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　２９　年　　９　月　２２　日現在

機関番号：　１２１０２
研究種目：　基盤研究(C)（一般）
研究期間：　2014～2016
課題番号：　２６３３０１５１

研究課題名（和文）機密データの漏洩防止と安全利用を同時に実現する暗号技術の確立

研究課題名（英文）Cryptographic Techniques for Both Protecting and Utilizing Confidential Data

研究代表者
西出　隆志（NISHIDE, Takashi）

筑波大学・システム情報系・准教授

研究者番号：７０５７０９８５

交付決定額（研究期間全体）：（直接経費）　　3,700,000円

研究成果の概要（和文）：システム設備の管理をクラウド環境へアウトソースすることによって利便性を得られる反面，機密データのアウトソースにおいては漏洩の危険が発生する。そのためデータの漏洩防止と安全利用を同時に実現することが重要な研究課題となる。
しかし暗号技術を単純に用いるだけではクラウド環境に対してデータ処理を効率的にアウトソースすることが難しくなる。
本プロジェクトでは機密データのアウトソースにおいて漏洩の危険性を排除しつつ，有効活用を可能とする暗号技術の確立に取り組んだ。

研究成果の概要（英文）：By utilizing cloud environments, we can outsource computer system maintenance, but simultaneously we encounter the risk of disclosing confidential data. Thus it is important to realize countermeasures against such a threat. However, employing encryption techniques simply prevents outsourcing of computation on confidential data.
In this project, we worked on developing cryptographic techniques by which we can outsource and utilize confidential data simultaneously.

研究分野：　暗号技術

キーワード：　暗号

１．研究開始当初の背景

クラウドコンピューティング環境を利用して情報システムの管理メンテナンスを外部へアウトソースする運用形態はコスト削減の手段として有効だと考えられている。しかしクラウドコンピューティングにおいてはインターネット利用が前提となり，情報をどこからでもアクセスできる利便性とともにデータ漏洩のリスクも発生する。よっていかにクラウドコンピューティングを安全に利用可能なものとするかは大きな課題であり，様々なセキュリティ観点からの研究が進められている。

２．研究の目的

クラウドコンピューティングを有効に利用するためには，データとデータに対する処理を同時に外部組織にアウトソースすることが望ましい。データを守る手法として暗号技術は既に様々な形で確立されてはいるが，暗号技術を単純に適用するだけではクラウド環境に対してデータ処理を効率的にアウトソースすることが難しくなることが知られている。例えば単純に暗号化したデータをクラウドサーバに置くだけでは暗号データへの検索処理をクラウドサーバに依頼することは困難となる。

本プロジェクトの目的は機密データをクラウド環境へアウトソースする状況において，漏洩の危険性を排除しつつ，有効活用を可能とする暗号技術の確立である。

３．研究の方法

クラウド環境での利用を目的とした暗号技術として以下の技術に注目し，さらなる改善を目指す。

(1) 関数型暗号:
データを暗号化しクラウドストレージに置く場合，データ共有に関するアクセス制御情報の指定も安全性を確保するために重要である。暗号化とアクセス制御を同時に実現する有用な技術として関数型暗号(属性ベース暗号と呼ばれることもある)が注目されている。本プロジェクトでは関数型暗号への機能拡張や使いやすいソフトウェアライブラリの開発に取り組む。

(2) 秘匿計算:
データを秘匿したままデータに対する演算処理を可能とする暗号技術として秘匿計算手法が存在する。データを暗号化してクラウドサーバに置くような状況や，より一般に秘密データを含む計算をアウトソースする状況で有用な秘匿計算手法の開発に取り組む。

(3) 検索可能暗号:
クラウドサーバの最もシンプルな利用形態であるストレージ利用において必須となる暗号データに対するキーワード検索処理のより進んだ機能の実現に取り組む。

４．研究成果

まず属性ベース暗号に関する成果について述べる。本プロジェクトでは暗号研究の専門家でなくとも平易に利用しやすい属性ベース暗号ライブラリの開発に取り組んだ。属性ベース暗号では暗号文作成者が暗号データ作成の際に，どういった属性を持つ人が復号可能かを指定できる機能を持っている。構築したソフトウェアライブラリではアクセス制御の指定を属性名と論理式の組み合わせによってシンプルに行える使い勝手のよいインタフェース設計を行った。また性能測定を通じて実用的なレベルを実現できていることを確認できた。

また属性ベース暗号方式において，利用権限の無くなったユーザの鍵をあとから失効することが可能で，かつ複数の鍵発効機関がシステムの中に存在可能な方式の提案も行った。提案方式では一度発行された復号鍵の権限を鍵発行機関が属性毎に失効可能な方式となっている。実際に属性ベース暗号が使用される状況においては，ユーザの所有する鍵全体を失効するだけでなく，ユーザのある特定の属性の所有状況のみを失効することもあるため，本方式ではそのような失効にも対応が可能となっている。

さらにいくつかの属性ベース暗号方式においては，復号可能条件が複雑なほど復号に必要な演算処理回数が長くなるという欠点があった。それを定数回数の演算処理によって実現する手法の提案も行った。

次に秘匿計算に関する成果について述べる。クラウドシステムなどの認証処理においてパスワードを一つのサーバに保存しておいたり，認証処理の中でパスワードを平文として扱う期間があると，パスワード漏えいの可能性が高まる危険がある。このような状況に対して，パスワードを暗号化して複数のサーバに保存し，パスワードの平文を一度も扱うことなく，ユーザを正しく認証する技術を秘匿計算の手法を用いて実現した。提案手法ではサーバもユーザのパスワードそのものに触れる機会がないため高い安全性を確保できている。

また複数の参加者の入札情報を秘匿しつつオークション処理を実現するシステムについても検討を行った。既存の秘匿計算に基づくオークションシステムでは，これまで自動にタイブレークを行う仕組みが組み込まれていなかった。提案方式では秘密乱数を入札値の最下位桁に付与し秘匿比較計算を適切に改良することで自動タイブレーク機能を実現した。

またこれまでの秘匿計算において，重要ながらもあまり考慮されてこなかった入力サイ

ズも秘匿する秘匿計算にも取り組んだ。ある条件を満たせばデータの中身だけでなくデータのサイズも秘匿しつつ秘匿計算が可能であることを明らかにした。
さらに秘密データを含むプログラム計算を安全にアウトソースすることを可能とするガーブルド回路(Garbled Circuit, GC)と呼ばれる手法に着目した。GC と特殊な耐タンパメモリを利用することでアウトソースされた計算の実行回数を制限する既存手法が知られていたが，複数のクラウドストレージシステムに特殊な耐タンパメモリの役割を担わせることで，その実行回数を制限する手法の提案も行った。

次に検索可能暗号に関する成果について述べる。クラウドストレージに置かれた暗号化データに対するキーワード検索を行う手法は様々なものが提案されている。提案方式はブルームフィルタと呼ばれるデータ構造とハッシュ関数を用いて構成した。公開鍵暗号処理で用いられるような剰余演算を必要としないため，その分，計算量の観点から軽量であると期待できる。提案方式ではキーワードが単純に一致した場合だけでなく，検索者がワイルドカードを用いて検索条件を指定することによって，類似したキーワードにも一致することも可能とし，より柔軟な検索機能を実現している。

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 16 件）


① Hikaru Tsuchida, Takashi Nishide, Eiji Okamoto, and Kwangjo Kim, ``Revocable Decentralized Multi-Authority Functional Encryption,'' Indocrypt, LNCS 10095, pp.248--265, Springer-Verlag, 査読有, 2016.

② Kazumasa Shinagawa, Koji Nuida, Takashi Nishide, Goichiro Hanaoka, and Eiji Okamoto, ``Size-Hiding Computation for Multiple Parties,'' Asiacrypt, LNCS 10032, pp.937--966, Springer-Verlag, 査読有, 2016.

③ Fangming Zhao and Takashi Nishide, ``Searchable Symmetric Encryption Supporting Queries with Multiple-Character Wildcards,'' 10th International Conference on Network and System Security (NSS), LNCS 9955, pp.266--282, Springer-Verlag, 査読有, 2016.

④ Keisuke Hasegawa, Naoki Kanayama, Takashi Nishide, and Eiji Okamoto, ``Software Library for Ciphertext/Key-Policy Functional Encryption with Simple Usability,'' Journal of Information Processing, Information Processing Society of Japan, Vol.24, No.5, pp.764--771, 査読有, 2016.

⑤ Nobuaki Kitajima, Naoto Yanai, Takashi Nishide, Goichiro Hanaoka, and Eiji Okamoto, ``Fail-Stop Signatures for Multiple-Signers: Definitions, Constructions, and Their Extensions,'' Journal of Information Processing, Information Processing Society of Japan, Vol.24, No.2, pp.275--291, 査読有, 2016.

⑥ Yusuke Kanbara, Tadanori Teruya, Naoki Kanayama, Takashi Nishide, and Eiji Okamoto, ``Software Implementation of a Pairing Function for Public Key Cryptosystems,'' 5th International Conference on IT Convergence and Security (ICITCS'15), pp.1--5, IEEE, 査読有, 2015.

⑦ Yukou Kobayashi, Naoto Yanai, Kazuki Yoneyama, Takashi Nishide, Goichiro Hanaoka, Kwangjo Kim, and Eiji Okamoto, ``Gateway Threshold Password-based Authenticated Key Exchange Secure against Undetectable On-line Dictionary Attack,'' International Conference on Security and Cryptography (SECRYPT), pp.39--52, SciTePress, 査読有, 2015.

⑧ Takashi Nishide, Mitsugu Iwamoto, Atsushi Iwasaki, and Kazuo Ohta, ``Secure (M+1)st-Price Auction with Automatic Tie-Break,'' 6th International Conference on Trustworthy Systems (Intrust 2014), LNCS 9473, pp.422--437, Springer-Verlag, 査読有, 2015.

⑨ Sanami Nakagawa, Keita Emura, Goichiro Hanaoka, Akihisa Kodate, Takashi Nishide, Eiji Okamoto, and Yusuke Sakai, ``A Privacy-enhanced Access Log Management Mechanism in SSO Systems from Nominative Signatures,'' 13th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp.565--574, 査読有, 2014.


〔学会発表〕（計 13 件）

① 神原佑輔，西出隆志，``TEPLA 上での内

積暗号の実装と評価，'' 暗号と情報セキュリティシンポジウム(SCIS)，ロワジールホテル那覇(沖縄県那覇市)，7pages，1月，2017．

② 土田光，金山直樹，西出隆志，岡本栄司，``高速復号可能かつ一般的なアクセス構造を実現した属性ベース暗号，'' Technical report of IEICE，ISEC，電気通信大学(東京都調布市)，7pages，2016．

③ 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，'' Technical report of IEICE，ISEC，電気通信大学(東京都調布市)，8pages，2016．

④ 長谷川佳祐，金山直樹，西出隆志，岡本栄司，``TEPLA に基づく暗号文/鍵規定型属性ベース暗号の実装，'' 暗号と情報セキュリティシンポジウム(SCIS)，ANA クラウンプラザホテル熊本(熊本県熊本市)，6pages，2016．

⑤ 品川和雅，縫田光司，金山直樹，西出隆志，花岡悟一郎，岡本栄司，``サイズを隠す多者間プロトコルの実現(不)可能性について，'' 暗号と情報セキュリティシンポジウム(SCIS)，ANA クラウンプラザホテル熊本(熊本県熊本市)，8pages，2016．

⑥ 小嶋陸大，品川和雅，金山直樹，西出隆志，岡本栄司，``共通鍵完全準同型暗号を用いた安全なブルームフィルタ，'' 暗号と情報セキュリティシンポジウム(SCIS)，ANA クラウンプラザホテル熊本(熊本県熊本市)，6pages，2016．

⑦ 北村拓也，品川和雅，金山直樹，西出隆志，岡本栄司，``クラウドを用いたワンタイムプログラムとその電子現金への応用，'' 暗号と情報セキュリティシンポジウム(SCIS)，ANA クラウンプラザホテル熊本(熊本県熊本市)，5pages，2016．

⑧ 佐久間淳，陸文傑，西出隆志，國廣昇，``プライバシーポリシー執行を保証する関数評価，'' コンピュータセキュリティシンポジウム(CSS)，長崎ブリックホール(長崎県長崎市)，8pages，2015．

⑨ 品川和雅，縫田光司，金山直樹，西出隆志，花岡悟一郎，岡本栄司，``隠し共有ストレージ機能を用いた入出力のサイズを隠す二者間秘密計算の実現(不)可能性，'' コンピュータセキュリティシンポジウム(CSS)，長崎ブリックホール(長崎県長崎市)，8pages，2015．

⑩ 田中和磨，矢内直人，岡田雅之，金山直樹，西出隆志，岡本栄司，``BGPSEC におけるアグリゲート署名の導入，'' コンピュータセキュリティシンポジウム(CSS)，長崎ブリックホール(長崎県長崎市)，8pages，2015．

⑪ 神原佑輔，金山直樹，西出隆志，岡本栄司，``BN 楕円曲線を用いた高速なペアリングライブラリの実装，'' 情報通信システムセキュリティ研究会(ICSS)，九工大(福岡県北九州市)，6pages，2015．

⑫ 土田光，金山直樹，西出隆志，岡本栄司，Kwangjo Kim，``複数の鍵発行機関が存在可能な関数型暗号に対する失効機能の実現，'' 暗号と情報セキュリティシンポジウム(SCIS)，リーガロイヤルホテル小倉(福岡県北九州市)，8pages，2015．

## ６．研究組織

(1)研究代表者
西出 隆志（NISHIDE Takashi）
筑波大学・システム情報系・准教授
研究者番号：70570985

(2)研究分担者
岡本 栄司（OKAMOTO Eiji）
筑波大学・名誉教授
研究者番号：60242567

(3)研究分担者
金山 直樹（KANAYAMA Naoki）
筑波大学・システム情報系・助教
研究者番号：70339696