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 ２８ 年　 ６ 月　 ２ 日現在

機関番号：１４５０１
研究種目：基盤研究(C)（一般）
研究期間：2013～2015
課題番号：２５３３０１５１

研究課題名（和文）利用者主導で開示先制御可能なデータ共有プラットフォームに関する研究

研究課題名（英文）Study on User Controllable Data Sharing

研究代表者
白石　善明（Shiraishi, Yoshiaki）

神戸大学・工学（系）研究科（研究院）・准教授

研究者番号：７０３５１５６７

交付決定額（研究期間全体）：（直接経費）　　3,800,000円

研究成果の概要（和文）：サイバー空間に蓄積されるパーソナル情報を活用した新たなサービスの出現による市場の創出が期待されている。利用者が安心してパーソナル情報を提供するために、利用者主導で開示先の制御ができ、セキュアに情報を流通させる技術の開発は必要不可欠である。本研究では、このようなデータ共有プラットフォームをパーソナル情報を保管する主体の導入により実現することを目指し、利用者とサービス提供者の間のデータ流通を安心して行える要素技術の開発を行った。

研究成果の概要（英文）：Market creation by the appearance of new services that utilized personal information stored in the Cyberspace is expected. One of important issues is to provide secure information sharing platform. This research proposes the three components for secure information sharing; a cryptographic cloud storage by attribute-based encryption, a keyword searchable encryption, and a fair exchange protocol.

研究分野：情報通信システムセキュリティ

キーワード：情報流通　プライバシー保護　アクセス制御　ネットワーク　利用者心理

１．研究開始当初の背景

実世界における人や物の行動や環境などの情報を携帯端末やセンサーにより収集し、実世界の状況を分析し、自律的に利用者に対してサービスを提供するようなコンピューティング環境の構築には、サービス利用者からパーソナル情報を提供してもらわなければならない。サイバー空間に蓄積されるパーソナル情報を活用した新たなサービスの出現による市場の創出が期待される中で、利用者の個人情報の悪用等に対する不安や、プライバシーが侵害されることに対する懸念が高まってきている。

自己情報コントロールができれば利用者のプライバシー懸念を緩和、払拭できる可能性がある。自己情報コントロールとは、利用者の意思に応じてパーソナル情報の開示先が制御できることである。パーソナル情報保管者にデータを預ける際の利用者の懸念事項は、(1)パーソナル情報保管者の閲覧、(2)第三者によるパーソナル情報の不正な入手、(3)パーソナル情報の不正な二次利用であり、これらを解消するシステムが必要となる。

また、パーソナル情報を登録する利用者は、安心してパーソナル情報を提供できるかどうかについて、技術がいかに優れているかということだけで判断はしていないと考えられる。利用者が安心して使えるデータ共有プラットフォームの構築にあたっては、ポリシ制御が適切に行える技術の開発だけではなく、利用者の心理面を考慮する必要がある。

２．研究の目的

本研究では、利用者が安心してパーソナル情報を提供するために、主に二つの研究項目を設定する。

1. 利用者主導で開示先制御ができるデータ共有方式の開発
2. データ共有プラットフォームに対する安心感の要因の分析

まず、利用者主導で開示先制御が可能なデータ共有プラットフォームを、パーソナル情報を保管する主体の存在するモデルで実現することを目指し、利用者とサービス提供者の間、異なるサービス提供者の間でデータ共有を安心して行える要素技術の開発を行う。

そして、データ共有プラットフォームにパーソナル情報を提供する利用者の安心感を高めるためにサービス開発者やサービス運用者が留意すべき点を明らかにするために、開発者だけでなく利用者も気づいていない心理的な要素を導出する。

３．研究の方法

本研究では、(1)パーソナル情報保管者はデータの閲覧ができない、(2)開示許可のない者はデータを利用できない、(3)利用許可の無い者に対するデータの二次利用の防止あるいは抑止がなされる、以上の 3 つの要件を満たすデータ共有方式を実装するための要素技術を開発する。(1)および(2)については、Cryptographic Cloud Storage の構成により、(3)についてはデータの確実な受け渡しと適切なログ保管により満たすことを考える。

また、パーソナル情報を登録する利用者の安心感について心理学的に分析する。

４．研究成果

Cryptographic Cloud Storage に保存した共有データのアクセス制御に適した暗号として、暗号文ポリシ属性ベース暗号（Ciphertext-Policy Attribute-Based Encryption: CP-ABE）がある。CP-ABE では、秘密鍵に関連付けられている属性集合が、暗号文に関連付けられているアクセス構造を満たす場合にのみ、その秘密鍵によって暗号文を復号することができる。属性ベース暗号ではユーザの属性を失効させるには、そのユーザが暗号文を復号できないようにしなければならない。効率良くユーザの属性を失効させることができる CP-ABE の提案がなされているが、属性失効ユーザに対する厳密な安全性証明は与えられていない、もしくは、強い仮定のモデルのもとで証明されている。本研究では、前方秘匿性（Forward Secrecy）を満たす属性失効機能付き属性ベース暗号を提案している。属性ベース暗号における前方秘匿性は、一度属性を失効したユーザはそこから先は暗号文を復号できないことを意味する。提案方式は不正ユーザ、データ保管者、属性失効ユーザの攻撃に対して、標準モデルのもと Decisional Bilinear Diffie-Hellman（DBDH）仮定において選択平文攻撃（Chosen-Plaintext Attack）に識別不可能性（Indistinguishability）を持つという IND-CPA 安全であることを証明している。

Cryptographic Cloud Storage において、ファイル名などのデータを検索するための情報が平文であると、不要に情報が漏れることがある。公開鍵暗号系の検索可能暗号（Public Key Encryption with Keyword Search, PEKS）がある。PEKS では秘密鍵を持つ一人だけがサーバに検索に関して何も情報を漏らすことなく暗号化されたキーワードを検索することができる。ID ベース暗号（Identity-Based Encryption, IBE）方式から PEKS 方式の構成がすでに示されている。IBE 方式では暗号文を復号できる受信者は、暗号化の際にメールアドレスなどの ID によって指定される。PEKS と IBE のコンセプトを結びつけて ID ベース検索可能暗号（Identity-Based Encryption with Keyword Search, IBEKS）が提案されている。例えば暗号文を復号できる受信者を、受信者の持つ属性の条件で指定できる属性ベース暗号（Attribute-Based Encryption, ABE）などの関数型暗号をベースにして検索可能暗号を構成すれば柔軟なアクセス制御が可能となるが、その一方で構成が複雑になるために計算コストは高くなる。IBEKS では暗号文の検索者を ID によって指定する単純なア

クセス制御しかできないが、構成が単純なためにその計算コストは他の検索可能暗号方式に比べて低くなる。モバイルアプリなどで検索可能暗号を使い、単純なアクセス制御を実現したい状況があれば、低コストな IBE で検索可能暗号を実現する方が適している場合があると言える。本研究では、匿名性を持つ階層型 ID ベース暗号（Anonymous Hierarchical IBE, A-HIBE）より計算コストの低い匿名性を持たない HIBE（Non-Anonymous HIBE, NA-HIBE）を変換元にして，より低コストで実現される IBEKS を構成した.

データの確実な受け渡しを実現するために、本研究では公平な交換プロトコル（Fair Exchange Protocol）に着目している。公平な交換とは、互いに目的のものを手に入れるか、どちらも手に入らないことを保証した交換である。特に、署名と署名の交換は Contract Signing（CS)、メッセージと署名の交換は Certified Email（CEM）と呼ばれる。慣例的に任意のメッセージを Email と称している。ネットワーク上で公平な交換を実現するためのアプローチには、二者だけで行う段階的秘密交換と信頼できる第三者（Trusted Third Party: TTP）を利用する交換があり、公平性や効率性の観点から TTP を利用する交換が実用的である。TTP を利用する交換には TTP の利用方法について二種類のタイプがあり、必ず TTP が通信に介入するタイプを On-line 型、不公平な状況になった場合にのみ TTP を利用するタイプを Optimistic 型という。Optimistic 型は On-line 型に比べて通信のボトルネックや TTP 依存が軽減できるという点で優れている。多くの二者間の公平交換プロトコルが提案されている一方で、アプリケーションの種類によっては三者以上の参加者が交換に参加したい場面がある。これまでにいくつかのトポロジ上で動作する多者間公平交換プロトコルが提案されている。本研究では線形トポロジ上の多者間 CEM プロトコルを提案している。提案方式は検証可能暗号化署名方式（Verifiable Encrypted Signature Scheme）をもとにした 4 回交換の二者間 CEM プロトコルを拡張したものである。メッシュ型トポロジの方式を線形トポロジで利用したときの通信コストよりも効率がよいことを示している。

パーソナル情報を登録する利用者の安心感について、質問紙調査と因子分析を行った。その結果、“ 能力・知識因子 ”、“ ユーザビリティ・プリファレンス因子 ”、“ 身近な他者因子 ”、“ 主観的な信用因子 ”、“ 安全性因子 ” の 5 因子が抽出された。抽出された因子は、先行研究の因子と異なり、対象の評判やうわさ、家族や友人などの身近な他者とともに登録することが安心感の要因になることがわかった。また、共分散構造分析の結果から、安心感の因子が “ 論理的要因 ”、“ 主観的要因 ” の 2 つに分かれるという構造が解釈できた。このことから、論理的要因と主観的要因の両方の内容を備えていることが安心感につながると考えられる。

５．主な発表論文等

〔雑誌論文〕（計　７件）

1. M. Sato, M. Mohri, H. Doi, Y. Shiraishi, "Partially Doubly-Encrypted Identity-Based Encryption Constructed from a Certain Scheme for Content Centric Networking", Journal of Information Processing, Vol.24, No.1, pp.2-8, Jan. 2016. （査読有）DOI: 10.2197/ipsjjip.24.2
2. K. Tomida, H. Doi, M. Mohri, Y. Shiraishi, "Ciphertext Divided Anonymous HIBE and Its Transformation to Identity-Based Encryption with Keyword Search," Journal of Information Processing, Vol.23, No.5, pp.562-569, Sep. 2015. （査読有） DOI: 10.2197/ipsjjip.23.562
3. T. Naruse, M. Mohri, Y. Shiraishi, “Provably secure attribute-based encryption with attribute revocation and grant function using proxy re-encryption and attribute key for updating,” Human-centric Computing and Information Sciences, Vol.5, No.8, 2015. （査読有） DOI: 10.1186/s13673-015-0027-0
4. 奥村 香保里，毛利 公美，白石 善明，岩田 彰，“ 情報システム・サービスの利用者の安心感と納得感の要因に関する調査 ”，情報処理学会論文誌，第 56 巻，第 3 号，pp.932-941，2015 年.（査読有）http://id.nii.ac.jp/1001/00122975/
5. M. Sato, M. Mohri, H. Doi, Y. Shiraishi, “Ciphertext Diverge-Merge Scheme of Identity-Based Encryption for Cloud-Based File Transmission Service,” International Journal of Digital Information and Wireless Communications, Vol.5, No.1, pp.52-59, 2015. （査読有） DOI: 10.17781/P001618
6. 成瀬 猛，毛利 公美，白石 善明，“ 前方秘匿性を満たす属性失効機能付き属性ベース暗号 ”，情報処理学会論文誌，第 55 巻，第 10 号，pp.2256-2264，2014 年 （査読有） http://id.nii.ac.jp/1001/00106365/
7. 奥村 香保里，毛利 公美，白石 善明，岩田 彰，“ プライバシー情報を登録する利用者の安心感の要因に関する調査 ”，情報処理学会論文誌，第 55 巻，第 9 号，pp.2159-2167，2014 年（査読有）http://id.nii.ac.jp/1001/00103089/

〔学会発表〕（計　２５件）

1. K. Isobe, M. Mohri, Y. Shiraishi, "A Build Signature-based Pre-Shared Key Exchange for Cyber-Physical Systems", IEICE Technical Report (Information Communication System Security), ICSS2015-69, pp.135-140, March 2016, Kyoto University (Kyoto・Kyoto)
2. Y. Kitamura, M. Mohri, Y. Shiraishi, "Storage-Efficient Packet Classification for Resource-Constrained Devices", IEICE Technical Report (Information Communication System Security), ICSS2015-49, pp.13-18, March 2016, Kyoto University (Kyoto・Kyoto)
3. K. Nomura, M. Mohri, Y. Shiraishi, M. Morii, "Attribute Revocable Attribute-Based Encryption for Decentralized Disruption-Tolerant Military Networks," Third International Symposium on Computing and Networking, pp.491-494, Dec. 2015, Sapporo Business Innovation Center (Hokkaido・Sapporo).
4. Y. Kitamura, M. Mohri, Y. Shiraishi and A. Iwata, "Storage-Efficient Tree Strucure with Level-Ordered Unary Degree sequence for Packet Classification," Third International Symposium on Computing and Networking, pp.487-490, Dec. 2015, Sapporo Business Innovation Center (Hokkaido・Sapporo).
5. Y. Shiraishi, M. Mohri, H. Miyazaki, M. Morii, "A Three-Party Optimistic Certified Email Protocol Using Verifiably Encrypted Signature Scheme for Line Topology," The 2nd IEEE International Conference on Cyber Security and Cloud Computing, pp.260-265, Nov. 2015, New York Institute of Technology(New York・USA).
6. 白石 善明，中井 敏晴，毛利 公美，福田 洋治，廣友 雅徳，森井 昌克，“長期追跡研究のための複数機関にある匿名化データの共有におけるセキュリティ対策の検討”，第 14 回情報科学技術フォーラム，第 4 巻，pp.61-64，2015 年 9 月，愛媛大学（愛媛県・松山市）.
7. 野村 健太，毛利 公美，白石 善明，森井 昌克，“ミリタリーネットワークのための前方秘匿性を満たす属性失効機能付き属性ベース暗号”，情報処理学会マルチメディア，分散，協調とモバイル（DICOMO2015）シンポジウム，pp.1589-1599，2015 年 7 月，ホテル安比グランド（岩手県・八幡平市）.
8. 福田 洋治，白石 善明，廣友 雅徳，毛利 公美，“クラウド型の情報システムの間接利用の不安因子について”，電子情報通信学会 情報通信システムセキュリティ研究会，ICSS2015-34, pp.143-149, 2015 年 7 月，名古屋市中小企業振興会館（愛知県・名古屋市）.
9. 奥村 香保里，毛利 公美，白石 善明，岩田 彰，“情報システム・サービスの利用者の利用意図による安心感・納得感・利用意図の関係について”，電子情報通信学会 ライフインテリジェンスとオフィス情報システム研究会，LOIS2014-82，pp.123-128，2015 年 3 月，沖縄科学技術大学院大学（沖縄県・国頭郡恩納村）.
10. 磯部 光平，毛利 公美，白石 善明，岩田 彰，“即時認証機能付きセッション鍵交換と視聴覚メディアの効果”，電子情報通信学会 ライフインテリジェンスとオフィス情報システム研究会，LOIS2014-62，pp.7-12，2015 年 3 月，沖縄科学技術大学院大学（沖縄県・国頭郡恩納村）.
11. T. Naruse, M. Mohri, Y. Shiraishi, “Attribute Revocable Attribute-Based Encryption with Forward Secrecy for Fine-Grained Access Control of Shared Data”, IEICE Technical Report (Information Communication System Security), ICSS2014-93, pp.181-186, March 2015, Meio University (Okinawa・Nago).
12. K. Tomida, H. Doi, M. Mohri, Y. Shiraishi, “A Transformation from Attribute-based Encryption to Associative Searchable Encryption by Using Hash Function”, IEICE Technical Report (Information Communication System Security), ICSS2014-92, pp.175-179, March 2015, Meio University (Okinawa・Nago)
13. M. Sato, M. Mohri, H. Doi, Y. Shiraishi, “Partially Doubly-Encrypted Identity-Based Encryption for Content Centric Networking”, IEICE Technical Report (Information Communication System Security), ICSS2014-91, pp.169-174, March 2015, Meio University (Okinawa・Nago).
14. H. Miyazaki, M. Mohri, Y. Shiraishi, “A Multi-Party Optimistic Certified Email Protocol Using Verifiably Encrypted Signature Scheme For Line Topology”, IEICE Technical Report (Information Communication System Security), ICSS2014-86, pp.139-144, March 2015, Meio University(, Okinawa・Nago).

15. 奥村 香保里, 毛利 公美, 白石 善明, 岩田 彰, “情報システム・サービスの利用者の利用意図による安心感・納得感の関係について”, 電子情報通信学会 暗号と情報セキュリティシンポジウム（SCIS2015）, 4D1-2, 2015 年 1 月, リーガロイヤルホテル小倉（福岡県・北九州市）.
16. 奥村 香保里, 毛利 公美, 白石 善明, 岩田 彰, “情報システム・サービスの利用者の安心感・納得感・利用意図の関係について”, 情報処理学会 コンピュータセキュリティシンポジウム（CSS2014）, pp.1222-1229, 3A4-2, 2014 年 10 月, 札幌コンベンションセンター（北海道・札幌市）.
17. 冨田 幸嗣, 土井 洋, 毛利 公美, 白石 善明, “暗号文分割型の ID ベース検索可能暗号の構成”, 情報処理学会 コンピュータセキュリティシンポジウム（CSS2014）, pp.551-558, 2E2-4, 2014 年 10 月, 札幌コンベンションセンター（北海道・札幌市）.
18. 奥村 香保里, 毛利 公美, 白石 善明, 岩田 彰, “情報システム・サービスの利用者の安心感と納得感の関係について”, 情報処理学会 セキュリティ心理学とトラスト研究会, 2014-SPT-10(29), 2014 年 7 月, サン・リフレ函館（北海道・函館市）.
19. 奥村 香保里, 毛利 公美, 白石 善明, 岩田 彰, “情報システム・サービスの利用者の安心感と納得感に関する調査”, 情報処理学会 セキュリティ心理学とトラスト研究会, 2014-SPT-8(16), 2014 年 3 月, 名桜大学（沖縄県・名護市）.
20. 宮嵜 仁志, 毛利 公美, 土井 洋, 白石 善明, 岩田 彰, “ID ベース暗号と ID ベース署名を用いた配達証明付きデータ送信の一般的な構成”, 電子情報通信学会 情報通信システムセキュリティ研究会, ICSS2013-65, pp.19-24, 2014 年 3 月, 名桜大学（沖縄県・名護市）.
21. M. Sato, M. Mohri, H. Doi, Y. Shiraishi, “Doubly Encrypted Identity-Based Encryption for File Transfer Service”, The 8th International Conference on Future Information Technology, Lecture Notes in Electrical Engineering, No.276, pp.139-144, Sept. 2013 (Gwanju・Korea).
22. T. Naruse, M. Mohri, Y. Shiraishi, ``Attribute-Based Encryption with Attribute Revocation and Grant Function Using Proxy Re-encryption and Attribute Key for Updating”, The 8th International Conference on Future Information Technology, Lecture Notes in Electrical Engineering, No.276, pp.119-125, Sept. 2013 (Gwanju・Korea).
23. K. Tomida, M. Mohri, Y. Shiraishi, ``Keyword Searchable Encryption with Access Control from a Certain Identity-Based Encryption”, The 8th International Conference on Future Information Technology, Lecture Notes in Electrical Engineering, No.276, pp.113-118, Sept. 2013(Gwanju・Korea).
24. 奥村 香保里, 白石 善明, 岩田 彰, “プライバシー情報を登録する利用者の安心感の要因に関する調査”, 情報処理学会 マルチメディア, 分散, 協調とモバイル（DICOMO2013）シンポジウム, pp.858-864, 4A-2, 2013 年 7 月, 十勝川温泉 ホテル大平原（北海道河東郡音更町）.
25. 宮嵜 仁志, 毛利 公美, 白石 善明, “暗号プロトコルの実装を支援するためのアプリケーションフレームワーク”, 情報処理学会 マルチメディア, 分散, 協調とモバイル（DICOMO2013）シンポジウム, pp.264-270, 2B-1, 2013 年 7 月, 十勝川温泉 ホテル大平原（北海道河東郡音更町）.

６．研究組織

(1)研究代表者

白石　善明（SHIRAISHI　YOSHIAKI）
神戸大学・工学研究科・准教授
研究者番号：７０３５１５６７