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　３ 年　 ６ 月 ２９ 日現在

機関番号：３２５０３
研究種目：基盤研究(C)（一般）
研究期間：2018～2020
課題番号：１８Ｋ１１２７３

研究課題名（和文）軽量Nパーティ秘匿関数計算の一般化に基づくセキュアなIoTモデルの提案

研究課題名（英文）A Secure IoT Model which is based on Generalized Lightweight N Party Secure Function Evaluation

研究代表者
藤田　茂（Fujita, Shigeru）

千葉工業大学・情報科学部・教授

研究者番号：４０２９６３２２

交付決定額（研究期間全体）：（直接経費）　　1,400,000円

研究成果の概要（和文）：データの秘密を守るために暗号化を行うが，一般に計算コストが高い．また暗号化されたデータを悪意ある第三者に奪取されると時間をかけて復号される懸念がある．複数のデータの関係を調べる時にデータを復号すると，その復号箇所がセキュリティリスクとなる．このため，暗号化したまま計算することが望まれる．本研究課題では，データに乱数を混入した上で複数の断片に分割して保存する，秘密分散の手法の一つに取り組んだ．また，分散されたデータを分散したまま計算するための秘密計算手法を一般化して，計算パワーが相対的に低いIoT機器へ適用するための研究を実施した．

研究成果の学術的意義や社会的意義
軽量3パーティ秘匿関数計算を，Nパーティ秘匿関数へ拡張し，適用範囲を明らかにした．千田らはデータを分散する際に乱数を用いる軽量秘匿関数計算を3つのパーティを対象に2011年に提案した．千田らの手法は，3つのパーティに限定して証明が与えられていたが，これをNパーティへ拡張した証明を与え，Nパーティで実行可能な範囲を明らかにした．秘密分散の方式では，閾値以下のデータ漏洩に対して情報理論的安全性を与えることができる．このため，セキュリティリスクを軽減することが可能であり，社会的な意義は大きい．

研究成果の概要（英文）：Encryption is used to protect the confidentiality of data, but the calculation cost is generally high. In addition, if the encrypted data is stolen by a malicious third party, there is a concern that it will be decrypted over time. If data is decrypted when examining the relationship between multiple data, the decrypted part becomes a security risk. Therefore, it is desirable to calculate with encryption. In this research project, we worked on one of the secret sharing methods, in which random numbers are mixed in the data and then divided into multiple fragments and stored. In addition, we generalized the secret calculation method for calculating distributed data while it is distributed, and conducted research to apply it to IoT devices with relatively low calculation power.

研究分野：分散処理

キーワード：秘密分散　秘密計算　軽量秘匿関数計算　共生コンピューティング　デジタル寺院　ネバーダイプロフェッサ

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

先行研究である軽量 3 パーティ秘匿関数計算では，データを 3 台の主体に分散して保存し，1 台が故障あるいはクラックされた場合でも計算が実行でき，かつ，故障あるいはクラックされたことを検出することを可能にした. これは, データの復元に必要な主体数を 2 として, 2 out of 3 というセキュアマルチパーティプロトコルとして，分散したデータを一箇所に復元することなく，加減算・定数倍・乗算・論理演算の各計算を行うことができる．これに対して，データを秘密分散する主体数を n，データの復元に必要な主体数を k とすると，k out of n として表現することができる．この k と n の関係は一見すると，n >= k であれば成立するように見えるが，3 out of 4 の場合(n = 4; k = 3)には，乗算が実行できないことが明らかになっていた.

２．研究の目的

IoT 機器が普及し，数多くのセンサーやカメラが設置されている．これら IoT 機器への不正なアクセスによるデータ流出は深刻な課題であり，解決が急務である．しかし，IoT 機器には盗難や紛失，セキュリティホールの発覚が多くあり，IoT 機器単体のセキュリティではデータを保護できない．そこで，たとえ幾つかの IoT 機器がクラックされたとしても，データを不正なアクセスから保護するモデルを作ることが急務となっている．本研究では，秘密分散・秘密計算の手法の一つである，軽量 3 パーティ秘匿関数計算を一般化し，4 台以上の IoT 機器，一般 PC，及びクラウド上で利用可能にする．これまでの軽量 3 パーティ秘匿関数計算は，3 台の主体にのみ適用されてきた．本研究では，これを N 台に一般化する条件を明らかにすることを目的とした.

本研究の結果を適用したシステムでは，たとえ幾つかの IoT 機器がクラックされたり，盗難にあったりしたとしても，データを復元できず，データの安全性が維持される.

３．研究の方法

先行研究である軽量 3 パーティ秘匿関数計算(2 out of 3)を一般化し，k out of n としたときにも計算が可能であることを証明した．この時，k と n の関係に一定の制約があることを明らかにし，スケールアップする際の条件を示した．以下，k out of n について，我々が示した条件下での一般化された n を N とし，k out of N として表記する.

軽量 N パーティ秘匿関数計算が一般的に利用可能なことを明らかにしたので，応用システムの設計により，提案手法の有効性を示すこととした.

応用システムとしてのデジタル寺院は，デジタル・アイデンティティが危殆化し，近い将来において参照不能な状態になるという課題を解決する概念である.

デジタル寺院（図 1）では，現在，企業やコミュニティが自主的に管理しているデジタル・アイデンティティを永続的に参照可能にするコミュニティベースの保管庫を持続可能な形で運用する．これまでに関連して設計について発表してきた．共生情報システムの一応用として，このデジタル寺院を構築することが可能である.

共生情報システムによってデジタル寺院を構成する際の階層モデルの概念を図 2 に示す.

デジタル寺院は当初，デジタル・アイデンティティの保存を目的としたが，研究の過程で，権利者の意図を死後にも維持する，適切なタイミングで実行するという機能が必要であるとなった．これは，紙の書簡が遺族の手によって，書簡の著作者の意図に反する形で公開されることになったという事例などを受けてのことである.

知を探求し，新たな知を人類の共通基盤として確立するという広い意味での研究活動も，永続的な営みが求められる活動である．これまで，知の蓄積は紙媒体での出版によるところが大きかったが，現在，急速に電子ジャーナル化が進み，利便性が大きく向上する一方，橋本誠志は，“ ペーパレス社会における学会の破産と知的成果のサステナビリティに関する一考察 ”,情報処理学会研究報告，Vol．2019-EIP-85，No．12，pp.1-8，2019/09/20 の中で，学術団体の破産によって知の継承というもっとも重要な学問の持続性が破壊される可能性のあることを指摘している.

プレプリントサーバである arXiv は，査読前の論文の投稿であるが，2020 年以降猛威を振るっている新型コロナウィルスに関して，その速報性の高さから，必ずしも専門家でないジャーナリストが参照して記事にした結果，信頼性の低い学説を元に一般向け記事が作成された.

プレプリントサーバに限らず，学術論文は出版後に取り消されたり，掲載を取り下げられたりすることがある．一般に健全な研究活動の世界では，後世の検証に耐えうる良質な論文が残るのが良いとされている．しかしながら，後世改めて取り下げられた論文の検証を行ったり，あるいはなぜ論文の取り消しや取り下げが発生したりしたのかを検証するためには，否定された論文すらも参照可能な形で保存することが必要である.

研究活動の本質的部分は知的な活動であって，人でなければ遂行が困難であると考えられる．一方で，研究の補助的な活動に関しては，共生情報システムによって支援が可能である．一つは研究データの蓄積である．歴史的なデータに関して，プライバシーや，その当時の倫理では世に受け入れられなかった活動の記録など，関係者の死後でなければ公にできないデータを，確実に後世へ伝える仕組みとなる．また研究の意図にそった網羅的なサーベイ実施は，共生情報システムによって構築される研究コミュニティの中で研究者，エージェントの協調によって実行される．

現在，個々の研究者の業績の最終的な一覧は，国立国会図書館のインデックスあるいは，research map 等のサービスに依存する．しかし，国立国会図書館のインデックスも完全ではなく，また research map 等では，死後の情報の取り扱いは本人による削除希望無いしは，遺族による削除希望によってなされる可能性があり，研究者の意図に必ずしも沿うものではない．
共生情報システムにより，研究者の意図に沿った研究成果の公表，研究意図を反映した自律的なデータ交換，研究プログラムの実行によって研究者の死後にも，研究者の研究分野が存続する可能性を遺すことが可能になる．

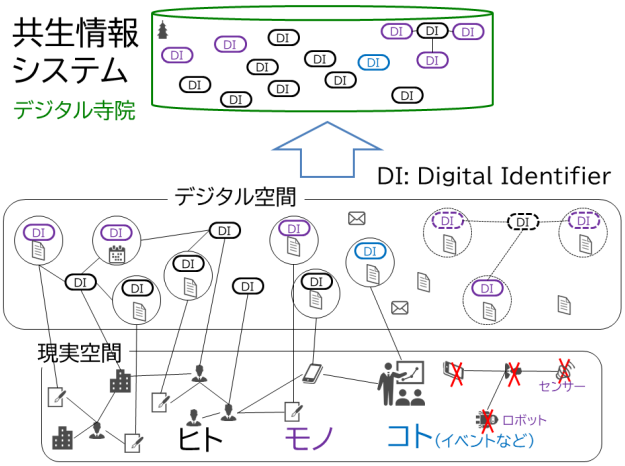

図１： デジタル寺院概念図

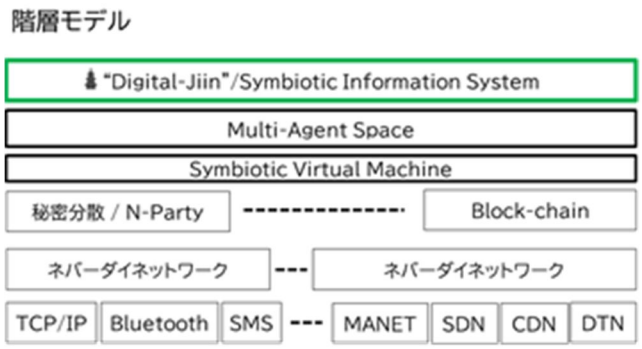

図 2: 共生情報システムとデジタル寺院構成の階層モデル

４．研究成果

３つに証明が限定されていた軽量３パーティ秘匿関数計算を一般化し，これに証明を与えた．また，一般化されるための条件を明らかにした．

先行研究である軽量３パーティ秘匿関数計算では，データを３台の主体に分散して保存し，1台が故障あるいはクラックされた場合でも計算が実行でき，かつ，故障あるいはクラックされたことを検出することを可能にした．これは，データの復元に必要な主体数を２として，2 out of 3 というセキュアマルチパーティプロトコルとして，分散したデータを一箇所に復元することなく，加減算・定数倍・乗算・論理演算の各計算を行うことができる．これに対して，データを秘密分散する主体数を n，データの復元に必要な主体数を k とすると，k out of n として表現することができる．この k と n の関係は一見すると，n >= k であれば成立するように見えるが，3 out of 4 の場合(n=4，k=3)には，乗算が実行できないことが明らかになっている．そこで，本研究では，データを分散する主体数 n と復元に必要な主体数 k の関係を明らかにした．我々が明らかにした条件下での k out of n の n を N として，軽量 N パーティ秘匿関数計算と表記する．

1年目は，軽量Nパーティ秘匿関数計算を一般化するための検討と証明を行い．その研究成果を情報処理学会論文誌ジャーナル，Vol.59，No.10，2018年に「軽量Nパーティ秘匿関数計算の一般化」として公表した．この論文は「特選論文」として表彰された．

応用面での検討結果を，DPSWS2018にて「軽量Nパーティ秘匿関数計算を用いたセキュアなIoTシステムの考察」として，JAWS2018にて「途絶遅延ネットワーク上での秘密分散によるセキュアなIoTシステムの検討」として，それぞれ発表を行った．

2年目は，これまで提案してきた「軽量Nパーティ秘匿関数計算」に対し文字列検索処理の拡張を行った．文字列検索のために,文字列のハッシュ化を行いその結果を分割・分散した.従来では整数値型のみであった秘匿関数計算のデータ検索を文字列型に拡張可能になった．情報システムの設計者に対して,文字列を秘密分散されたまま検索可能なため，利便性が向上する．また，検索にあたっていずれの場所でもデータを復元しないので，秘密分散のセキュアな状態の維持に繋がる．

セキュアなIoTモデルのための基盤技術として，軽量3パーティ秘匿関数計算を一般化して適用可能な範囲を明らかにしたうえで，文字列検索を可能にし，秘密分散の実用性を高めることができた．この拡張によって，計算のみならずデータベース的な利用が可能になり，プライバシーを重視するデータの利用が可能になると期待できる．

また本研究の応用を検討し，クラウドサービスに依存しない形で，永続的にデータを保管する仕組みとして,“デジタル寺院”:設計と開発へ向けて,“デジタル寺院”:モデルと基盤技術の研究を実施した．この仕組みの検討のなかで，セキュアなデータ保管を実現するために，軽量Nパーティ秘匿計算が有効であること，クラウドサービスにデータを保存するだけでは，利用者の望むデータ保存ポリシーを実現できない可能性があることを示した．

更に，国際共同研究に「軽量 N パーティ秘匿関数計算」の利用を提案し，"Enforcing Methodological Rules During Collaborative Brainstorming to Enhance Results"の研究を日仏の共同研究者と実施した．

3年目に至るまでに，ブロックチェーン技術の計算機負荷が高く，SDGsの障害となっていることが指摘された．一方秘密分散手法の一つである軽量Nパーティ秘匿関数計算は，計算機負荷が低く，持続可能な社会の実現へ貢献するという意義がある．また，情報システムが社会基盤を構成する重要な位置を占めるに伴って，その持続的なサービス提供が重要な課題となっていることを示し，本研究で一般化した軽量Nパーティ秘匿関数計算に基づく分散処理システムとして，共生情報システムを提唱した．また具体的な応用システムとして，デジタル識別子の永続的な保存を担うデジタル寺院，持続的な研究室活動の支援を行うネバーダイプロフェッサーの例を示した．

本研究の成果は，フランスの研究者の興味を引き，国際共同研究へ発展した．その結果は国際ジャーナル，国際会議へ報告した．また新たにイタリアの研究者が研究グループへ参加し，本研究の国際化が進められている．

今後，得られた知見を元に，情報漏洩の危険の無い持続可能な分散処理システムを構築するためのプログラミング言語とその処理系を秘密計算・秘密分散の枠組みの上に開発する．本研究は今後のSociety5.0を支える基礎技術を確立したという意義があった．

５．主な発表論文等

〔雑誌論文〕　計2件（うち査読付論文　2件／うち国際共著　1件／うちオープンアクセス　1件）

１．著者名 Gidel Thierry、Tucker Andrea、Fujita Shigeru、Moulin Claude、Sugawara Kenji、Suganuma Takuo、Kaeri Yuki、Shiratori Norio	４．巻 5
２．論文標題 Interaction Model and Respect of Rules to Enhance Collaborative Brainstorming Results	５．発行年 2020年
３．雑誌名 Advances in Science, Technology and Engineering Systems Journal	６．最初と最後の頁 484～493
掲載論文のDOI（デジタルオブジェクト識別子） 10.25046/aj050262	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

１．著者名 滝 雄太郎, 藤田 茂, 宮西 洋太郎, 白鳥 則郎	４．巻 59
２．論文標題 軽量Nパーティ秘匿関数計算の一般化	５．発行年 2018年
３．雑誌名 情報処理学会論文誌	６．最初と最後の頁 1895-1902
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 －

〔学会発表〕　計12件（うち招待講演　0件／うち国際学会　4件）

１．発表者名 Shigeru Fujita, Thierry Gidel, Yuki Kaeri, Andrea Tucker, Kenji Sugawara, Claude Moulin
２．発表標題 AI-based Automatic Activity Recognition of Single Persons and Groups During Brainstoming
３．学会等名 2020 IEEE International Conference on Systems, Man and Cybernetics (SMC)（国際学会）
４．発表年 2020年

１．発表者名 Masahiro Hiji, Yuichi Hashi, Kazuhiko Kikuchi, Shigeru Fujita, Yotaro Miyanishi, Norio Shiratori
２．発表標題 Nobel Inferitance Mechanism of Digital Content for "Digital-Ji-in" toward Sustainable Society
３．学会等名 2020 Eighth International Symposium on Computing and Networking Workshop (CANDARW)（国際学会）
４．発表年 2020年

１．発表者名
Shigeru Fujita, Yutaro Taki, Yotaro Miyanishi, Tokuyasu Kakuta, Masahiro Hiji, Kenj Sugawara, Norio Shiratori, Claude Moulin, Thierry Gidel

２．発表標題
"Digital-Ji-in": A Framework for Sustainable Digital Identification Records Based on A Peer-to-peer Netwok

３．学会等名
2021 IEEE 24th International Conference on Computer Supported Cooperative Work in Design（国際学会）

４．発表年
2020年～2021年

１．発表者名
藤田茂，白鳥則郎，滝雄太郎

２．発表標題
共生情報システム：自律・進化・持続可能な情報システムの提唱

３．学会等名
情報処理学会マルチメディア通信と分散処理研究会

４．発表年
2020年

１．発表者名
藤田茂，滝雄太郎，白鳥則郎

２．発表標題
持続可能なセキュア共生情報システムの提案とデジタル寺院・ネバーダイプロフェッサへの応用

３．学会等名
情報処理学会マルチメディア通信と分散処理研究会

４．発表年
2021年

１．発表者名
滝 雄太郎，藤田 茂，宮西 洋太郎，樋地 正浩，白鳥 則郎

２．発表標題
軽量Nパーティ秘匿関数計算の文字列検索拡張

３．学会等名
情報処理学会，シンポジウムシリーズDICOMO

４．発表年
2019年

１．発表者名
藤田 茂 , 樋地 正浩 , 滝 雄太郎 , 宮西 洋太郎 , 角田 篤泰 , 菅原 研次 , 白鳥 則郎

２．発表標題
“デジタル寺院”:設計と開発へ向けて

３．学会等名
情報処理学会マルチメディア通信と分散処理研究会

４．発表年
2019年

１．発表者名
藤田 茂 , 樋地 正浩 , 滝 雄太郎 , 宮西 洋太郎 , 角田 篤泰 , 菅原 研次 , 白鳥 則郎

２．発表標題
“デジタル寺院”：モデルと基盤技術

３．学会等名
情報処理学会コンシューマ・デバイス＆システム研究会

４．発表年
2019年

１．発表者名
Thierry Gidel, Shigeru Fujita, Claude Moulin, Kenji Sugawara, Takuo Suganuma, Yuki Kaeri, Norio Shiratori

２．発表標題
Enforcing Methodological Rules During Collaborative Brainstorming to Enhance Results

３．学会等名
IEEE-CSCWD, 2019（国際学会）

４．発表年
2019年

１．発表者名
藤田茂

２．発表標題
軽量N パーティ秘匿関数計算による“デジタル寺院” 実装の試み

３．学会等名
合同エージェントワークショップ&シンポジウム2019

４．発表年
2019年

１．発表者名 藤田茂
２．発表標題 軽量Nパーティ秘匿関数計算を用いたセキュアなIoTシステムの考察
３．学会等名 情報処理学会DPSWS，ポスター
４．発表年 2018年

１．発表者名 藤田茂
２．発表標題 途絶遅延ネットワーク上での秘密分散によるセキュアなIoTシステムの検討
３．学会等名 JAWS: Joint Agent Workshops & Symposium，ポスター
４．発表年 2018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	白鳥　則郎 (Shiratori Norio) (60111316)	中央大学・研究開発機構・機構教授 (32641)	

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			
フランス	Sorbonne Universit´es	Universit´e de Technologie de Compi`egne	Universit´e de Lille	