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　５ 年　 ６ 月　 ９ 日現在

機関番号：１２１０２
研究種目：基盤研究(C)（一般）
研究期間：2020～2022
課題番号：２０Ｋ１１８０７

研究課題名（和文）機密データを含むプログラム実行の安全かつ容易な外部委託とその応用

研究課題名（英文）Secure Outsourcing of Program Execution with Private Inputs

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）　　3,300,000円

研究成果の概要（和文）：各種データの電子化，共有，処理が可能な今日，機密データさえも他組織と共有し利活用を可能とする手法が期待されており，その中で秘密計算と呼ばれる暗号技術が中心的役割を果たしている。秘密計算により複数のデータ保有者らは持ち寄った機密データを秘匿したまま計算し，出力のみを得ることができる。一方、秘密計算ではデータを秘匿したままでの計算を行うことから通常の計算と比べ、計算速度が遅いという欠点がある。本研究では秘密計算の社会での利用促進に向けその効率化に取り組んだ。

研究成果の学術的意義や社会的意義
本研究では(1)秘密分散に基づく秘密計算手法、(2)完全準同型暗号に基づく秘密計算手法、(3)ワンタイムプログラムという形式で秘密データの提供者と使用者が直接に通信しなくとも秘密計算を行える手法の署名権限委譲への適用、に取り組んだ。また分散電子台帳を利用することでワンタイムプログラム形式の暗号文を作成し、秘密計算などに利用する暗号鍵の漏洩対策技術の開発にも取り組んだ。

研究成果の概要（英文）：Various types of data can be digitized, shared, and processed today, and there is a need for methods that enable the sharing and utilization of even confidential data with other organizations. Among these methods, cryptographic techniques known as secure computation play a central role. With secure computation, multiple data holders can bring together their confidential data, perform calculations while keeping the data secret, and obtain only the output. On the other hand, secure computation has the disadvantage of slower computation speed compared to regular computation, as it involves performing calculations while keeping the data secret. In this study, we focused on improving the efficiency of secure computation to promote its use in society.

研究分野：暗号技術

キーワード：プライバシ保護

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

各種データの電子化，共有，計算処理が今日では可能であり、大量のデータを解析することで新たな知見が得られ、より豊かな社会の創造につながる可能性がある。しかし機微な解析対象データを外部と共有することは難しく、それによりデータの広い範囲での利活用が阻害されていた。そのためより高度な暗号技術の開発により、機密データさえも他組織と共有し利活用を可能とする手法の開発が期待されていた。

２．研究の目的

データを保護しつつ、計算を可能とする暗号技術として秘密計算と呼ばれる手法が注目を集めている。秘密計算により複数のデータ保有者らは持ち寄った機密データを秘匿したまま計算し，出力のみを得ることができる。一方、秘密計算ではデータを秘匿したままでの計算を行うことから通常の計算と比べ、計算速度が遅いという欠点がある。本研究では秘密計算の社会での利用促進に向けその効率化に取り組む。

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，その効率化に取り組む。

秘密分散技術に基づく秘密計算:
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密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，元の情報を計算の途中で断片から一度も復元することなく、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外部委託する状況で有用な秘密計算手法である。

完全準同型暗号技術に基づく秘密計算:
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，乗算などの演算の適用が可能となる。このとき演算結果もまた暗号化された状態を保持することができる。このような暗号方式は完全準同型暗号方式と呼ばれる。１台のクラウドサーバへ計算の全ての入力を暗号化した暗号文を渡し、計算を外部委託する状況で有用な秘密計算手法である。

ワンタイムプログラム形式の秘密計算:
ある秘密データ保持者が、機密データが埋め込まれ、指定された入力に対して一度だけ実行可能なプログラム(ワンタイムプログラムと呼ばれる)として外部に計算委託を行える秘密計算方式である。ワンタイムプログラム実行時に秘密データ保持者とワンタイムプログラム実行者が直接通信をしなくてもよいという利点を持っている。

分散電子台帳を組み込んだ暗号技術:
秘密計算の中で通信を行う際にはデータの漏洩を防ぐために暗号通信が必要となる。一般に暗号の復号に用いる秘密鍵がのちに漏洩した場合、過去の暗号通信の安全性を保つことは難しい。分散電子台帳を部分的に応用することで秘密計算の中で用いる暗号鍵をより安全に管理する手法の開発に取り組む。

４．研究成果

まず秘密分散を用いた秘密計算手法の成果について述べる。

- 機械学習では決定木と呼ばれるデータ構造を用いて入力に対する複数の条件判定を繰り返し、入力の分類結果を出力する手法が存在している。本研究では決定木に対する入力を秘匿し、かつ条件判定に用いられる各種パラメータも秘匿しながら分類結果のみを出力する

秘密計算手法を構成した。またこの構成法では計算に必要な通信回数が決定木のサイズによらず一定とすることで効率的な構成とすることに成功した。また秘密計算に対する攻撃者が計算途中で不正行為を行ったとしても、攻撃者のみが出力結果を得られることはないという安全性も同時に達成することに成功した。

- 秘密計算において複雑な関数計算を直接計算するのではなく、関数計算結果を持つルックアップテーブルを事前に用意しておき、関数の引数が決まった時点で引数の値に基づきルックアップテーブルを参照することで関数計算を行う手法が存在する。既存手法ではルックアップテーブルは 1 次元で構成されていたが、本研究ではこのルックアップテーブルを 2 次元に変形し、もし計算対象関数が周期関数のような構造を持っていれば、この 2 次元のルックアップテーブルを用いて秘密計算を行うことでより効率的に関数計算が可能なことを示した。

次に完全準同型暗号技術を用いた秘密計算手法の成果について述べる。

- 整数を暗号化するタイプの完全準同型暗号で加算乗算以外のより複雑な計算を実行するには多項式評価がしばしば用いられる。本研究では大小比較計算に用いる多項式評価方法の効率化を行った。従来であれば大小比較関数は 2 変数多項式関数と見なすことになるが、より効率的に計算できる 1 変数多項式関数の組み合わせで表現できることを示し、その手法を完全準同型暗号ソフトウェアライブラリで実装することで既存手法よりも効率的に計算が可能であることを示した。
- 整数を暗号化するタイプの完全準同型暗号において 2 変数関数を実行する既存手法は実行時間が平文空間の 2 乗となり、平文空間が大きい場合に多くの実行時間を必要としていた。本研究では従来では並列計算を行うために使用されていた完全準同型暗号におけるスロットと呼ばれる数学的構造を、ルックアップテーブルとして活用することで実行時間を大幅に減少させることに成功した。

次にワンタイムプログラムを用いた秘密計算手法の成果について述べる。

- 電子署名の生成権限を第三者に貸与することで一時的な権限委譲を行えれば便利な場面はよくある。しかし署名生成用の署名鍵をそのまま第三者に貸与することは安全性の観点から望ましくないため秘密計算的な手法が必要となる。本研究では署名鍵の所有者が署名鍵そのものをワンタイムプログラムに埋め込む必要がなく、また仮にワンタイムプログラムが 2 度実行された場合、どの不正者が 2 度実行したかを署名鍵所有者が特定できるような署名生成用ワンタイムプログラムの構成を行った。またワンタイムプログラム実行者が署名生成の際に署名鍵所有者との通信を不要とし、かつワンタイム性を実現するために、署名鍵所有者が一時的な鍵を複数のクラウドサーバに秘密分散で格納し、一度使用されたデータはクラウドサーバが削除するという仮定のもと構成を行った。

次に分散電子台帳を組み込んだ暗号技術の成果について述べる。

- 公開鍵暗号を用いた暗号通信ではのちに秘密鍵が漏洩すると、過去の暗号通信を傍受し長期間保存していた攻撃者はその秘匿性を破ることができてしまう。このような攻撃を防ぐ方法として既存研究で用いられていた方法は、公開鍵に対する秘密鍵を定期的に更新し、過去の暗号文を復号するための情報を現在の秘密鍵から削除していくというものであった。しかし秘密鍵を定期的に更新しなければならない手法は使い勝手が悪く、また定期的に更新せずにこのような攻撃を防ぐ手法が存在するのかは未解決の問題であった。本研究では分散電子台帳を暗号文の復号記録ログのように使用し、ある暗号文が既に復号されたか否かを分散電子台帳に記録し、暗号文の復号には Witness Encryption の復号処理を用いることで秘密鍵の定期的更新無しに攻撃を防げることを示した。ここでは Witness Encryption の復号のために分散電子台帳のブロックの一部を必要とするよう構成し、Witness Encryption の復号条件のチェックの中で既に暗号文が復号済みか否かを確認することで 1 度のみ復号可能な暗号文を構成することに成功した。この構成法により正しい受信者に 1 度復号された暗号文はのちに秘密鍵が漏洩したとしても、攻撃者から復号されることはなく強い安全性が達成可能であることを示した。

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　0件／うちオープンアクセス　0件）

１．著者名 Hikaru Tsuchida, Takashi Nishide, and Yusaku Maeda	４．巻 Vol. E105-A, No. 3
２．論文標題 Private Decision Tree Evaluation with Constant Rounds via (only) SS-3PC over Ring and Field	５．発行年 2021年
３．雑誌名 IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	６．最初と最後の頁 214-230
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.2021CIP0018	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, and Takashi Nishide	４．巻 29
２．論文標題 Client-aided Robust Bit-composition Protocol with Deterministic Cheater Identification in Standard Model	５．発行年 2021年
３．雑誌名 Journal of Information Processing, Information Processing Society of Japan	６．最初と最後の頁 515-524
掲載論文のDOI（デジタルオブジェクト識別子） 10.2197/ipsjjip.29.515	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 Seiya Nuta, Jacob C.N. Schuldt, and Takashi Nishide	４．巻 13143
２．論文標題 Forward-Secure Public Key Encryption without Key Update from Proof-of-Stake Blockchain	５．発行年 2021年
３．雑誌名 Indocrypt, LNCS, Springer	６．最初と最後の頁 436-461
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-92518-5_20	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, and Takashi Nishide	４．巻 13083
２．論文標題 Private Decision Tree Evaluation with Constant Rounds via (Only) Fair SS-4PC	５．発行年 2021年
３．雑誌名 ACISP, LNCS, Springer	６．最初と最後の頁 309-329
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-90567-5_16	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 Takashi Nishide	4．巻 LNCS 12505
2．論文標題 One-Time Delegation of Unlinkable Signing Rights and Its Application	5．発行年 2020年
3．雑誌名 International Conference on Provable Security, Springer-Verlag	6．最初と最後の頁 103-123
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-62576-4_6	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, and Yusaku Maeda	4．巻 LNCS 12505
2．論文標題 Private Decision Tree Evaluation with Constant Rounds via (Only) SS-3PC over Ring	5．発行年 2020年
3．雑誌名 International Conference on Provable Security, Springer-Verlag	6．最初と最後の頁 298-317
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-62576-4_15	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 Genki Osada, Budrul Ahsan, Revoti Prasad Bora, Takashi Nishide	4．巻 LNCS 12346
2．論文標題 Regularization with Latent Space Virtual Adversarial Training	5．発行年 2020年
3．雑誌名 European Conference on Computer Vision (ECCV), Springer-Verlag	6．最初と最後の頁 565-581
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-58452-8_33	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 and Takashi Nishide	4．巻 -
2．論文標題 Client-Aided Bit-Composition Protocol with Guaranteed Output Delivery	5．発行年 2020年
3．雑誌名 International Symposium on Information Theory and its Application (ISITA)	6．最初と最後の頁 387-391
掲載論文のDOI（デジタルオブジェクト識別子） 10.34385/proc.65.C01-11	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 Naoya Okanami, Ryuya Nakamura, and Takashi Nishide	4．巻 LNCS 12063
2．論文標題 Load Balancing in Sharded Blockchains	5．発行年 2020年
3．雑誌名 Workshop on Trusted Smart Contracts (in Financial Cryptography), Springer-Verlag	6．最初と最後の頁 512-524
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-54455-3_36	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3件（うち招待講演　0件／うち国際学会　0件）

1．発表者名 前田大輔，西出隆志
2．発表標題 整数型平文空間における非線形2変数準同型演算の高速化
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 2022年

1．発表者名 森村洸生，西出隆志
2．発表標題 多項式補間による整数型準同型大小比較/除算の改良
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 2022年

1．発表者名 小林正英，西出隆志
2．発表標題 TEE 技術に基づく非対話紛失通信プロトコルの構成
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 2020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
研究分担者	國廣　昇 (Kunihiro Noboru) (60345436)	筑波大学・システム情報系・教授 (12102)	

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関