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

令和　２ 年　 ６ 月 １２ 日現在

機関番号：１２１０２
研究種目：基盤研究(C)（一般）
研究期間：2017～2019
課題番号：１７Ｋ００１７８

研究課題名（和文）データ秘匿計算の具体的問題構造に基づく機能性・効率性向上

研究課題名（英文）Improving functionality and efficiency of secure computation by using structures of problems

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）　　3,400,000円

研究成果の概要（和文）：暗号技術は現代において通信データを秘匿するために広く利用されているが，それ以外に，電子化され保存されたデータの暗号化にも広く利用されている。データの暗号化は安全性の向上に大きく寄与する一方で，データの利便性にも大きな影響をもたらす。つまり暗号化したデータは復号しなければ利用できないが，コンピュータシステムへの侵入を完全に防止するのが困難な状況において，可能な限り暗号データを復号せずに利用したいという要請がある。本研究プロジェクトではそのような状況へ対応すべく，可能な限り暗号データを秘匿したまま様々な演算処理が可能な手法の実現に取り組んだ。

研究成果の学術的意義や社会的意義
様々なデータを電子化し，大量に保存することが可能になった現代において，多種多様な場面で情報を活用することが求められている。集められた情報を分析することで新たな知見が得られることが期待できる一方で，機密情報は公開/共有することが難しく有効活用できていないという状況があった。そのような価値の高い機密情報を保護したまま処理することを可能とする技術の開発は，有用な情報の利活用を促すことにつながる。

研究成果の概要（英文）：Nowadays cryptographic techniques are widely used to protect communication data, while digital data stored at various computers/servers are also protected by cryptography. Employing encryption techniques simply can sometimes lead to inconvenience, i.e., encrypted data need to be decrypted in the environment which may be compromised by an adversary. It is not easy to prevent server breaches perfectly, so to tackle such a situation, we work on how to process encrypted data while keeping them in the encrypted form.

研究分野：暗号

キーワード：暗号技術

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

現代では多種多様，かつ大量の情報を電子化して保存することが可能となっている。またそれらのデータを機械学習などの情報技術でコンピュータ上で分析し，新たな知見を得るということも可能となった。このように情報の扱いやすさや利活用により大きな恩恵を得られる反面，情報の窃盗や漏えいのリスクはさらに増大し，適切な情報保護技術に対する要請はより大きくなっている。

２．研究の目的

暗号技術は現代において，ネットワーク上の通信データを秘匿するために広く利用されているが，それ以外に，電子化されて様々なクラウドコンピューティング環境に保存されたデータの暗号化にも広く利用されている。データの暗号化は漏えいなどに対する安全性の向上に大きく寄与するが，それと同時に，データの利便性にも大きな影響をもたらす。つまり暗号化したデータは復号しなければ利用することができないが，攻撃者によるネットワークを介したコンピュータシステムへの侵入を完全に防止するのが困難な状況においては，可能な限り暗号データを復号せずに利用したいという要請がある。

そこで本研究プロジェクトでは重要な情報の共有や利活用を，複数の組織間でより促進することを目的に，可能な限り情報を秘匿したまま処理可能とする様々な暗号技術の開発に取り組んだ。

３．研究の方法

機密情報を秘匿したまま処理を可能とする暗号技術として以下の手法に注目し，さらなる改善を目指す。

秘密分散技術に基づく秘匿計算:
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密分散に基づく秘匿計算手法が存在する。これは機密情報を複数の断片情報に分割し，元の情報を断片から復元することなく断片情報のまま計算を行う手法である。データを分割して秘密データを含む計算を複数のクラウドサーバへアウトソースする状況で有用な秘匿計算手法である。

準同型暗号技術に基づく秘匿計算:
特殊な数学的構造を用いて作成された暗号化データは，そのデータを復号することなく複数の暗号文同士に加算，乗算などの演算が可能となる。このとき演算結果もまた暗号化された状態を保持できる。このような暗号方式を準同型暗号方式と呼ぶ。１台のクラウドサーバへ計算をアウトソースする状況で有用な秘匿計算手法である。

方式に特化したアルゴリズムを組み込んだ秘匿計算:
上記の一般的な秘匿計算手法に加えて，実現したい特定機能に特化した手法を織り交ぜて秘匿計算方法を構成することで，従来方式よりもよい効率を持つ方式の構成が可能となることもある。本研究プロジェクトではこのような方式の実現にも取り組む。

ブロックチェーンを組み込んだ暗号技術:
従来の秘匿計算手法に加えて，ブロックチェーンを部分的に応用することで秘匿計算の中で用いる暗号鍵をより安全に管理する手法や公平なデータ交換の実現に取り組む。

４．研究成果

まず秘密分散を用いた秘匿計算手法の成果について述べる。

- サーバに保存されたどのデータをクライアントがアクセスしたかをサーバから秘匿できる Oblivious RAM (ORAM) と呼ばれる暗号プロトコルが存在する。この ORAM を再帰的に用い，個人データのサーバへの登録を行う利用者のプライバシ情報を保護しながら，その利用者に関するデータの集計を可能とする方式の設計に取り組んだ。

- データを秘密にしたまま演算処理する秘匿計算において，ビット列から元の値を復元する処理が必要となることがある。この処理において事前に行う処理を幾分多めに実行しておくことで，実際に計算に必要なデータがそろった際の処理を効率化させる手法の研究に取り組んだ。

- 秘匿計算における秘密データが単なる整数ではなく浮動小数点を持つ形式のデータである場合も考慮し，計算の法をより小さく取ることを可能にすることで，処理に必要な参加者間

の通信量を削減する手法の研究に取り組んだ。

次に準同型暗号技術を用いた秘匿計算手法の成果について述べる。

- 暗号文を復号せずに演算処理を可能とする完全準同型暗号方式なるものがあるが，その中でも異なる鍵で暗号化されたデータ同士の演算を可能とする方式に着目した。その既存方式における暗号文同士の複数の演算処理の一部を結合することにより，処理の更なる効率化を試みた。

- データを暗号化したままで演算が可能となる準同型暗号方式において，暗号化された複数のデータの大小比較を効率的に可能とする手法を構成した。特に複数人が独立して異なる鍵でデータを暗号化可能なタイプの準同型暗号においても大小比較が可能な方式を構成した。

次に方式に特化したアルゴリズムを組み込んだ秘匿計算の成果について述べる。

- 機密データの保有者がクラウドサーバにアップロードした自分のデータに対して，誰がどのような操作をしてよいか，またその操作結果を誰が得てよいかを指定可能な形でデータをクラウドストレージにアップロードするシステムを提案した。このとき，データそのものの暗号化には準同型暗号方式を用い，権限を指定する部分では属性ベース暗号方式と呼ばれる手法を利用することで，暗号文から誰が操作してよいのかという情報も分からないようにすることでより漏えいする情報を削減した。主に医療用データを関係する分析者のみに操作を可能としたい場面での利用を想定している。

- 秘匿したいデータを内部に含む実行ファイルを安全に第三者に実行させる手法の初期構成案の検討を行った。ここで実行ファイルを受け取る者は，実行ファイルの実行時に，実行ファイルの作成者とコンタクトを不要とするためにクラウドストレージへ必要なデータを安全にアウトソースする手法を用いた。実行ファイルから秘密に埋め込まれたデータが実行者へ漏れないよう，ガーブルド回路と呼ばれる手法を適用した。特にここでは電子署名を他者に安全に生成させる実行処理に特化した手法の検討を進めた。この手法をさらに発展させることで秘密データを可能な操作を制限させた形で安全に外部へアウトソースすることが可能となる。

次にブロックチェーンを用いた暗号構成の成果について述べる。

- 二人の参加者間で電子契約を公平に行う暗号プロトコルの構成にも取り組んだ。ここでの電子契約は二人の参加者のそれぞれが，同時に公平に他方からの電子署名を得ようとするものである。単に電子署名データを同時に送りあって交換するだけでは，片方が不正行為により，他方の署名データを持ち逃げしてしまうことが発生しうる。そのため，そのような不正を防ぐために，特別な暗号プロトコルの仕組みが必要となる。本研究ではブロックチェーンの機能を導入し，両方の電子署名がある決められた期限内にブロックチェーン上にそろったときのみ，両方の電子署名が有効となるようプロトコルを構成し，問題の解決を図った。

- 秘匿計算システムの中においても暗号の鍵管理は重要となる。従来の暗号方式において，暗号用の鍵が漏えいするとこれまでの全ての暗号文が復号されうる。そのような被害を軽減するために，用いている暗号の鍵が漏洩しても過去に暗号化されたデータは復号可能とならないような公開鍵暗号方式の構成に取り組んだ。その中では復号処理とブロックチェーンの利用を組み合わせることで，復号された履歴がブロックチェーンに既に存在する場合は，復号できないようにすることで，一度だけ復号可能な暗号文の生成を行う方式を実現させた。

５．主な発表論文等

〔雑誌論文〕　計9件（うち査読付論文　9件／うち国際共著　1件／うちオープンアクセス　0件）

１．著者名 天田拓磨，奈良成泰，西出隆志，吉浦裕	４．巻 60
２．論文標題 通信量を削減した浮動小数演算のためのマルチパーティ計算	５．発行年 2019年
３．雑誌名 情報処理学会論文誌	６．最初と最後の頁 1433--1447
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Noboru Kunihiro, Wen-jie Lu, Takashi Nishide, Jun Sakuma	４．巻 -
２．論文標題 Outsourced Private Function Evaluation with Privacy Policy Enforcement	５．発行年 2018年
３．雑誌名 IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)	６．最初と最後の頁 412--423
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Hikaru Tsuchida, Takashi Nishide, Eiji Okamoto	４．巻 8
２．論文標題 Expressive Ciphertext-Policy Attribute-Based Encryption with Fast Decryption	５．発行年 2018年
３．雑誌名 ProvSec Workshop (Journal of Internet Services and Information Security (JISIS))	６．最初と最後の頁 37--56
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Yukou Kobayashi, Naoto Yanai, Kazuki Yoneyama, Takashi Nishide, Goichiro Hanaoka, Kwangjo Kim, Eiji Okamoto	４．巻 Vol. E100--A, No. 12
２．論文標題 Provably Secure Gateway Threshold Password-based Authenticated Key Exchange Secure against Undetectable On-line Dictionary Attack	５．発行年 2017年
３．雑誌名 IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	６．最初と最後の頁 2991--3006
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

1．著者名 Sanami Nakagawa, Keita Emura, Goichiro Hanaoka, Akihisa Kodate, Takashi Nishide, Eiji Okamoto, Yusuke Sakai	4．巻 Vol. 3, No. 4
2．論文標題 A Privacy-enhanced Access Log Management Mechanism in SSO Systems from Nominative Signatures	5．発行年 2017年
3．雑誌名 International Journal of Applied Cryptography	6．最初と最後の頁 394--406
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 奈良成泰，天田拓磨，西出隆志，土井洋，吉浦裕	4．巻 Vol.58, No.9
2．論文標題 秘密計算を用いた時系列情報の安全な集計方法	5．発行年 2017年
3．雑誌名 情報処理学会論文誌	6．最初と最後の頁 1464--1482
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Kazumasa Shinagawa, Mizuki Takaaki, Jacob C.N. Schuldt, Koji Nuida, Naoki Kanayama, Takashi Nishide, Goichiro Hanaoka, Eiji Okamoto	4．巻 Vol. E100-A, No. 9
2．論文標題 Card-Based Protocols Using Regular Polygon Cards	5．発行年 2017年
3．雑誌名 IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	6．最初と最後の頁 1900--1909
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Nobuaki Kitajima, Naoto Yanai, Takashi Nishide	4．巻 LNCS 10726
2．論文標題 Identity-Based Key-Insulated Aggregate Signatures, Revisited	5．発行年 2017年
3．雑誌名 Inscrypt	6．最初と最後の頁 141--156
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Takuya Kitamura, Kazumasa Shinagawa, Takashi Nishide, Eiji Okamoto	４．巻 -
２．論文標題 One-time Programs with Cloud Storage and Its Application to Electronic Money	５．発行年 2017年
３．雑誌名 ACM International Workshop on ASIA Public-Key Cryptography	６．最初と最後の頁 25--30
掲載論文のDOI（デジタルオブジェクト識別子） 10.1145/3055504.3055507	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計15件（うち招待講演　0件／うち国際学会　0件）

１．発表者名 怒田晟也, Jacob Schuldt, 西出隆志
２．発表標題 ブロックチェーンを用いた鍵更新なしフォワード安全公開鍵暗号
３．学会等名 暗号と情報セキュリティシンポジウム
４．発表年 2020年

１．発表者名 土田光, 西出隆志
２．発表標題 効率的なOnlineフェーズを持つビット結合プロトコル
３．学会等名 暗号と情報セキュリティシンポジウム
４．発表年 2020年

１．発表者名 Naoya Okanami, Ryuya Nakamura, Takashi Nishide
２．発表標題 Load Balancing for Sharded Blockchains
３．学会等名 暗号と情報セキュリティシンポジウム
４．発表年 2020年

１．発表者名
南翔，西出隆志

２．発表標題
暗号通貨MoneroへのKleptographic攻撃に関する考察

３．学会等名
暗号と情報セキュリティシンポジウム

４．発表年
2020年

１．発表者名
布施慶太，西出隆志

２．発表標題
HSM上での耐量子暗号の実装と評価

３．学会等名
暗号と情報セキュリティシンポジウム

４．発表年
2020年

１．発表者名
西出隆志

２．発表標題
ワンタイムプログラムとそのシュノア署名への応用

３．学会等名
Technical report of IEICE, ISEC

４．発表年
2019年

１．発表者名
樋口裕二，西出隆志

２．発表標題
複数鍵完全準同型暗号を用いた非対話型大小比較プロトコル

３．学会等名
Technical report of IEICE, ISEC

４．発表年
2019年

１．発表者名
三島貴務，西出隆志

２．発表標題
ノンスベースのハイブリッド暗号

３．学会等名
Technical report of IEICE, ISEC

４．発表年
2019年

１．発表者名
樋口裕二，西出隆志

２．発表標題
完全準同型暗号に基づく非対話型大小比較の拡張

３．学会等名
暗号と情報セキュリティシンポジウム

４．発表年
2019年

１．発表者名
南翔，西出隆志

２．発表標題
ランサムウェア検知ソフトCryptoDropの耐性評価

３．学会等名
情報通信システムセキュリティ研究会

４．発表年
2018年

１．発表者名
怒田晟也，西出隆志

２．発表標題
マルチパス通信を実現する Datagram TLS 拡張

３．学会等名
情報通信システムセキュリティ研究会

４．発表年
2018年

１．発表者名
小嶋陸大，西出隆志

２．発表標題
準同型演算と暗号文拡張を同時に実行する動的な複数鍵完全準同型暗号

３．学会等名
暗号と情報セキュリティシンポジウム

４．発表年
2018年

１．発表者名
北村拓也，西出隆志

２．発表標題
クラウドワンタイムプログラムとその電子現金への応用

３．学会等名
暗号と情報セキュリティシンポジウム

４．発表年
2018年

１．発表者名
天田拓磨，奈良成泰，西出隆志，吉浦裕

２．発表標題
浮動小数点演算のための通信コストを削減したマルチパーティ計算

３．学会等名
暗号と情報セキュリティシンポジウム

４．発表年
2018年

１．発表者名
三島貴務，西出隆志

２．発表標題
ブロックチェーンを用いた電子契約プロトコル

３．学会等名
情報通信システムセキュリティ研究会

４．発表年
2017年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考