様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　３０　年　　６　月　　４　日現在

機関番号：　３２６４４
研究種目：　基盤研究(C)（一般）
研究期間：　2015～2017
課題番号：　１５Ｋ００１８５

研究課題名（和文）複数組織間で相互利用可能な属性ベース暗号に基づくファイル共有システムの研究開発

研究課題名（英文）A Research on File Sharing System using CP-ABE Support for Multi-Authorities

研究代表者
大東　俊博（Ohigashi, Toshihiro）

東海大学・情報通信学部・准教授

研究者番号：８０５０８１２７

交付決定額（研究期間全体）：（直接経費）　　3,600,000円

研究成果の概要（和文）：Dropboxに代表されるオンラインストレージサービスが普及してきている．このようなサービスではストレージの管理者によりデータを覗き見られる危険性があることから，ユーザ側で暗号化してデータを保護するシステムが注目されている．本研究では，暗号文ポリシー属性ベース暗号(CP-ABE)と呼ばれる暗号化方式を利用したファイル共有サービスについて複数組織が共同で安全に利用するための方法について検討し，その有効性について評価した．

研究成果の概要（英文）：A lot of online storage services, e.g. Dropbox, have been widely used. These services have a weakness, which the storage administrator can obtain contents of user's files. Hence client based encryption systems are used in order to protect user's files on online storage server. In this research, I discuss a file sharing system using Ciphertext-Policy Attribute-Based Encryption (CP-ABE) support for Multi-Authorities.

研究分野：　情報セキュリティ

キーワード：　属性ベース暗号　オンラインストレージ　複数組織対応

１．研究開始当初の背景

クラウド技術の普及により Dropbox に代表されるオンラインストレージサービスが手軽に利用できるようになった．これらのサービスは自身のファイルのバックアップ以外にもファイル共有の用途にも利用できる．一方，ユーザのデータが常にオンライン上のサーバに保存されるため，データの機密性や完全性の保護が課題となる．多くのストレージサービスではサーバ側でアクセス制御や暗号化を行い，アクセス権限の無い利用者からファイルを保護している．しかしながら，この方法ではストレージサービスの管理者によるデータの覗き見を防ぐことはできない．

サーバ管理者の覗き見を防ぐ方法として，クライアント側でコンテンツを暗号化し，その暗号文を共有するシステムが議論されている．クラウド上のサービスに有効な新しい公開鍵暗号方式として暗号文ポリシー属性ベース暗号（CP-ABE: Ciphertext-Policy Attribute Based Encryption）がある．図 1 は CP-ABE の暗号化の概要を示している．この方式は属性値の論理式（例:人事部 OR (総務部 AND 部長)）で表現されたアクセスポリシーを公開鍵とし，その暗号文はポリシーを満たす属性を有した利用者の秘密鍵でしか復号できなくすることで，きめ細やかなアクセス制御の機能を暗号化処理に付加できる．利用者は鍵発行センター（KGC）に自身の属性が含まれた秘密鍵を発行してもらい，それを適切な認証を経て取得することで閲覧権限があるファイルを復号できるようになる．CP-ABE を用いたファイル共有システムの研究は活発に行われており，研究代表者らもコンテンツだけでなくファイル名/ディレクトリ名までも保護の対象に拡張したファイル共有システムの研究開発を進めてきた**[1]**.

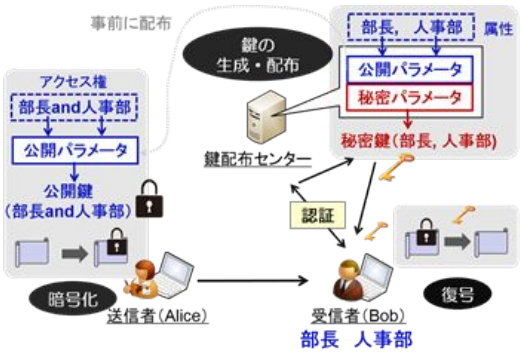

図 1 CP-ABE の処理の概要

２．研究の目的

従来の CP-ABE を用いたファイル共有システムの研究では単一の KGC に所属している利用者間でのファイル共有を目的としたシステムを議論している．しかしながら，KGC は所属している利用者の全ての秘密鍵を生成可能であり権限が強いため，実際の運用では組織外への情報漏えいのリスクを最小限にするために KGC はそれぞれの組織で個別に運用することが考えられる．このような従来の研究では実現が困難な条件においても，例えば共同研究などで組織を超えた利用者のグループでファイルを共有するような利用シーンは存在する．したがって，CP-ABE によるファイル共有の仕組みを複数組織間で相互利用可能とする拡張に関する研究開発は重要な研究課題の一つと考えられる．

本研究では，管理が異なる組織が連携して CP-ABE を用いたファイル共有を実現するために，強い権限を持つ鍵発行センターの影響範囲を組織内に留める連携手法について検討し，その安全性及び有効性について評価することを目的とする．

３．研究の方法

本研究では，所属する KGC が異なる場合でも属性値の論理式で復号権限を制御できる CP-ABE に基づくファイル共有方式について検討する．まず初めに，CP-ABE を用いた既存のファイル共有システムがハイブリッド型の暗号方式を前提としていることから，その暗号化の手順を工夫することで複数の KGC が連携して AND や OR を含むアクセス制御を可能にする方法について検討する．さらに，方式自体が複数の KGC に対応している CP-ABE について調査し，本研究で想定している利用方法に合致するものを選定する．さらに，その方式を実装し性能評価を実施する．

ファイル共有システムを実運用するに当たって課題となる点についても検討する．複数組織に共通した KGC や暗号ソフトウェアを配布して運用できる基盤としてコンテナ型仮想環境（docker）をベースにしたシステムを開発し，性能評価する．さらに，複数の組織が連携してファイル共有をする場合，必要なデータの流通の効率化をするために暗号化ファイルに検索機能も必要となる．暗号化ファイルのまま検索できる技術である検索可能暗号をファイル共有システムに組み込むための基礎的な検討も本研究では実施する．また，ハイブリッド型の暗号化ではコンテンツ本体に対して共通鍵暗号を用いるが，その方式について安全性を評価する手法についても検討する．

４．研究成果

(1) ハイブリッド型暗号化に注目した素朴な方法

図 2 のようにそれぞれ組織が異なる KGC を管理している条件の下で各組織の属性を利用したアクセスポリシーを構成し，それを用いて暗号化する方法について検討した．CP-ABE で暗号化をするとき，属性の文字列だけでなく属性が所属している KGC から公開パラメータを取得する必要がある．図 2 のようなケースでは PKI（公開鍵基盤）の仕組みを

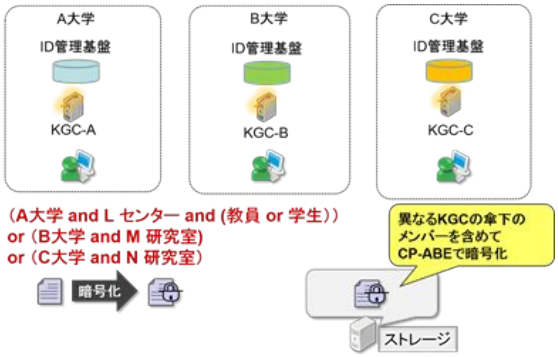

図 2 複数組織での KGC 管理の概要

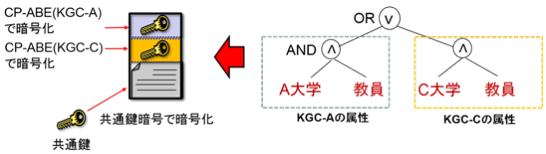

図 3 ハイブリッド型暗号での OR 表現の方法

利用して A 大学，B 大学，C 大学の全ての KGC の公開パラメータを安全に配布する仕組みを提供することで，別の KGC 傘下の利用者のための暗号化を実行できると思われる．しかしながら，それだけでは異なる KGC の利用者のための暗号文を作ることが可能になるだけであり，通常の CP-ABE のような AND や OR を含むような論理式を利用して柔軟に権限を指定できるわけではない．そこで，本研究ではハイブリッド型の暗号化に注目し，その暗号化手順に手を加えることで複数の組織間での CP-ABE 暗号化を実現する方法を検討する．

通常，CP-ABE を用いて巨大なファイルを暗号化する場合は処理速度の向上のためにハイブリッド型の暗号化が用いられる．ハイブリッド暗号化では，ファイル本体を暗号化している共通鍵を取り出せるかどうかを CP-ABE で制御することで属性の有無を表現している．この共通鍵を取り出す部分について工夫をすることで，属性の OR 表現や AND 表現を実現する．まず初めに属性の OR 表現について考える．複数の KGC の属性が混ざった表現で暗号化するとき，前処理として図 3 のように論理式を KGC が共通のものでまとまるように加法標準形(OR の連結)に変換する．さらに，共通鍵を含まれている KGC の数だけ複製し，それぞれを各 KGC についてアクセス権と対応する公開パラメータで暗号化する．最後にこれらの暗号文を共通鍵暗号の暗号文に連結することで，それぞれの組織のユーザは自分に関係する CP-ABE 暗号文から共通鍵を入手し，最終的に平文を得ることができるようになる．図 3 で言えば，KGC-A に属するユーザまたは KGC-C に属するユーザが共通鍵を手に入れることができ，OR 表現が実現できる．

次に同様に AND 表現について実現することを考える．これは複数の組織に所属しているユーザ(例: A 大学の教員であり，B 大学の客員研究員でもある）の権限が対応する．複数の KGC のアクセス権に対応する秘密鍵を全て持っている場合に共通鍵が入手できるようにするためには，素朴な方法として共通鍵をそれぞれのアクセス権の公開鍵で多重暗号化することが挙げられる．上記の例では，共通鍵を B 大学の客員研究員が復号できるように暗号化し，さらにその暗号文を A 大学の教員が復号できるように暗号化する．この方法で AND 表現は実現できるが，結託に関する安全性（結託耐性）に問題が生じてしまう．具体的には，アクセス権の部分木の属性を持つユーザ，たとえば A 大学の教員と B 大学の客員研究員が協力して復号処理をすることで，両方の属性を持つユーザ以外でも共通鍵を復元することができてしまう．以上のようにハイブリッド型の暗号化に注目した素朴な方式では OR 表現は可能であるが，AND 表現に結託耐性が無いことがわかる．A 大学の教員かつ B 大学の客員研究員の属性を持ったユーザだけが属する専用の KGC を用意すれば対応できる可能性もあるが，組み合わせの増加に伴って運用する KGC の数が増加すること，管理主体をどこにするかという問題もあるため，この方法は採用しにくいと考えられる．

(2) 鍵発行機関が複数存在可能な属性ベース暗号

CP-ABE では鍵発行機関が複数存在可能な方式が提案されている．これらの方式は方式自体に結託耐性があるため，(1)で述べた方法の AND 表現のときに問題になった結託攻撃に対して安全性を有している．表 1 は，本研究で調査した方式を以下の 2 つの条件で分類したものである．

① 中央機関の有無

中央機関としての KGC の配下に各機関の KGC を置くような KGC の分散管理を目的とした方式では，中央機関から他の全ての KGC の秘密鍵を生成できるため，本研究課題の目的に合致しない．したがって，中央機関が不必要な方式(De-centralized CP-ABE) を採用する．

② 方式が用いている楕円曲線の位数

複数の鍵発行機関が存在可能な属性ベース暗号は対称ペアリング暗号を用いて実現されている．そのため対称ペアリングを使用するにあたって C 言語のペアリングライブラリ，PBC library を使用している．PBC library でサポートしている楕円曲線は素数位数(prime order) であるため，合成数位数(composite order) の楕円曲線を必要とする方式は既存のライブラリを使用できないという観点から採用しないこととした．

表 1 より，2 つの条件を満たす方式の中から Lewko の方式に注目し，実装・評価をした．Lewko の方式は，システム全体のパラメータを生成する **Global Setup**，新規の KGC がシステムに加入するときに実行される **Authority**

表 1 複数の鍵発行機関が存在可能な属性ベース暗号の分類

	中央機関	楕円曲線の位数
Chase の方式 [2]	必要	Prime
Lewko らの方式 [3]	不必要	Composite
Lewko の方式 [4]	不必要	Prime
岡本らの方式 [5]	不必要	Prime
土田らの方式 [6]	不必要	Prime

表 2 計測結果

	処理時間 [sec]
Global Setup	0.096
Authority Setup	0.606
KeyGen	0.342
Encrypt	0.343
Decrypt	0.410

Setup，ユーザが自身の属性の秘密鍵を取得するときに KGC で実行される **KeyGen**，暗号化や復号の際にユーザが実行する **Encrypt** と **Decrypt** の 5 つアルゴリズムから構成されている．アルゴリズムの詳細は省略する．

本研究では Lewko の方式を C 言語で実装した．ペアリングライブラリは PBC Library (version 0.5.14)を使用し，対称ペアリング用の曲線である Type A curve を用いて実装した．ただし，Type A curve として PBC library で提供されている楕円曲線の位数が 160 ビットで 80 ビット安全性しか有していないため，PairingParameters Generator API を用いて 256 ビット位数の曲線を生成して 128 ビット安全性を確保している．なお，同様にペアリング計算の出力となる拡大体のサイズは 3072 ビットとした．評価実験では，暗号化/復号での平文は拡大体の一つの要素にエンコードする実装にしている．有限体のサイズは 3072 ビットあるため，128 ビットなどの共通鍵を暗号化するには十分であり，ハイブリッド型暗号化の公開鍵部分の処理の評価としては十分であると考えられる．また，実験において KGC の数は 4 とし，それぞれの KGC は 1 つの属性を有しているとして暗号化を行う条件で実験をしている．各 KGC が有している属性を A，B，C，D という文字としたとき暗号化の際のアクセス権は A AND ((B AND C) OR D) と固定し，A AND D のユーザの鍵で復号し実験を行った．この条件のみでは論理演算と処理の関係を示しているとは言えないが，4 種類の KGC の属性が混合されたアクセス権での暗号化が動作すること，および処理が極端に遅くは無いことを確認できると考えている．

CPU を Core i7 3.00GHz，メモリを 64GB とした実験環境において，各アルゴリズムを 100 回実行した平均処理時間を表 2 に示す．KGC を構築したときの処理である Authority Setup やユーザが鍵を取得する処理である KeyGen は 1 秒未満で実行できている．これらは最初に一度のみ実行する処理であるため許容できる処理時間だと考える．暗号化/復号処理である Encrypt や Decrypt は 0.5 秒未満で実行できていることが確認できた．以上のように，Lewko の方式を用いてハイブリッド型の暗号化を実行する場合，現実的な処理時間でファイル共有システムを実現できる可能性があることがわかった．共通鍵暗号部分や通信処理に関する評価は今後の課題とする．

(3) ファイル共有システムを実運用するに当たっての諸検討

本研究のシステムを実運用する際には各機関に KGC を配置して運用する必要がある。そこで，本研究では属性ベース暗号よりシンプルな ID ベース暗号の KGC をコンテナ型仮想環境である docker に基づくネットワーク上に実装し，通信時間を考慮しても現実的な時間で実行可能でかつ各拠点に配布可能であることを確かめた．

さらに，ファイル共有システムの暗号化データを暗号化したままで検索する方式として公開鍵型検索可能暗号(PEKS)について検討し，過去に代表者らが取り組んだファイル共有システム[1]のファイル名/ディレクトリ名管理ファイルに含めることで効率的に検索が可能なこと，PEKS を拡張して複数のキーワードの検索に対応した SCF-MPEKS が現実的な時間で実行可能なことを示した．

また，ハイブリッド型の暗号化においてコンテンツ本体の暗号化に用いる共通鍵ストリーム暗号について，利用を予定している暗号の安全性に関する検討も実施している．

＜引用文献＞

[1] 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.
[2] M. Chase，“Multi-authority Attribute Based Encryption”，Proceedings of TCC 2007，pp. 515-534，2007.
[3] A. Lewko and B. Waters，“Decentralizing attribute-based encryption”，Proceedings of EUROCRYPT 2011，pp. 568-588，2011.
[4] A. Lewko “Functional encryption: new proof techniques and advancing capabilities”，PhD Thesis，2012.
[5] T. Okamoto and K. Takashima，“Decentralized Attribute-Based Signatures”，Proceedings of PKC 2013，pp. 125-142，2013).
[6] 土田 光，金山直樹，西出隆志，岡本栄司，“Non-Programmable ランダムオラクルモデルで安全性証明可能かつ複数の鍵発行機関が存在可能な属性ベース暗号”，信学技報，Vol. 115，No. 502，pp. 197-204，2016.

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計３件）
[1] Tohru KONDO, Hidenobu WATANABE, and Toshihiro OHIGASHI, "Development of the Edge Computing Platform based on Functional Modulation Architecture," Proceedings of COMPSAC Workshops 2017, Fast Abstracts, 査読有, 巻無し, pp. 284-285, IEEE Computer Society, 2017, DOI: 10.1109/COMPSAC.2017.108
[2] Yuhei WATANABE, Takanori ISOBE, Toshihiro OHIGASHI, and Masakatu MORII, "How to Efficiently Exploit Different Types of Biases for Plaintext Recovery of RC4," IEICE Trans. on Fundamentals of Electronics, Comm. and Computer Sciences, 査読有, vol. E100-A, no.3, pp.803-810, 2017, DOI: 10.1587/transfun.E100.A.803
[3] 支強，大東俊博，相原玲二，西村浩二，"クラウドストレージにおける安全な検索機能の実装と評価," 第 17 回 IEEE 広島支部学生シンポジウム論文集，査読有，巻無し，pp.527-532，2015 年 11 月，DOI: なし.

〔学会発表〕（計 10 件）
[1] 柳 宏之，木村隼人，近堂 徹，渡邉英伸，大東俊博，"モジュラー型エッジコンピューティング基盤ためのセキュリティモジュールの実装および評価," 電子情報通信学会 インターネットアーキテクチャ研究会，電子情報通信学会技術研究報告，vol. 117, no. 472, IA2017-76, pp. 91-96, 2018 年.
[2] 石橋拓哉，鈴木達也，伊藤勝彦，大東俊博，相原玲二，"属性ベース暗号を用いたファイル共有サービスの複数組織対応に関する考察," 情報処理学会 IOT 研究会， 情報処理学会研究報告，vol.2018-IOT-40, no.14, 6 pages, 2018 年.
[3] 伊藤勝彦，江村恵太，大東俊博，"複数キーワードをサポートしたセキュアチャネルフリー検索可能暗号の実装評価," 2018 年暗号と情報セキュリティシンポジウム (SCIS2018), 8 pages, 2018 年.
[4] 鈴木達也，江村恵太，木村隼人，大東俊博，"公開検証可能なプライバシー保護時系列データ統計計算の実装評価," 電子情報通信学会情報セキュリティ(ISEC)研究会，電子情報通信学会技術研究報告，vol.117, no.369, pp.43-50, 2017 年.
[5] 棚本清也，大東俊博，"RC4 のバイアス探索に関する一考察," 2017 年電子情報通信学会ソサイエティ大会，A-7, p.63, 2017 年.
[6] Tatsuya SUZUKI, Keita EMURA, Hayato KIMURA, and Toshihiro OHIGASHI, "Implementation Results of Privacy-Preserving and Public Verifiable Data Aggregation Protocols," The 12th International Workshop on Security (IWSEC 2017), poster session, 2017. **(IWSEC 2017 Best Poster Award 受賞)**
[7] Katsuhiko ITO, Keita EMURA, and Toshihiro OHIGASHI, "Implementation Results of an Adaptive Secure Secure-Channel Free Searchable Encryption Scheme with Multiple Keywords," The 12th International Workshop on Security (IWSEC 2017), poster session, 2017.
[8] 城所賢史，五十部孝典，大東俊博，"ストリーム暗号 Grain v1 の出力の鍵依存度に関する考察," 電子情報通信学会情報セキュリティ(ISEC)研究会，電子情報通信学会技術研究報告， vol.116, no.505, pp.1-6, 2017 年. **(電子情報通信学会 情報セキュリティ研究奨励賞 受賞)**
[9] 嶋田健太，大東俊博，"属性ベース暗号を用いたファイル共有システムの高速化の検討," MAT ワークショップ 2016, 2016 年,
[10] 大東俊博，"新世代暗号の応用に関する取り組み," MAT ワークショップ 2016, 2016 年,

６．研究組織
(1)研究代表者
大東　俊博（OHIGASHI, Toshihiro）
東海大学・情報通信学部・准教授
研究者番号：８０５０８１２７