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　４ 年　 ５ 月 ２０ 日現在

機関番号：１４１０１
研究種目：若手研究(B)
研究期間：2017～2021
課題番号：１７Ｋ１２６４０

研究課題名（和文）計算内在暗号化技術の計算モデル

研究課題名（英文）Computational Models in Cryptography for Encrypted Computation

研究代表者
河内　亮周（Kawachi, Akinori）

三重大学・工学研究科・教授

研究者番号：００３９７０３５

交付決定額（研究期間全体）：（直接経費）　　3,000,000円

研究成果の概要（和文）：本研究では計算プロセスが内在する暗号化技術に親和性の高い計算モデルを解析し，効率的でかつ高機能な暗号プロトコル設計へ応用することを目的に研究を進めた．研究成果として，行列ベクトル積に人為ノイズを乗せる計算モデルにおける公開鍵暗号のエラー解析技術や同モデル上での公開鍵暗号の代数的性質を利用して参加者の持つデータのプライバシーを保護しながら計算を行う秘匿計算，さらに同モデル上でのコミットメントスキームという電子封筒，等の技術の開発を行い，その幅広い応用を示した．さらにその研究で得た知見でより高度な安全性を達成しつつ通信回数が一度だけの高効率の秘匿計算プロトコルの計算資源の解析技術を得た．

研究成果の学術的意義や社会的意義
本研究で主に用いたモデルは人為ノイズを加えられた行列ベクトル積という従来の暗号理論で広く用いられてきた整数論に基づくものと異なる数学的構造を持っている．この構造は今後暗号プロトコルの脅威となる量子計算機の攻撃に対する耐性を持ちながら単純で高速な計算が期待できる特徴を持っており，量子計算機の脅威が顕在化する将来の情報通信における安全な情報セキュリティ技術の確立に資する成果であると言える．

研究成果の概要（英文）：This study analyzed a computational model with high affinity to cryptographic techniques with inherent computational processes and applied it to develop efficient and highly functional cryptographic protocols. Our results include error analysis techniques for public-key encryption schemes in a computational model in which artificial noise is added to the matrix-vector product, confidentiality computation in which the algebraic properties of public-key cryptography are exploited to protect the privacy of the participant's data, and a commitment scheme, an electronic envelope, based on the model, and showed its wide range of applications. Furthermore, we developed a technique for analyzing the computational resources of a highly efficient secure computation protocol that achieves a higher level of security and communicates only once.

研究分野：暗号理論，計算量理論

キーワード：秘匿計算　コミットメントスキーム　耐量子計算機暗号

１．研究開始当初の背景

1976 年の Diffie と Hellman の鍵共有プロトコルや 1977 年の Rivest, Shamir, Adelman の RSA 公開鍵暗号方式を端に発する現代暗号理論は元来，通信においてメッセージを敵対者から秘匿することを基本としてきたが，その後の発展によりメッセージ秘匿を超えて情報セキュリティに幅広い応用を与えてきた．特に近年，計算プロセスの暗号化や暗号化情報に対する計算プロセス実行といった計算プロセスが内在する暗号化技術（以下，計算内在暗号化技術）の研究がいくつかのブレイクスルーにより爆発的に発展している．

Gentry は長年未解決であった完全準同型暗号(Fully Homomorphic Encryption; FHE)の具体的方式を与え，現代暗号理論を含む情報セキュリティ各分野に大きな衝撃を与えた[Gentry, FOCS 2009]．FHE とは暗号化された情報を復号せずに演算できる，例えば平文情報 a の暗号文 Enc(a)と平文情報 b の暗号文 Enc(b)が与えられたとき，a と b を入力とした関数 f を計算して得られる f(a,b)の暗号文 Enc(f(a,b))が復号することなく直接的に計算可能，となる方式である．つまり暗号化された情報に対してそのプライバシーを守りながら計算プロセスが適用可能となるため，幅広い応用が展開できる．例えば，弱い計算資源しか持たないクライアントが計算対象のデータの秘匿性を守ったまま潤沢な計算資源を持つサーバにそのデータに対する計算を委託する委託計算が FHE により実現可能であるが[Chuang et al., CRYPTO 2010]この技術はクラウドコンピューティングや IoT のための情報セキュリティに活用可能である．

また Barak らはプログラム難読化，つまりプログラムの実行可能性を保持したままその記述の解読を不可能にする技術，の暗号理論的定式化に成功し，一部の強い難読化は理論的に実現不可能であることを示した[Barak et al., JACM 2001]が，弱い難読化概念である識別不可能難読化(Indistinguishability Obfuscation; iO)の実現可能性については未解決であった．これに対し Garg らは iO の具体的方式を提案することで未解決問題を解決し，さらに iO から新しいアプローチで様々な重要な暗号プリミティブ（基本要素技術）や高機能暗号プロトコルが構成されることが示されたことで大きなブレイクスルーとなった[Garg et al., FOCS 2013]．例えば，一方向性関数と iO から落とし戸付き一方向性置換[Bitansky et al., TCC 2016]，対称鍵暗号と iO から公開鍵暗号[Sahai & Waters STOC 2013]が構成可能である．また参加者の各自のデータを他の参加者に秘匿したまま参加者全員のデータから計算を行う秘匿計算への応用も示されており[Garg & Polychroniadou, TCC 2015]，FHE と同様に情報セキュリティへの応用展開が可能である．FHE や iO 以外にも計算プロセスのプライバシー保護を行う乱択符号化[Applebaum et al., Comput. Compl. 2006]，暗号文の復号可能条件を計算によって決定する関数型暗号[Boneh et al., TCC 2011]など計算内在暗号化技術の研究は多様な発展を遂げている．

２．研究の目的

計算プロセスが内在する暗号化技術はプログラム難読化や完全準同型暗号など近年数多くのブレイクスルーにより飛躍的な発展を遂げ，暗号理論の可能性を大きく拡げている．しかしその技術で計算プロセスを実現するのは論理回路などの親和性が必ずしも高くはない計算モデルであり，またその計算汎用性の高さから効率的な構成が一般的に困難である．本研究では計算内在暗号化技術に適した計算モデルの設計・解析を行い，それを計算内在暗号化技術へ展開することで高い汎用性と安全性・効率性の達成を目指す．また委託計算・秘匿計算などのプライバシー保護のための暗号プロトコルへ応用展開し，現実的な機能と高い効率性を両立できる技術を確立する．

３．研究の方法

本研究を円滑に遂行していくために，申請者と専門分野が異なる研究者チームからの研究支援体制を確立する．申請者は来年度より暗号理論・情報セキュリティの研究を行っている宮地充子教授（大阪大学）の研究室に異動予定であるため，当該研究室のスタッフと研究連携を行う．また外部専門家として西巻陵氏（NTT セキュアプラットフォーム研究所研究主任）に本研究の研究協力者を依頼し，既に承諾を得ている．研究体制の詳細は以下のとおりである．

申請者の専門分野は計算量理論・暗号理論の境界領域であり，計算モデルの計算能力解析と暗号プロトコル設計と安全性解析の研究実績を持つ．申請者はその双方の背景が必要となる計算内在暗号化技術のための計算モデル構築およびその計算能力・機能解析を中心に研究を進める．世界屈指の専門家である西巻氏は既に有名国際会議にてプログラムへの電子透かしという計算内在暗号化技術の先進的成果を発表しており，本研究のための高度な暗号理論の専門知識を有している．さらに西巻氏の所属するセキュリティ基盤研究グループは暗号理論全般において世界的に著名な研究グループであり申請者と共同研究実績のある藤崎英一郎氏・草川恵太氏も在籍している．また西巻氏は長期研究滞在していた Daniel Wichs 助教(Northeasten Univ.)のグループをはじめとして MIT，Stanford 大学などの強力な米国研究グループとの共同研究による繋がりを持っている．必要に応じてこれらの研究グループとの連携体制のグローバルな拡大も可能であり，西巻氏を中心とした研究連携を通じて新しいモデルにおける計算内在暗号化技術

への展開，その効率性・安全性の解析を推進する．

また前述のとおり，計算内在暗号化技術のための計算モデル構成には代数的アプローチが有効であると予想される．楕円曲線の暗号理論における数理構造解析をはじめとした暗号理論での代数構造解析の専門家である宮地充子教授，田中覚特任助教（大阪大学宮地研）との連携を図り，計算モデルの代数構造の解析を進める．

また宮地教授は CREST「ビッグデータ統合利活用促進のためのセキュリティ基盤技術の体系化」の研究代表者であり，蘇春華助教，Cheng Chen-Mou 特任講師（大阪大宮地研）をはじめとするプロジェクトメンバーはビッグデータを対象としたプライバシー保護技術の研究に取り組んでいる．本研究は背景で述べたように委託計算や秘匿計算といったプライバシー保護技術を実現する暗号プロトコルへの応用可能であるため，蘇助教・Chen-Mou 特任講師および当該メンバーとの研究連携によりプライバシー保護技術への応用展開を推進する．

４．研究成果

平成 29 年度の成果は以下の通りである．2015 年に Canetti らは内部乱数を持つような論理回路を難読化する確率的論理回路難読化器が満たすべきいくつかの性質および安全性を定義し，その中で静的入力識別不可能性と呼ばれる安全性を満たす確率的論理回路難読化器の構成を穴開け可能疑似ランダム関数と準指数時間安全な決定性論理回路に対する識別不可能性難読化器から示していた．今年度の研究において彼らが定義していた最悪時入力識別不可能性という安全性について検討し，その亜種の安全性を満たすような確率的論理回路難読化器の構成を準指数時間安全な疑似ランダム関数と準指数時間安全な識別不可能性難読化器から示した．

また難読化器から構成され，また難読化器に近い機能を持つ汎用標本器という暗号プリミティブがあり，様々な暗号プロトコルのセットアップアルゴリズムを実行する信頼された機関を統一化するために元々構成されていたが，高度な暗号プロトコル構成に有用であることも知られており，例えば 2016 年に Hofheiz らによって通常の公開鍵暗号と汎用標本器を組合わせることで ID ベース公開鍵暗号が構成されていた．今年度の研究では，彼らの構成を一般化することで階層型 ID ベース公開鍵暗号を構成し，その安全性を示した．また，同様に汎用標本器から階層型 ID ベース公開鍵暗号を構成する方法として 2017 年の Ma らの構成が知られていたが，彼らの構成方法および本研究における構成方法の効率を解析し，効率を比較することで本研究における構成方法の効率が優れていることを示した．

平成 30 年度においては計算内在型暗号のモデルとして行列－ベクトル積に人為的雑音を加えるフレームワークに着目し，その計算能力および暗号理論的安全性に関する研究を行った．特に，現在米国標準技術研究所が実施している耐量子暗号標準化に対して Melchor らが 2018 年に提案している行列－ベクトル積に雑音を加える誤り訂正符号ベースの公開鍵暗号システム HQC においてその暗号文上での準同型演算を解析し，線形関数計算および大小比較計算を可能にする秘匿計算プロトコルの構成を行った．またその暗号理論的安全性を誤り訂正符号における計算困難問題に基づいて証明した．この秘匿計算プロトコルにおいて参加者 A が入力 x を持ち，参加者 B が関数 f（例えば線型関数 f(x)=ax+b の場合には f の記述である対(a,b)，大小比較の場合には x>b なら f(x)=1，それ以外なら f(x)=0 を記述する値 b）を持っている場合に，それぞれが相手に自身の持つ情報を明らかにせずに計算結果 f(x)を得ることが可能となる．既存のプロトコルでも同様の計算を可能とするものが既に提案されているが，それらと比較して本研究提案のプロトコルでは量子計算機による有効な攻撃が見つかっていない点ならびに紛失通信と呼ばれる高コストのプロトコルを利用しない点について優越性を持っている．

またその他関連する計算モデルとしてブール型有限ダイナミカルシステムの研究を行い，その計算量理論的な性質の解明を行った．特に本モデルにおいて利用できる素子の種類を限定した場合のエデンの園問題と呼ばれるブール型有限ダイナミカルシステムモデルにおける計算困難性の解析を行い，計算モデルの能力およびその限界についての知見を得た．

令和元年度においては，計算内在型暗号の中でも重要な技術である乱択符号化を応用してコミットメントスキーム（電子封筒）と呼ばれる暗号基盤要素の構成を行い，その耐量子安全性（量子コンピュータによる攻撃に耐える安全性）を解析した．コミットメントスキームはゼロ知識証明システムなどネットワーク認証技術などに応用される基盤技術である．特に本研究で提案されたコミットメントスキームは出力局所性と呼ばれる並列計算機で高速化するのに適した構造を持っており，既存のコミットメントスキームと比較して並列化による高速化が容易になっているという特徴を持っている．既存研究として Applebaum らは同様に暗号基盤要素である耐衝突ハッシュ関数が乱択符号化に基づいて構成していたが，本研究では研究プロジェクトで得た行列解析の知見により更にその結果を発展させることによって構成を可能とした．また米国標準技術研究所が実施している耐量子暗号標準化において Melchor らが 2018 年に提案している行列－ベクトル積に雑音を加える誤り訂正符号ベースの公開鍵暗号システム HQC に基づいた秘匿計算プロトコルを提案していたが，この秘匿計算プロトコルおよび基となる公開鍵暗号システム HQC の復号誤り確率は実験的には尤もらしいことが確認できる数学的仮定をおいて解析されていた．本研究においては本研究プロジェクトにて得られた確率解析の技術を駆使し，その数学的仮定無しで復号誤り確率を評価する手法を得ることができ，数学的により厳密に復号誤り確率の評価を行うことに成功した．さらに情報理論的安全な秘匿計算プロトコルの亜種である秘匿同時通報および条件付き秘密開示と呼ばれるプロトコルの通信効率の限界をいくつかの具体

な計算タスクについて明らかにした.

令和二年度では計算内在暗号化技術の発展として，秘密計算の実用上重要なモデルである秘密同時通信プロトコルおよび条件付き秘密開示プロトコルにおける必要十分な通信ビット数および事前共有乱数ビット数の解析を行った．秘密同時通信プロトコルとは各参加者の秘密情報を明らかにせずに暗号メッセージをそれぞれ評価者に送り，評価者が参加者の秘密情報から計算できる関数値を暗号メッセージから計算するプロトコルである.

秘密同時通信プロトコルおよび条件付き秘密開示プロトコルにおいて必要な通信ビット数と事前乱数ビット数の一般的な関係性を明らかにした．その応用として，任意の関数を計算する秘匿同時通信プロトコルにおいて，評価者が関数に依存しない設定での必要十分な通信ビット数および十分な事前乱数ビット数は既に解析されていたが，その関係を用いることによって，必要な事前乱数ビット数を証明し，既知のプロトコルが事前乱数ビット数について最適であることを示した．また秘密同時通信プロトコルおよび条件付き秘密開示プロトコルの両方において重要な具体的関数に対する必要な通信ビット数，事前乱数ビット数を明らかにした.

令和三年度では，データを秘密にしたまま計算を行う代表的なモデルである秘密同時通信および条件付き秘密開示において汎用的な通信複雑度（秘密情報を保持している複数の参加者から関数値を計算する評価者へ秘密を漏らさずにデータを送るための通信量）と乱数複雑度（評価者へ秘密情報を漏らさない通信を実現するための参加者間の共有乱数の量）の解析を行った．秘密同時通信では複数の参加者が秘密情報を保持しており，その秘密情報を入力とする関数（例えば平均値など）を共有乱数を利用して暗号化された情報を評価者に送ることで，評価者に情報を漏らすことなく計算させることを目的とする．また条件付き秘密開示では共通の秘密を持った複数の参加者が各参加者個別の入力と共有乱数を利用して暗号化された情報を評価者に送り，参加者の個別入力が与えられた条件を満たすときだけ評価者が秘密を復元できることを要請する．これらのモデルの解析の研究結果として，いくつかの代表的な関数に対して組合せ論的な手法および情報理論的な手法によって新しい通信複雑度の下界証明，つまり通信量削減の原理的な限界を示すことができた.

またこの二つのプロトコルに対して通信複雑度の下界から乱数複雑度の下界を示すための非常に汎用的な関係式を示した．この結果によって新たに多くの具体的な関数について共有乱数削減の限界を示すことができた．いくつかの重要な例においては上下界が定数倍の範囲で一致することも確認することができた．例えば，任意の論理関数を計算する汎用的評価者を持つ秘密同時通信に対する通信量複雑度の上下界は入力長の指数関数であり，乱数複雑度の上界は入力長の指数関数であることが知られていたが，今回の通信複雑度と乱数複雑度の関係式より乱数複雑度の下界が入力長の指数関数であることが証明でき，乱数複雑度の上下界の強い関係も明らかにすることができた.

５．主な発表論文等

〔雑誌論文〕　計3件（うち査読付論文　3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 Akinori Kawachi	４．巻 C01-7
２．論文標題 Hamming Weight of Product of Random Sparse Polynomials	５．発行年 2020年
３．雑誌名 IEICE Proceedings Series: The 2020 International Symposium on Information Theory and its Applications	６．最初と最後の頁 368-371
掲載論文のDOI（デジタルオブジェクト識別子） 10.34385/proc.65.C01-7	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 Kawachi Akinori、Ogihara Mitsunori、Uchizawa Kei	４．巻 762
２．論文標題 Generalized predecessor existence problems for Boolean finite dynamical systems on directed graphs	５．発行年 2019年
３．雑誌名 Theoretical Computer Science	６．最初と最後の頁 25～40
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.tcs.2018.08.026	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 KAWACHI Akinori、KAWANO Kenichi、LE GALL Francois、TAMAKI Suguru	４．巻 E102.D
２．論文標題 Quantum Query Complexity of Unitary Operator Discrimination	５．発行年 2019年
３．雑誌名 IEICE Transactions on Information and Systems	６．最初と最後の頁 483～491
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transinf.2018FCP0012	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 －

〔学会発表〕　計16件（うち招待講演　2件／うち国際学会　2件）

１．発表者名 河内 亮周
２．発表標題 量子攻撃者に対する安全性証明技術の進展
３．学会等名 電子情報通信学会総合大会企画セッション「量子計算と暗号の進展」，ADI-1-2（招待講演）
４．発表年 2021年

１．発表者名
河内 亮周，西村 治道

２．発表標題
量子秘密同時メッセージプロトコルの通信計算量

３．学会等名
2020年度冬のLAシンポジウム，[9]

４．発表年
2021年

１．発表者名
河内 亮周，吉田 真紀

２．発表標題
秘密同時メッセージと条件付き秘密開示に対する乱数長下界

３．学会等名
情報セキュリティシンポジウム(SCIS)，3A2-3

４．発表年
2021年

１．発表者名
Hideaki Miyaji, Akinori Kawachi, and Atsuko Miyaji

２．発表標題
String commitment schemes with low output locality

３．学会等名
AsiaJCIS 2019（国際学会）

４．発表年
2019年

１．発表者名
河内 亮周

２．発表標題
量子攻撃者に対する安全性概念

３．学会等名
電子情報通信学会総合大会企画セッション「量子計算と暗号の発展」，ADI-1-2（招待講演）

４．発表年
2020年

１．発表者名
河内 亮周，吉田 真紀

２．発表標題
Private Simultaneous Messages および Conditional Disclosure of Secrets に関する情報理論的下界

３．学会等名
2019年度冬のLAシンポジウム，[3]

４．発表年
2020年

１．発表者名
河内 亮周

２．発表標題
符号ベース公開鍵暗号HQCにおける復号誤り確率の理論的解析

３．学会等名
暗号と情報セキュリティシンポジウム(SCIS)，2A1-5

４．発表年
2020年

１．発表者名
宮地 秀至，河内 亮周，宮地 充子

２．発表標題
定数4出力局所性を持つコミットメント方式

３．学会等名
暗号と情報セキュリティシンポジウム(SCIS)，1A2-4

４．発表年
2020年

１．発表者名
堀内 弘武，森本 尚之，山田 俊行，河内 亮周

２．発表標題
解の個数を限定した充足可能性問題の計算困難性

３．学会等名
電子情報通信学会コンピュテーション研究会，IEICE-COMP2019-34

４．発表年
2019年

１．発表者名
河内 亮周

２．発表標題
疎なランダム多項式の積のハミング重み

３．学会等名
2019年度夏のLAシンポジウム，[9]

４．発表年
2019年

１．発表者名
祁 儀穎，河内 亮周，宮地 充子

２．発表標題
準巡回符号に基づく二者間秘匿大小比較プロトコル

３．学会等名
電気情報通信学会情報セキュリティ研究会IEICE-ISEC2018-110

４．発表年
2019年

１．発表者名
祁 儀穎，河内 亮周，宮地 充子

２．発表標題
準巡回シンドローム復号問題に基づく線形関数秘匿計算

３．学会等名
コンピュータセキュリティシンポジウム2018 4A2-3

４．発表年
2018年

１．発表者名
Akinori Kawachi and Yoshiki Tabata

２．発表標題
On Indistinguishability Obfuscation of Probabilistic Circuits for Worst-case-input Subexponentially Indistinguishable Samplers

３．学会等名
The 12th International Workshop on Security（国際学会）

４．発表年
2017年

１．発表者名
田端 芳樹，河内 亮周

２．発表標題
最悪時入力標本器に対する確率的回路の識別不可能性難読化器

３．学会等名
2018年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
大塚 俊輔，宮地 充子，河内 亮周

２．発表標題
ユニバーサルサンプラを用いた階層型IDベース暗号方式の提案

３．学会等名
電子情報通信学会情報セキュリティ研究会

４．発表年
2017年

１．発表者名
大塚 俊輔，河内 亮周，宮地 充子

２．発表標題
ユニバーサルサンプラを用いた階層型IDベース暗号方式の評価

３．学会等名
電子情報通信学会情報通信システムセキュリティ研究会

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

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