様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　２７　年　　６　月　２０　日現在

機関番号：　１５４０１
研究種目：　若手研究(B)
研究期間：　2013～2014
課題番号：　２５７３００８５

研究課題名（和文）ファイル名/ディレクトリ名を秘匿可能なクラウド向け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 for Cloud Storages with File/Directory Name Encryption

研究代表者

大東　俊博（Ohigashi, Toshihiro）

広島大学・情報メディア教育研究センター・助教

研究者番号：８０５０８１２７

交付決定額（研究期間全体）：（直接経費）　　3,200,000円

研究成果の概要（和文）：クラウド上のオンラインストレージを安全に利用するために，暗号文ポリシー属性ベース暗号を利用してクライアント側でアクセス制御付きの暗号化を行うシステムを研究開発した．本研究では，従来の方式で考慮されていなかったファイル名/ディレクトリ名の情報も秘匿可能とし，なおかつ高速に動作する方式を検討した．さらにプロトタイプを作成して性能評価を行い，提案方式が実用的な時間で実行可能であることを確かめている．

研究成果の概要（英文）：In this research, I proposed a secure file sharing system for cloud storage services with access control by using Ciphertext-Policy Attribute Based Encryption (CP-ABE). The proposed system can protect the contents of files and the file names/directory names, which were not discussed by the past CP-ABE based systems. Moreover, I implemented a prototype system, and evaluated the processing time in order to demonstrate the practicality of the proposed system.

研究分野：　情報セキュリティ

キーワード：　属性ベース暗号　クラウドストレージ　秘密分散法　ストリーム暗号

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ファイル共有の用途にも利用できる．特に自組織にサーバを設置・管理するコストを削減できるため，組織内での会議用ファイルなどの共有を目的とした利用が期待される．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．特に，政治的な理由等によりディスクの検閲が実施できる国に設置されたサーバではその懸念は大きくなる．

サーバ管理者の覗き見を防ぐ方法として，TrueCryptなどのクライアント側でコンテンツを暗号化するシステムが注目されている．しかし，これらは共通鍵暗号や従来の公開鍵暗号を利用するためユーザはファイルを共有するグループの数に応じた鍵を配布・管理することとなり，組織内でのファイル共有などの用途ではコストが大きくなるという問題が生じる．さらに，既存のシステムの多くはコンテンツ本体のみを暗号化の対象とし，ファイル名やディレクトリ名を対象としていない．ファイル名やディレクトリ名はコンテンツの内容を要約する情報が含まれている場合も多く，アクセス権限の無い利用者に知られることは望ましくない．

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．この方式は暗号文に属性値の論理式（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（以下，アクセス権）を埋め込むタイプの公開鍵暗号であり，アクセス権を公開鍵にすることで暗号文を復号できる利用者のグループを任意に設定できる．利用者が管理する秘密鍵の個数は自身の持つ属性の数に依存するため管理する鍵は多くなり難く，組織内でのファイル共有のような共有するグループ数が多くなる場合でも有効となる．このように CP-ABE はクラウド環境において重要な技術であるが，比較的新しい暗号方式であることや方式自体が発展途上であることから，実際のシステムへの応用に関する詳細な検討や運用を想定した性能評価の例は多くなく，さらにファイル名/ディレクトリ名という重要な内容を含み得る情報の秘匿についてほとんど検討されていない．

２．研究の目的

本研究では，ファイル名/ディレクトリ名の秘匿も考慮したクラウド向けファイル共有システムを研究開発し，プロトタイプシステムの実装と実運用を意識した評価を行うことを目的とする．また，提案方式において，安全に保存データの冗長化を実現する仕組みについても検討する．具体的には，以下の内容について取り組む．

（１）　ファイル名/ディレクトリ名を秘匿可能な方式の検討および評価

CP-ABE を用いて，読み取り権限を持つ属性のユーザだけが真のファイル名やディレクトリ名を表示することができるシステムについて検討する．その際，これらの表示が数秒～数十秒程度で終わるような効率的なプロトコルを提案する．また，システム全体の処理時間についても評価し，実用的なシステムであることを示す．

（２）　保存データの冗長化

（１）のシステムでは，CP-ABE によって作られる暗号文はオンラインストレージに保存される．しかしながら，暗号化するのみでは保存したサーバが故障した場合などにデータが失われてしまい，また暗号化だけの処理では法的な理由で保存が許されない場合もある．そこで，閾値秘密分散法を用いることで，保存したデータの冗長化および安全性の向上を実現する．なお，利用する端末はモバイル環境で使用することも想定しているため，端末からの通信量は極力小さく，なおかつ一定の安全性を持つ方式について検討する．

３．研究の方法

（１）　ファイル名/ディレクトリ名を秘匿可能な方式の検討および評価

基本的なアイディアは，真のファイル名をランダムな文字列（仮ファイル名）に置き換え，仮ファイル名と真のファイル名の対応関係を CP-ABE で暗号化することでファイル名の秘匿を実現する．しかしながら，この方法ではファイル名を 1 つ表示するごとに CP-ABE の復号処理を 1 回実行することになり，多数のファイル名を表示するときには膨大な時間が必要となる．例えば，1 回の表示の処理に 0.1 秒を要したとして，10000 個のファイル名を表示するには 1000 秒の時間が必要となってしまう．ここで，研究代表者らは以下の点に注目した．

① CP-ABE と共通鍵暗号を利用したハイブリッド型の暗号化を前提としたとき，小さなデータを何度も暗号化/復号するより，大きなデータにまとめて 1 回暗号化/復号するほうが動作が早くなる．

② 業務の単位が何らかの意味のあるグループ（権限の組み合わせ）となることから，異なる複数のファイルが同一のアクセス権で暗号化されることも多い．

ファイルの総数が多くなった場合でも，上記のグループ数は比較的少なく抑えられると考えられるため，同じアクセス権を持つファイル名をまとめて一つのファイルで管理するようにすれば，暗号化/復号処理の呼び出し回数を減らすことができ，高速化が期待できる．

さらに，ファイル名だけでなく，ディレクトリ名およびディレクトリ間のリンク構造などメタ情報をまとめてリストファイルという単位で管理し，それを CP-ABE で暗号化して表示を制御するようにした．こうすることで，複数のオンラインストレージに分散配置することができることや，表示範囲をディレクトリ内のファイル名だけに抑えられるため 1 回の表示あたりに通信するデータサイズを小さくできることなどの利点が生じる．

このようなリストファイルを複数人で利用する場合，リストファイルに登録するファイル名やディレクトリ名の編集権限を制御する仕組みが必要となる．研究代表者らは，この制御を担う特別なサーバ（アップロードマネージャ）を定義し，それらにメタ情報の管理のみ実行できる限定的な権限を与えることにした．

（2） 保存データの冗長化

CP-ABE で暗号化したデータを保存する際にデータに安全性と冗長性を与えるために秘密分散法を導入することを検討した．特に高速性に優れた方式として XOR 演算に基づく秘密分散法（以下，XOR-SSS と呼ぶ）に注目し，それらを用いて分散して保存することができるようにリストファイルの構造を修正している．

XOR-SSS は高速に動作して安全性も高いが，データサイズが分割数倍になるという欠点がある．これはモバイル環境など通信環境が悪い場合に顕著になる．そこで，クラウド上に設置した Semi Trusted な分散用サーバで秘密分散法を代理で実行するシステムを検討した．ここで，Semi Trusted のモデルでは，管理者はデータの内容を覗くかもしれないが，プロトコルどおりの作業は正しく行うことを仮定している．このように分散用サーバを用いると，モバイル端末からの通信量は元のデータと同程度に抑えることができ，その代わりに分散用サーバからストレージに保存する際に通信量が増えることになる．分散用サーバ・ストレージ間は有線接続された潤沢なネットワーク資源があると想定できるため，上記の通信量の増加の影響は大きくないと考えられる．

このような構成にすればモバイル環境からの通信量は削減できるが，分散用サーバに平文がそのまま渡ってしまうため，サーバ管理者が覗き見をするような状況では必ずしも安全とは言えない．そこで，モバイル端末から分散用サーバにデータ渡すときに事前に暗号化処理を行うことで一定の安全性を与えることを考える．しかしながら，単純に暗号化をするだけでは，復元時に暗号化に用いた鍵を保持しておく必要があるため，その管理が繁雑になってしまう．そこで，秘密鍵によって生成した擬似乱数列と平文を XOR 演算することで暗号化できるストリーム暗号を暗号化アルゴリズムに利用することを考える．ストリーム暗号と XOR-SSS は両方とも XOR 演算によって動作するため，暗号化データを秘密分散法で分散したときのデータに対して秘密鍵の情報を使った操作を加えることで，分散データを元に戻さなくても暗号化の効果をキャンセルできるようになる．この性質を使って，分散用サーバで作業するときだけ暗号化されており，ストレージに保存するときには暗号化の効果が解除される，すなわち鍵の管理が不要になる方式が実現できる．

提案する方式ではストリーム暗号を利用する．そこでストリーム暗号として業界標準として使われている RC4 暗号がどのような状況で安全に使用できるかについても検討する．RC4 は FSE2013 で提案された Isobe らの攻撃によって broadcast setting と呼ばれる使い方では安全でないことが示されていた．しかしながら，生成する擬似乱数列の先頭の 3072 バイトを使わずに捨てれば安全になるという実装が知られており，その実装には Isobe らの攻撃は有効ではなかった．

研究代表者らは，FSE2000 で Fluhrer らが発見した擬似乱数列の統計的な偏り(bias)と EUROCRYPT2005 で Mantin が発見した擬似乱数列の bias をそれぞれ補うように組み合わせることで安全と言われていた実装でも攻撃できる方法を考案した．さらに，AlFardan らが USENIX Security symposium 2013 で提案した方法を参考に，上記の攻撃の性能を改善する方法も与えている．

4．研究成果

（1） ファイル名/ディレクトリ名を秘匿可能な方式の検討および評価

3．（1）で述べたアイディアに基づき CP-ABE を用いてファイル名/ディレクトリ名の表示を制御するシステム（図 1）について具体的な処理を検討し，それを実装したプロトタイプを開発した．さらに，複数のリストファイルによって表現されたディレクトリ構造が正しく表示・更新でき，妥当な速度で動作するかについて実証実験を行っている．

実験環境として，ストレージはクラウドサービスである Dropbox と研究代表者が設置したローカルストレージ（WebDAV で構築）を利用した．システムを構成するサーバ，クライアント，ネットワーク等の機器は一般的な性能のものを用いて構築している．さらにシステムが前提とするノード間の HTTPS 通信および利用者/属性認証は一般的な方式を利用して処理速度を計測した．

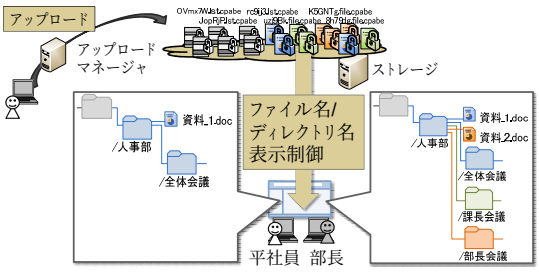

図１　ファイル名/ディレクトリ名を秘匿可能なファイル共有システム

実験では，リストファイルをダウンロード・復号することでファイル名/ディレクトリ名を表示する処理の時間，ファイルをアップロードしてリストファイルにファイル名を追加する処理の時間を計測した．ここで，リストファイルのサイズと登録されたファイル名/ディレクトリ名の関係は，100KB（200 個），1MB（2000 個），10MB（20000 個）のように設定し，リストファイルに登録されたファイル名/ディレクトリ名は 10 種類のアクセス権のグループに均等に分割されているものとしている．

リストファイルの全てのファイル名/ディレクトリ名を表示する時間と 1 つのファイルをアップロードしてリストファイルに登録するまでの時間について，保存先のストレージを dropbox にした場合とローカルストレージにした場合の実験結果をぞれぞれ表 1，表 2 に示す．

表１　dropbox を利用した場合の処理時間（単位：秒）

リストファイルのサイズ	100KB	1MB	10MB
ファイル名/ディレクトリ名表示時間	2.07	4.99	16.53
ファイルのアップロード時間	10.68	15.82	41.36

表２　ローカルストレージを利用した場合の処理時間（単位：秒）

リストファイルのサイズ	100KB	1MB	10MB
ファイル名/ディレクトリ名表示時間	0.20	0.30	0.89
ファイルのアップロード時間	2.95	2.99	3.39

表 1 より，提案システムで 2000 個のファイル名（1MB のリストファイル）を dropbox でも約 5 秒で表示でき，さらにレスポンスが良いローカルストレージを用いた場合には 0.3 秒まで短縮でき，現実的に利用可能な速度で動作することがわかった．ローカルストレージでは 20000 個のファイル名（10MB のリストファイル）でも 1 秒未満で実行できているなど，全体の処理時間の中でストレージとの通信時間が支配的になる傾向にある．表 2 は，ファイルのアップロード処理に関する処理時間であるが，ファイル名/ディレクトリ名の表示に要する時間と比べて数倍以上時間を必要とすることがわかる．しかしながら，現実的には待つことが出来ない時間ではないため，例えばペーパレス会議などで事前にファイルをアップロードして，会議の際に一斉にファイルをダウンロードするような使い方では大きな問題とはならないと考える．なお，アップロード処理は複数のサーバを利用して処理を分散させられるように設計しているため，コストをかけることで安定した処理時間を確保することは可能となる．これらの研究成果によって，ファイル名/ディレクトリ名を秘匿する仕組みを入れたとしても，現実的なシステムで提案方式が利用可能であることを示すことができた．

（２）　保存データの冗長化

３．（２）で述べたアイディアに基づき XOR-SSS とストリーム暗号を組み合わせた方式を認証や通信路暗号化の処理を含めて実装した．その結果，32MB のデータを秘密分散法により分散保存するとき，分散用サーバを利用しない方法では端末側の処理が 30 秒必要だったのに対し，提案手法は 10 秒まで短縮できることがわかった．また，分散用サーバを利用することで全体の処理時間が増加すると思われたが，分散用サーバ・ストレージ間の回線速度の速さや分散用サーバの計算性能を比較的良いものを仮定できることから，ほとんど変わらない時間でストレージまでデータが保存されることを確認している．　この方式を図 1 のシステムと統合することは今後の課題とする．

ストリーム暗号 RC4 の安全性については，３．（２）で述べた 2 つの bias を用いる方法によって，たとえ擬似乱数列の先頭の 3072 バイトを捨てたとしても broadcast setting で送信された 2^{35} 個の暗号文から元の平文を確率 1 で復元できることが明らかになった．さらに，AlFardan らの方法に似た改良を施すことで，平文の復元に必要な暗号文数を更に 1/2 に減らせることも明らかにしている．これらの安全性解析の成果は本課題以外にも，日本国の電子政府用暗号リストの策定の際に参考にされ，その社会的な影響は大きい．

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 5 件）

[1] Toshihiro OHIGASHI, Takanori ISOBE, Yuhei WATANABE, and Masakatu MORII, "Full Plaintext Recovery Attacks on RC4 using Multiple Biases," IEICE Trans. on Fundamentals of Electronics, Comm. and Computer Sciences, 査読有, vol.E98-A,

no.1, pp.81-91, Jan. 2015, DOI: 10.1587/transfun.E98.A.81.
[2] Toshihiro OHIGASHI, Takanori ISOBE, Yuhei WATANABE, and Masakatu MORII, "How to Recover Any Byte of Plaintext on RC4," Proceedings of Selected Areas in Cryptography 2013 (SAC 2013), 査読有, 巻無し, LNCS 8282, pp. 155-173, Springer-Verlag, 2014, DOI: 10.1007/978-3-662-43414-7 8.
[3] Toshihiro OHIGASHI, Kouta YOSHIDA, Kouji NISHIMURA, and Reiji AIBARA, "Implementation and Evaluation of Secure Outsourcing Scheme for Secret Sharing Scheme on Cloud Storage Services," Proceedings of the 2014 IEEE 38th Annual International Computers, Software and Applications Conference Workshops (COMPSAC Workshops 2014), ADMNET 2014, 査読有, 巻無し, pp. 78-83, 2014, DOI: 10.1109/COMPSACW.2014.17.
[4] 吉田耕太, 西村浩二, 大東俊博, 相原玲二, "秘密分散法を利用したクラウドストレージサービスにおけるモバイル機器を考慮した安全な処理委託方式," 情報処理学会論文誌, 査読有, vol.55, no.3, pp.1117-1125, 2014年3月, ISSN:1882-7764.
[5] 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, 査読有, vol.55, no.3, pp.1126-1139, 2014年3月, ISSN:1882-7764.

〔学会発表〕(計10件)
[1] 大東俊博, "RC4 に関する一連の攻撃," Small-workshop on Communications between Academia and Industry for Security (SCAIS), 2015年1月19日, 福岡県福岡市.
[2] 大東俊博, 渡辺優平, 森井昌克, "RC4に対する平文回復攻撃の改良," CSS2014 (Computer Security Symposium 2014), vol.2014, no.2, 8 pages, CD-ROM, 2014年10月, 北海道札幌市. **(CSS2014 優秀論文賞受賞)**
[3] 大東俊博, 五十部孝典, 渡辺優平, 野島良, 森井昌克, "SSL/TLSのRC4へのActive Attack," 電子情報通信学会技術研究報告, 情報通信システムセキュリティ(ICSS)研究会, vol.113, no.502, ICSS2013-63, pp.7-12, 2014年3月, 沖縄県名護市. **(ICSS2013年度研究賞 受賞)**
[4] 渡辺優平, 大東俊博, 森井昌克, "SSL/TLSでのRC4に対する平文回復攻撃の改良," 2014 年暗号と情報セキュリティシンポジウム(SCIS2014), 7 pages, CD-ROM, 2014年1月, 鹿児島県鹿児島市.
[5] Kouta YOSHIDA, Kouji NISHIMURA, Toshihiro OHIGASHI, and Reiji AIBARA, "Implementation and Evaluation of Secure Outsourcing Scheme for Cloud Storage Services using Secret Sharing Scheme," The 8th International Workshop on Security (IWSEC 2013), poster session, Nov. 18-20, 2013, 沖縄県那覇市.
[6] 吉田耕太, 西村浩二, 大東俊博, 相原玲二, "秘密分散法を利用したクラウドストレージサービスのための安全な処理委託方式の実装と評価," CSS2013 (Computer Security Symposium 2013), vol.2013, no.4, 8 pages, CD-ROM, 2013年10月, 香川県高松市.
[7] 大東俊博, "共通鍵ストリーム暗号 RC4の安全性評価の現状について", 2013 年電子情報通信学会ソサイエティ大会 依頼シンポジウム (AI-1. 暗号研究の現状とブレークスルーに向けて), AI-1-2, 2013年9月17日, 福岡県北九州市. **(招待講演)**

[8] 大東俊博, "属性ベース暗号を用いたセキュアオンラインストレージシステムの開発について," 次世代セキュア情報基盤ワークショップ, 2013年8月29日, 広島県東広島市.
[9] 吉田耕太, 西村浩二, 大東俊博, 相原玲二, "秘密分散法を利用したクラウドストレージサービスのための安全な処理委託方式," 情報処理学会研究報告, vol.2013-IOT-22, no.15, pp.1-6, 2013年8月, 東京都練馬区.
[10] Yuhei WATANABE, Takanori ISOBE, Toshihiro OHIGASHI, and Masakatu MORII, "Vulnerability of RC4 in SSL/TLS," 電子情報通信学会技術研究報告, 情報通信システムセキュリティ(ICSS)研究会, vol.113, no.95, ICSS2013-4, pp.19-24, 2013年6月, 新潟県長岡市.

６．研究組織
(1)研究代表者
大東　俊博　(OHIGASHI TOSHIHIRO)
広島大学・情報メディア教育研究センター・助教
研究者番号：８０５０８１２７