の公開用 URL を利用してダウンロードのみ可能にしている．

アップロード時のアップロードマネージャの処理手順は以下の通りである．

1. MA-ABE を用いたチャレンジ＆レスポン

ス認証により，アップロードするユーザが適切な権限を持っていることを確認する．
2. アップロードするデータのファイル名を含めるために，Dropbox からリストファイルを取得する．
3. 公開パラメータを所持していない場合，サーバから公開パラメータを取得する．
4. リストファイル内の該当する暗号化ブロックを MA-ABE で復号してファイル名および公開用 URL を含めて再度暗号化する．
5. リストファイルを Dropbox にアップロードする．

過去にリストファイルに含まれていないアクセス権（属性の論理式）を新規に追加する場合はリストファイルの末尾に暗号化ブロックを追加する．これらの暗号化時にはアクセス権に含まれる属性の KGC から公開パラメータを取得する．なお，通信回数を減らすために，各 KGC の公開パラメータを公開パラメータ取得サーバに集約して提供するシステム構成としている（図 1）．さらに，過去に暗号化に使用した公開パラメータを短期間キャッシュすることで公開パラメータ取得サーバへのアクセス回数を削減する工夫もしている．

ダウンロード時のユーザの処理手順を以下に示す．

1. Dropbox からリストファイルを取得し一致する属性が存在するか確認する．
2. 一致した属性の暗号データを復号し公開用 URL を取得する．
3. 公開用 URL からファイルを取得し，復号する．

3 評価

文献 [3] と本システムの大きな違いは，MA-ABE で利用する複数の公開パラメータを効率的にダウンロードするために公開パラメータ取得サーバを設置したことである．したがって，本研究では公開パラメータ取得処理を中心に評価を行った．

公開パラメータがキャッシュされていない場合は，複数の公開パラメータを取得しなければならないため，そのオーバヘッドを評価する．その際，個別に公開パラメータを取得する場合と公開パラメータ取得サーバからまとめて取得

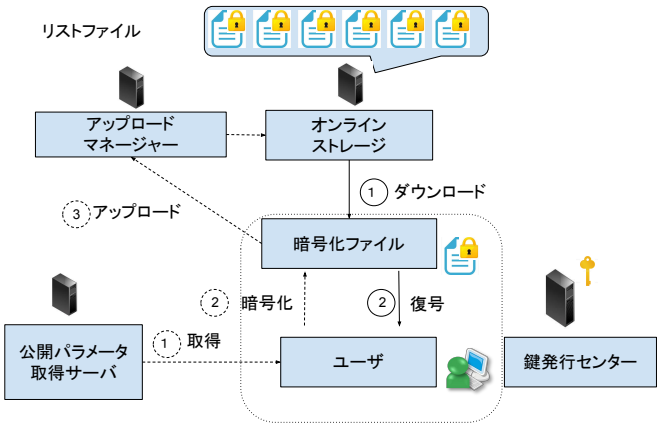

図 1　提案システムの概要

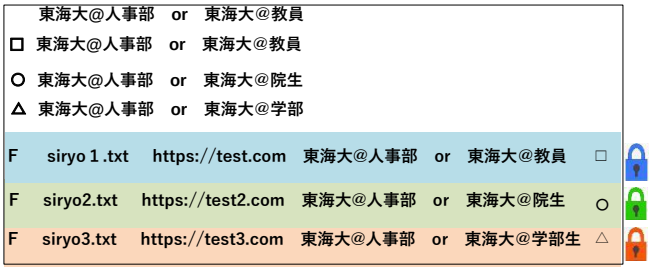

図 2　リストファイルの例

する場合の通信時間の違いについて評価することで効率的になることを示す．

紙面の都合により，実験結果については割愛し，発表時に詳細を報告する予定である．

謝辞

本研究の一部は JSPS 科研費（課題番号 22K12034）の助成，JST，CREST，PMJCR22M4 の支援を受けたものである．

参考文献

[1] 石橋拓哉, 小林海, 大東俊博, 土田光, 金岡晃, 柿崎淑郎, 相原玲二, “複数組織対応属性ベース暗号を用いたファイル共有システムの実現可能性に関する考察,” 情報処理学会論文誌, vol.64, no.3, pp.670-686, 2023 年 3 月.
[2] 石橋拓哉, 鈴木智也, 大東俊博, 土田光, 金岡晃, 柿崎淑郎, 相原玲二．複数組織対応属性ベース暗号を用いたファイル共有システムの設計，東海大学紀要 情報通信学部，出版予定，2024.
[3] 大東俊博, 後藤めぐ美, 西村浩二, 相原玲二, “暗号文ポリシー属性ベース暗号を利用したファイル名暗号化ファイル共有サービスの実装と性能評価,” 情報処理学会論文誌, vol.55, no.3, pp.1126-1139, 2014 年 3 月.