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　６ 年　 ６ 月 １７ 日現在

機関番号：３２６７５
研究種目：基盤研究(C)（一般）
研究期間：2018～2023
課題番号：１８Ｋ１１３０４

研究課題名（和文）ユーザ間の通信が不要な分散セキュリティ技術に関する研究

研究課題名（英文）Security Technologies without User Interaction in Distributed Environment

研究代表者
尾花　賢（Obana, Satoshi）

法政大学・情報科学部・教授

研究者番号：７０６３３６００

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）：ユーザ間が通信を行うことなく安全性を担保する暗号技術について検討を行った．具体的には，ユーザー間で通信を行うことなく自身の有する秘密情報を明かさずに，任意の関数に対し複数ユーザの秘密情報を入力とした関数値を計算する暗号プロトコルである NIMPC (Non-Interactive Multi Party Computation)，秘密情報を分散管理する秘密分散法において，ユーザ間で通信を行わずに分散情報を偽造したユーザの存在を検知する方式，ユーザ間の複雑な通信を行わずにリプレイを防止可能であることを特徴とする情報理論的に安全な秘匿認証通信方式等の研究開発を行った．

研究成果の学術的意義や社会的意義
分散型の暗号プロトコルでは，複雑な通信がプロトコルのデッドロックの要因となったり，プロトコルの実行速度のボトルネックとなることが多く，ユーザ間での複雑な通信を可能な限り排除することが理想である．本研究で提案した暗号プロトコルは全て，非常に単純な一方向の通信で構成されており，通信に起因するデッドロックの発生やパフォーマンス低下を防ぐことが可能となっている．しかし，複雑な通信を行うプロトコルと比較して，非対話的なプロトコルは通信量の増大を招くことが多いが，本研究ではNIMPC(非対話型のマルチパーティ計算)において，通信量の削減に成功している点で学術的意義は大きいと言える．

研究成果の概要（英文）：We have developed cryptographic protocols in a distributed environment. The notable feature of proposed protocols is that no interaction among users is required. More concretely, we have developed cryptographic protocols such as NIMPC (Non-Interactive Multi Party Computation), CDSS (Cheating Detectable Secret Sharing), and information theoretically secure authenticated encryption secure against replay attack. Here, NIMPC is a cryptographic primitive which enables users to evaluate any function with input secret information of users without revealing their secret information. Cheating Detectable Secret Sharing is a variant of secret sharing (a cryptographic protocol for split secret information into pieces (called share) in such a way that no partial information about the secret is revealed unless certain number of pieces are obtained by the adversary) with an extra functionality to detect the presence of forged shares in reconstructing the secret.

研究分野：暗号・情報セキュリティ

キーワード：マルチパーティ計算　非対話型プロトコル　通信量削減

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

クラウドの普及に伴い，機密度の高いデータがインターネットにつながったサーバ上に保存され，その情報に基づいて高度な情報処理を行うことが可能になった．このような情報の管理・利活用の方法はユーザに利便性をもたらす一方，公開ネットワークからアクセス可能なデータの情報漏洩対策が喫緊の課題となっている．公開ネットワークからアクセス可能なデータの情報漏洩対策として，複数のサーバが協調し，個々のサーバの保有するデータを秘匿しつつ全サーバが保有するデータに基づく情報処理を可能とするマルチパーティ計算が知られている．近年，マルチパーティ計算は目覚ましく発展し，複雑な処理を現実的な時間で実現できるようになってきた．例えば Araki らの提案したマルチパーティ計算(Araki et al., The ACM Conference on Computer and Communications Security, ACM CCS 2016)では，1 秒あたり 70 億回の論理ゲート演算を，入力を秘匿したまま行えることが示されている．しかし，マルチパーティ計算を行うためには，サーバ間で膨大なサイズのデータ通信が必要であり，サーバ間をつなぐネットワークの速度が処理のボトルネックとなっている．実際，近年行われているほとんどの研究では，複雑な処理を実時間で行うためにサーバ間を 10Gbps 程度の非常に高速なネットワークで接続しており，サーバ間が距離の離れた場所に配置されている現実的な環境下では，理想的な演算速度は実現できないという課題が残されている．また，マルチパーティ計算を行うために各サーバは膨大な演算処理を行う必要があり，スマートフォンなど，我々の身近にあるデバイスをサーバとして処理を実現することは困難な状況である．

上述のような状況に鑑みて，高速なネットワークや，演算処理が高速なデバイスを必要とせずに，高速にマルチパーティ計算を行うことを可能とする非対話型マルチパーティ計算(以下，NIMPC と記す)と呼ばれる技術が注目されている．非対話型マルチパーティ計算とは，Beimel ら(CRYPTO 2014)によって提案されたマルチパーティ計算の一種であり，各サーバS_iが保持する秘密x_iを秘匿しつつ複数のサーバの保持するデータ$x_1, x_2, \dots, x_n$ を入力とした情報処理の結果を出力する暗号プロトコルである．通常のマルチパーティ計算が，処理結果$f(x_1, x_2, \dots, x_n)$の計算過程で多量のサーバ間通信を必要とするのに対し，NIMPC では，プロトコル開始時に各プレイヤーに処理内容を表現する関数 f にのみ依存する特別な乱数R_iをサーバS_iに配布することにより，サーバS_iは関数値$f(x_1, x_2, \dots, x_n)$の計算時に他のサーバと通信を行う必要はなく，入力x_iと乱数R_iのみから計算される計算結果M_iを出力するだけで所望の関数値$f(x_1, x_2, \dots, x_n)$を全てのサーバが出力したM_iの合計値によって計算することが可能となる．乱数R_iはプロトコル実行開始前に配布しておけば良いため，関数値計算時に高速なネットワークが不要となり，無線 LAN など比較的低速なネットワークにつながったデバイスでもマルチパーティ計算を行うことが可能となる．また，既存の全ての非対話型マルチパーティ計算の方式では，サーバがローカルに行う演算は非常に少ない回数の排他的論理和や加算で実現されるため，スマートフォンなど，計算能力が貧弱なデバイスでも十分マルチパーティ計算を行うことが可能となる．

２．研究の目的

上述のように望ましい性質を有する NIMPC の主要な課題として，(1)サーバが保持する乱数のサイズの上界と下界を明らかにすること，(2)定められたプロトコルに従わない不正者に耐性のある方式を構築すること，の二点が挙げられる．(1)に関しては，Yoshida と Obana (International Conference on Information Security and Cryptography, ICISC 2015)により，乱数のサイズの下界がプロトコルで扱うことのできる関数集合の要素数と出力ビットの積で与えられることが示されている．また，任意の関数に対する NIMPC の上界は，Beimel ら(CRYPTO 2014)が最初に導出した後，Yoshida と Obana (ICISC 2015)，Obana と Yoshida (International Conference on Cryptology and Network Security, CANS 2016)により改善されてきた．しかし，現時点でも最良の上界と最良の下界の間には無視できないギャップが存在しており，このギャップを改善することは，より効率的なプロトコルをもたらすという実用上の意義だけではなく，効率的な非対話型マルチパーティ計算の構成な数学的構造を明らかにすることや，内在する理論的限界を明らかにすることが可能になるなど，理論的にも非常に重要な意義をもたらすことになる．(2)に関しては，関数の計算過程でサーバ間の通信を許す通常のマルチパーティ計算では既に研究が進んでおり，不正者に耐性のある方式が既に知られている．また理論的にも，安全な方式が構成できる不正なサーバ数の上限が明らかになるなど，多くの結果が得られている．一方，関数の計算過程でサーバ間の通信が許されない NIMPC では，関数の計算過程にサーバが不正を行う研究は従来行われておらず，非常にチャレンジングな目的課題となる．

３．研究の方法

NIMPC の理論的，実用的発展に向けて重要となる上述した二つの課題について，以下のような

方針で研究を推進する予定である．
(1) サーバが保持する乱数のサイズの上界と下界を明らかにする課題に関しては，まず，下界を明らかにして理論限界を求めた上で，上界の改善を行った．既存の方式のうち，最良の乱数サイズを達成している方式**(Obana, Yoshida, CANS 2016)**は，入力データのビット長に比例するサイズの乱数を必要としているが，本研究ではまず，乱数の個数が入力データのサイズに依存しない方式の構成を検討した．方式を定数個に抑える基本的なアイデアとしては，既存の方式では例を見ない入力データと乱数データが直接演算を行う方式を検討する．非対話型マルチパーティ計算を実現する既存の方式では，各サーバの出力から，サーバの保持する入力データの部分情報が漏洩することを防ぐため，入力データと乱数データの直接演算を避けて方式を構成していた．しかし，乱数データを情報理論的に安全な暗号プロトコルで利用される強ユニバーサル・ハッシュ関数族の鍵として利用し，入力データと乱数データ**(**鍵**)**との直接演算を施した結果を出力とすることにより，出力データから入力データを情報理論的に秘匿可能な方式が構成できると考え，強ユニバーサル・ハッシュ関数族をベースにした方式の構成を検討した．
(2) 定められたプロトコルに従わない不正者に耐性のある方式を構築する課題に関しては，まず非対話型のプロトコルでサーバが行える不正のパターンを洗い出すとともに，どのような不正であれば非対話型マルチパーティ計算で防止できるかを検討した．不正のパターンの洗い出しに関しては，非対話型マルチパーティ計算における通信と非常に近い通信モデルを有する非対話型の秘密分散法に着目し，非対話型秘密分散法における代表的な不正であるサーバによる出力データの偽造を非対話型マルチパーティ計算のモデルに適用することで新たなモデルを構築した．また，防止可能な不正の種類の特定に関しても，不正を防止可能な秘密分散法における不正検知技術や不正なサーバを特定する際に有用であった **AMD (Algebraic Manipulation Detection)**コード**(Cramer et al., Eurocrypt 2008)**やリード・ソロモン誤り訂正符号などの技術の非対話型マルチパーティ計算への適用可能性について検討を行い，効率的な実現方法の検討を行った．

４．研究成果

非対話型マルチパーティ計算に関する研究成果: **NIMPC** の理論的限界を明らかにする上で，まず下界の導出を行った．その結果，n個のサーバが計算する関数に入力する定義域の集合を$\mathcal{X} = \mathcal{X}_1 \times \mathcal{X}_2 \times \cdots \times \mathcal{X}_n$ **(**ここで，$\mathcal{X}_i$はi番目のサーバが関数に入力する値の集合**)**とし，関数の出力ビット長をLとしたとき，任意の関数に対する **NIMPC** で必要となる**(**全サーバの**)**乱数のサイズの下界が$L \cdot |\mathcal{X}|$ビットとなることが示された．

さらに，サーバが保持する乱数のサイズの上界の改善を行った．具体的には，**indicator** 関数と呼ばれる **NIMPC** の基本となる関数**(**定義域中のある **1** つの入力に対してのみ **1** を出力し，その他の入力に対しては **0** を出力する関数**)**に対して従来よりも乱数サイズの少ない具体的な **NIMPC** を提案することによって上界の改善を行った．上界の改善は研究期間内で二度行われた．パラメータdを$|\mathcal{X}_i| \leq d$を満たす値としたとき，従来知られている最も効率の良い **indicator** 関数に対する **NIMPC** の構成法で必要とされる乱数のビット長$d^2 \cdot n$であったのに対し，はじめに行った上界の改善では，乱数サイズを$\lceil \log_2 d \rceil^2 \cdot n$」へと削減した．$d = 2^{16}$ **(**各ユーザの入力を **16** ビットとすると**)**$d^2 = 2^{32}$に対して，$\lceil \log_2 d \rceil^2 = 2^8$であるため，必要な乱数が従来と比較して **1**/2^{24} 程度と劇的に削減されたこととなる．続けて実施した改良では，強ユニバーサル・ハッシュ関数族と呼ばれる関数属を用いて **indicator** 関数および **indicator** 関数を多ビット出力に拡張した **generalized indicator** 関数に対する効率的な **NIMPC** の提案を行った．提案方式で必要とされる乱数サイズは$4 \cdot \lceil \log_2 d \rceil$と，最初の改良と比較して必要な乱数サイズを$1/\log d$程度にまで削減することができた．提案した **generalized indicator** 関数に対する **NIMPC** から任意の関数に対する **NIMPC** を構成した結果，任意の関数に対する **NIMPC** を構成するために必要な乱数サイズは$(4 \cdot \lceil \log_2 d \rceil \cdot n + \max(2L, L + \lceil \log_2 d \rceil)) \cdot |\mathcal{X}|$となり，下界とのギャップを$4n + 2$程度にまで削減することができた．また，線形関数をベースにした強ユニバーサル・ハッシュ関数族と線形一次方程式の解空間の関係を検討することにより，必要な乱数サイズがさらに半分程度にまで削減できる見込みも得られた．また，**NIMPC** について，定められたプロトコルに従わない不正者に耐性のある方式の構築に向けて，このモデルにおいて不正者が行う可能性のある不正の整理を行った．具体的には，非対話型マルチパーティ計算において，プロトコルに従わない不正者が本来の関数の出力とは異なる値を出力させようとする不正なふるまいを整理し，不正，および不正に対する安全性のフォーマルな定義を行った．このような不正者に対して，強ユニバーサル･ハッシュ関数族のハッシュ値と，ハッシュ値を計算するための鍵の値を関数の出力に付与し，最終出力結果とハッシュ値が整合するか否かを確認する処理を追加することにより，不正者が存在しない場合の **NIMPC** の **2** 倍程度のオーバーヘッド**(**乱数サイズ，通信サイズの増加**)**で不正者の検知が可能となる一定の目処が付いた．提案した方式に関しては，ソフトウェア，およびハードウェア記述言語である **VHDL** で実装を行った．提案方式は拡大体上の乗算と加算のみで実装可能なため，ソフトウェアでもハードウェアでも非常に軽量な処理で実現できることが示された．

本研究では，非対話型マルチパーティ計算以外にも，複数のユーザが参加者となる実用的な

暗号プロトコルにおいて，ユーザ間の通信を可能な限り削減できるようないくつかのプロトコルの設計を行った．以下では NIMPC 以外で得られた成果について概説する．

秘密分散法(Secret Sharing)に関する研究成果: 秘密分散法とは秘密情報を分散環境において安全に管理する暗号技術である．秘密分散においては，秘密情報はシェアと呼ばれる複数の部分情報に分割されて管理される．秘密分散の中で，シェアの個数がn個存在し，そのうちの任意のk個から秘密が一意に復元され，$k-1$個未満のシェアからは秘密に関するいかなる部分情報も得られないことを保証する(k,n)閾値秘密分散法が多くの場面で利用されている．(k,n)閾値秘密分散法の特別なクラスとして，$k-1$個以下のシェアが改竄された場合でも高い確率で改竄を検知することができる **Cheating Detectable Secret Sharing (CDSS)**と呼ばれる秘密分散技術が知られている．本研究では，ユーザ間で通信を行わずに改竄を検知する **CDSS** について検討を行なった．**CDSS** については従来から多くの優れた方式が開発されてきたが，従来方式では不正を検出する検証関数 A として任意の定数δとΔに対し$A(s+\Delta)=A(s)+\delta$を満たす s の数が少ない関数を採用してきた．これに対して，本方式では$A(s)=C$となる根sの数が少ないことを保証するだけで安全性を証明できる新たな検証関数のクラスを導入し，巡回群上の冪乗関数がそのクラスに含まれることを示した．また，**2019** 年に国際会議 **NISS 2019 (International Conference on Networking, Information Systems & Security)**で発表された **CDSS** に対する攻撃法を提案した．**NISS 2019** で発表された **CDSS** は，不正の検出にユーザ間の通信が不要なだけでなく，不正検出のための演算が加法群$\mathbb{Z}/n\mathbb{Z}$上の加算だけで構成されており計算効率の良い方式であった．しかし，従来から有限体上の加法だけで構成する **CDSS** は安全ではないことが知られており，有限体上の加法と類似した構造を有する $\mathbb{Z}/n\mathbb{Z}$ 上の加法だけで構成された方式も十分な安全性を有しているとは考えづらかった．本研究では，特定の値に関して，$\mathbb{Z}/n\mathbb{Z}$上の加算と有限体上の加算が高い確率で一致することを示し，その数学的性質を利用して，確率 **1** で **NISS 2019** で提案された方式を攻撃(不正を検出されずに意図した値と異なる秘密に復元させることが)可能であることを示した．また，ユーザ間で通信を行わずに関数の値を計算するプロトコルにおいて不正を検出する方法として，**VMSS** と呼ばれる特別な秘密分散技術について検討を行なった．**VMSS** は秘密情報を安全に分散管理するとともに，ユーザ間の通信なしに管理された秘密の乗算を計算できる特別な秘密分散方式であり，不正を行うユーザを高い確率で検知する機能を備えている．今年度は，秘密の部分情報に有限体の要素一つを追加するだけでプロトコルのルールに従わない参加者の存在を検知する方式の開発を行った．

小型ロケットの秘匿認証通信に関する研究成果: 小型ロケットや小型人工衛星と基地局間の通信においてユーザ間のインタラクションを極力排除しつつ，通信の機密性と完全性に関して情報理論的安全性と呼ばれる理論上最も高い安全性を保証する方式の検討を行った．ユーザ間のインタラクションを極力排除した通信はデッドロックが発生しづらいという利点を有するが，複雑な通信を行えないことに起因して，リプレイ攻撃と呼ばれる過去の通信データを再送することによる通信データの偽造を防ぐことが困難であることが知られている．本研究で開発した秘匿認証通信の方式は時刻情報を利用してリプレイ攻撃を防止する点を特徴とする．本研究で開発した方式のプロトタイプは，国内初の民間ロケットに実験装置として搭載し，実際に宇宙空間での飛行という過酷な環境でも問題なく利用できることを確認した．

公開鍵暗号系に関する研究成果: 公開鍵暗号系においてユーザ間の通信を極力行わずに安全性を担保する方式として，暗号化したまま検索処理を行うことのできる検索可能暗号と呼ばれる技術について検討を行い，キーワード推測攻撃と呼ばれる検索可能暗号に特有な攻撃に対して安全であり，また内部サーバの鍵が漏洩した場合にも一定の安全性を保証する方式の提案を行った．また，サブリミナル・フリー署名と呼ばれる方式において，ユーザ間の通信を極力排除する方式の検討を行った．サブリミナル・フリー署名とは，デジタル署名を計算する署名者が署名の中に不正な情報を埋め込むことを防止できる署名方式である．従来，サブリミナル・フリー署名を実現するためには署名者に加え，署名に情報を埋め込むことを防止するためのユーザである監視者の存在を仮定し，監視者と署名者の間で複雑な通信を行うことによって署名への不正なデータ埋め込みを禁止していた．これに対し提案方式では，署名者と監視者の間の通信を簡略化するために完全準同型暗号を導入し，暗号化したまま署名の計算に必要なハッシュ値を計算することで，演算は複雑になるものの，ユーザ間の通信回数を従来方式に対して削減することに成功している．提案した方式は，署名の乱数部に不正な情報を埋め込むことを禁止可能な方式であり，署名者が監視者に気づかれずに不正な情報埋め込みに成功するまで何度も繰り返し署名生成を行う **Fail-Stop** チャネルと呼ばれる不正と，監視者が署名の中に不正に情報を埋め込む **Cackoo** チャネルと呼ばれる不正を共に防止可能なはじめての方式となっている．

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　2件）

１．著者名 Maki Yoshida, Satoshi Obana	４．巻 65
２．論文標題 Verifiably Multiplicative Secret Sharing	５．発行年 2019年
３．雑誌名 IEEE Transactions on Information Theory	６．最初と最後の頁 3233～3245
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TIT.2018.2886262	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 －

１．著者名 Maki Yoshida, Satoshi Obana	４．巻 86
２．論文標題 On the (in)efficiency of non-interactive secure multiparty computation	５．発行年 2018年
３．雑誌名 Designs, Codes and Cryptography	６．最初と最後の頁 1793-1805
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s10623-017-0424-7	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

〔学会発表〕　計22件（うち招待講演　1件／うち国際学会　11件）

１．発表者名 森岡澄夫，尾花賢，吉田真紀
２．発表標題 GNSS時刻情報を用いたセキュア通信用鍵同期機構における鍵キャッシュ設計
３．学会等名 第67回宇宙科学技術連合講演会
４．発表年 2023年

１．発表者名 Kiminori Kaneko, Satoshi Obana
２．発表標題 A Cryptanalysis against the Cheating Detectable Secret Sharing from NISS 2019
３．学会等名 Eleventh International Symposium on Computing and Networking, CANDAR 2023（国際学会）
４．発表年 2023年

１．発表者名
森岡澄夫，尾花賢，吉田真紀

２．発表標題
宇宙ロケット用セキュア通信のためのGNSS測位情報を用いた鍵同期方式

３．学会等名
2024年 暗号と情報セキュリティシンポジウム（SCIS 2024）

４．発表年
2024年

１．発表者名
森岡澄夫，尾花賢，吉田真紀

２．発表標題
小型宇宙機用セキュア通信におけるGNSS時刻情報を用いた鍵同期方式

３．学会等名
第66回宇宙科学技術連合講演会

４．発表年
2022年

１．発表者名
Sho Sugauchi, Satoshi Obana

２．発表標題
Fully Subliminal-Free Schnorr Signature for Nonce

３．学会等名
The Tenth International Symposium on Computing and Networking (CANDAR 2022)（国際学会）

４．発表年
2022年

１．発表者名
Kaito Uemura, Satoshi Obana

２．発表標題
Exposure Resilient Public-key Encryption with Keyword Search against Keyword Guessing Attack

３．学会等名
International Conference on Security and Cryptography - SECRYPT（国際学会）

４．発表年
2021年

１．発表者名
Kaichi Sato, Satoshi Obana

２．発表標題
Cheating Detectable Secret Sharing Scheme from Multiplicative Homomorphic Authentication Function

３．学会等名
International Symposium on Computing and Networking Workshops (CANDARW)（国際学会）

４．発表年
2021年

１．発表者名
森岡澄夫，尾花賢，吉田真紀

２．発表標題
情報理論的安全性を有する宇宙ロケット用セキュア通信方式の性能実証飛行

３．学会等名
2022年 暗号と情報セキュリティシンポジウム (SCIS 2022)

４．発表年
2022年

１．発表者名
Satoshi Obana, Maki Yoshida

２．発表標題
Efficient Constructions of Non-interactive Secure Multiparty Computation from Pairwise Independent Hashing

３．学会等名
17th International Joint Conference on e-Business and Telecommunications, ICETE 2020 - Volume 2: SECRYPT（国際学会）

４．発表年
2020年

１．発表者名
Maki Yoshida, Satoshi Obana

２．発表標題
Compact Verifiably Multiplicative Secret Sharing

３．学会等名
International Symposium on Information Theory and Its Applications, ISITA 2020（国際学会）

４．発表年
2020年

１．発表者名
吉田真紀，森岡澄夫，尾花賢

２．発表標題
観測ロケットMOMO3号機によるセキュア通信方式の基礎実験

３．学会等名
セキュリティサマーサミット2019

４．発表年
2019年

１．発表者名
Haruna Higo, Toshiyuki Isshiki, Masahiro Nara, Satoshi Obana, Toshihiko Okamura, Hiroto Tamiya

２．発表標題
Security Requirements for Store-on-Client and Verify-on-Server Secure Biometric Authentication

３．学会等名
Emerging Technologies for Authorization and Authentication, ETAA 2019（国際学会）

４．発表年
2019年

１．発表者名
吉田真紀，尾花賢

２．発表標題
検証可能な乗法秘密分散の効率向上

３．学会等名
コンピュータセキュリティシンポジウム2019

４．発表年
2019年

１．発表者名
Tomoki Agematsu, Satoshi Obana

２．発表標題
Almost Optimal Cheating-Detectable (2,2,n) Ramp Secret Sharing Scheme

３．学会等名
International Symposium on Computing and Networking, CANDAR 2019（国際学会）

４．発表年
2019年

１．発表者名
森岡澄夫，尾花賢，吉田真紀

２．発表標題
情報理論的安全性を有する小型衛星・小型ロケット用セキュア通信方式の実装検討と飛行評価

３．学会等名
2020年暗号と情報セキュリティシンポジウム，SCIS2020

４．発表年
2020年

１．発表者名
森岡澄夫，尾花賢，吉田真紀

２．発表標題
超小型衛星・小型ロケット用セキュア通信のための情報理論的安全性の検討

３．学会等名
第62回宇宙科学技術連合講演会

４．発表年
2018年

１．発表者名
Satoshi Obana

２．発表標題
How to Guarantee Integrity in Secret Sharing

３．学会等名
The Sixth International Symposium on Computing and Networking（招待講演）（国際学会）

４．発表年
2018年

１．発表者名
Tomoki Agematsu, Satoshi Obana

２．発表標題
How to Realize Highly Accurate Computation with Fully Homomorphic Encryption

３．学会等名
5th International Workshop on Information and Communication Security（国際学会）

４．発表年
2018年

１．発表者名
Motoki Miyano, Satoshi Obana

２．発表標題
Updatable Searchable Symmetric Encryption with Fine-Grained Delete Functionality

３．学会等名
5th International Workshop on Information and Communication Security（国際学会）

４．発表年
2018年

１．発表者名
奈良成泰，田宮寛人，肥後春菜，一色寿幸，尾花賢，岡村利彦

２．発表標題
テンプレートをクライアントが持つオンライン秘匿生体認証の安全性

３．学会等名
2019年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
田宮寛人，奈良成泰，肥後春菜，一色寿幸，尾花賢，岡村利彦

２．発表標題
テンプレートをクライアントが持つオンライン秘匿生体認証方式

３．学会等名
2019年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
尾花賢，吉田真紀，森岡澄夫

２．発表標題
小型衛星・小型ロケット用通信のセキュリティモデルとプロトタイプ実装

３．学会等名
第84回コンピュータセキュリティ研究会研究発表会

４．発表年
2019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
研究協力者	上村　海斗 (Uemura Kaito)	法政大学大学院・情報科学研究科	
研究協力者	上松　知貴 (Agematsu Tomoki)	法政大学大学院・情報科学研究科	
研究協力者	須河内　翔 (Sho Sugauchi)	法政大学大学院・情報科学研究科	
研究協力者	佐藤　開智 (Kaichi Sato)	法政大学大学院・情報科学研究科	
研究協力者	金子　公徳 (Kiminori Kaneko)	法政大学大学院・情報科学研究科	

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