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

平成 ２９ 年　 ４ 月　 ７ 日現在

機関番号：３２６１３
研究種目：基盤研究(C)（一般）
研究期間：2014～2016
課題番号：２６３３００１９

研究課題名（和文）時間制約およびセキュリティを考慮した公平分割手法

研究課題名（英文）Fair division protocols considering time constraints and security

研究代表者
真鍋　義文（Manabe, Yoshifumi）

工学院大学・情報学部（情報工学部）・教授

研究者番号：８０４６６４０８

交付決定額（研究期間全体）：（直接経費）　　3,700,000円

研究成果の概要（和文）：公平分割を行うプロトコルにおいて、参加者が同時にプロトコルを実行する必要があるという制約をなくし、参加者が自分の都合のよい時刻に自由に参加・退出が可能にしたうえで、公平性を達成するプロトコルを考案した。
また、参加者の財に対する好みの情報が他の参加者に知られるとその情報を用いた不正が可能となるので、自分の好みを他人に一切知られることなく公平分割を実行することが必要である。この条件を満足するセキュアな公平分割プロトコルを示した。

研究成果の概要（英文）：Conventional cake-cutting protocols require that all players must execute a protocol at the same time. This work eliminates this restriction. In the proposed protocol, all player can join to and leave from the cake-cutting procedure at his/her convenience. How to cut the cake to maximize each player's utility by this setting is shown.
Security is another important issue to realize fair cake-cutting. If a player's preference to the cake is known to another player, the player can cut the cake falsely and obtain more utility. In order to prevent this flaw, we show a secure cake-cutting protocol using a secure auction protocol.

研究分野：情報学基礎

キーワード：公平分割　ケーキ分割　オンラインアルゴリズム　セキュリティ

１．研究開始当初の背景

複数人の間で分割可能な単一の財を公平に分割する問題は、ケーキ分割問題と呼ばれ、領土の分割やセールスマンの担当エリアの割り当てや業務の担当時間の割り振りなど実生活で起きるさまざまな問題をモデル化しており、多くの研究が行われてきている。しかしながら現在までの主なケーキ分割アルゴリズムは、全参加者が１か所に同時に集まることを前提としており、遠隔地からの参加の場合には、遅延が０とみなせる通信路の利用が必要である。この前提は遅延のあるインターネットの利用時には成立しない。インターネット上でオークションを提供することにより、オークションが身近になり多くの人が利用するようになったように、ケーキ分割アルゴリズムもインターネット上で実行可能とすることにより、グローバル企業内での業務の割り振りなど、多くの人が利用するようになることが期待される。

２．研究の目的

本研究の目的は、時差のある状況下など、各参加者が参加できる時間帯が異なっている場合にも公平な分割を実現する手法を求めることを目的とする。さらに、このような途中参加・途中離脱を許す状況下においては、未参加の者がすでに離脱した参加者から、その参加者の得た途中情報を得ることにより不当に有利な分割結果を得る可能性がある。このような不正行為を不可能にするには、各参加者に途中状況に関する不要な情報を一切与えないアルゴリズムが必要となる。

このような、時間制約とセキュリティを考慮した公平分割プロトコルを得ることを本研究の目的とした。

３．研究の方法

上記の目的を達成するため、以下のテーマに取り組んだ。

(1) 参加者の時間制約のモデル化と、そのモデルのもとでの公平分割プロトコルの考案
(2) 分割不可能な財に対する公平分割プロコルの考案
(3) セキュアな公平分割プロトコル実現のために必要な暗号プリミティブのモデル化とセキュアプロトコルの考案
(4) 公平性達成問題の、ネットワークなど他分野の問題への応用

４．研究成果

各テーマに対する研究成果を以下にまとめる。

(1) 参加者の時間制約のモデル化と、そのモデルのもとでの公平分割プロトコルの考案

既存研究のモデル化のもとでは、参加者数が不明である場合に最後の参加者が分割を得られないデッドロックが発生することを明らかにした。また、後に到着する参加者が有利となるため、参加を遅らせるインセンティブが働くことも明らかにした。従って、時間とともに財の価値が減少するという現実的なモデルを立てた。このモデルの元では、一定時間待機後に退出を許すことが可能であり、デッドロックがなく、早く参加するインセンティブを持つプロトコルを考案した。

(2) 分割不可能な財に対する公平分割プロコルの考案

分割不可能な異なる種類の財が存在する場合に公平に分割することが求められることも多い。この問題について、近似解を求めるアルゴリズムを示した。さらに、参加者が時々刻々現れる場合のオンライン公平分割プロトコルを示した。オフラインで解を求める場合との近似比の最悪値を求め、シミュレーション実験により提案プロトコルが最悪値より多くの場合よい値を達成していることを示した。

(3) セキュアな公平分割プロトコル実現のために必要な暗号プリミティブのモデル化とセキュアプロトコルの考案

参加者間で自分の評価値は相手に隠した状態で相手の持つ値との計算を行う必要がある。好みの情報をセキュアに求めるプロトコルや、カードを用いて財の交換をセキュアに行うプロトコル、セキュアオークションプロトコルを用いることによるナイフ移動法での公平分割プロトコルの実現など、公平分割問題を実現するために重要なセキュアプロトコルの考案を行った。

(4) 公平性達成問題の、ネットワークなど他分野の問題への応用

モバイルアドホックネットワーク(MANET)を題材に、公平性達成問題の他分野への応用を考察した。MANET においては各参加者が他の参加者間の通信の中継を行う。無線端末は電池容量が限られていることが多く、他者の通信の中継で電池が消耗することは不公平である。中継に対する公平性を達成するための通信経路選択プロトコルを示し、シミュレーション実験により提案プロトコルの有効性を示した。

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計　２　件）

① Masaru Yoshimachi and Yoshifumi

Manabe: ``Battery Power Management Routing Considering Participation Duration for Mobile Ad Hoc Networks,'' Journal of Advances in Computer Networks, Vol. 4, No. 1, pp.13-18 (March 2016). **査読有**
DOI: 10.18178/JACN.2016.4.1.196

② Yoshifumi Manabe, Risako Otsuka, and Tastuaki Okamoto: ``A Cryptographic Moving-Knife Cake-Cutting Protocol with High Social Surplus,'' Journal of Information Processing Vol. 23, No. 3, pp.299-304 (May 2015). **査読有**
DOI: 10.2197/ipsjjip.23.299

〔学会発表〕（計　１９　件）

① **吉町優,真鍋義文**: ``**アドホックネットワーク向けの公平性経路制御** AODV **プロトコル**,'' 2017 **年電子情報通信学会総合大会** B-7-54(Mar. 2017).**名城大学（名古屋市）**

② **清水航平,真鍋義文**: `` **戦略性を考慮した分割不可能な財のオンライン配分方式**,'' 2017 **年電子情報通信学会総合大会** D-1-8(Mar. 2017). **名城大学（名古屋市）**

③ **安井賢也**, **真鍋義文**: ``**合理的な複数の敵に対し、信頼性・機密性を満たす秘密分散通信**,'' **暗号と情報セキュリティシンポジウム** SCIS2017 1A1-3(Jan. 2017). **ロワジールホテル那覇（那覇市）**

④ Yoshifumi Manabe: ``Cake-cutting protocols: How fair allocation can be achieved?''8th International Conference on Information Management and Engineering (ICIME 2016) (Nov. 2016). **招待講演** Istanbul(Turkey).

⑤ Masaru Yoshimachi and Yoshifumi Manabe: ``A New AODV Route Discovery Protocol to Achieve Fair Routing for Mobile Ad Hoc Networks,'' Proc. of 6th IEEE International Conference on Information Communication and Management (ICICM 2016), pp.222-226 (Oct. 2016). **査読有** Hatfield (UK).

⑥ Kohei Shimizu and Yoshifumi Manabe: ``An Online Allocation Algorithm of Indivisible Goods,'' Proc. of 6th IEEE International Conference on Information Communication and Management (ICICM 2016), pp.57-61 (Oct. 2016). **査読有** Hatfield (UK).

⑦ **吉町優,真鍋義文**: ``MANET **向けの通信性質を考慮した公平性ルーティングプロトコル**,'' **第１２回情報科学ワークショップ**(Sep. 2016). **工学院大学富士吉田セミナー校舎（富士吉田市）**

⑧ **清水航平,真鍋義文**: `` **分割不可能な財のオンライン配分問題**,'' **第１２回情報科学ワークショップ**(Sep. 2016). **工学院大学富士吉田セミナー校舎（富士吉田市）**

⑨ Koki Kubo and Yoshifumi Manabe: ``A Non-blocking Online Cake-cutting Protocol,'' Proc. of 3rd International Conference on Mathematics and Computers in Sciences and Industry(MCSI 2016), pp.258-263 (Aug. 2016)**査読有** Crete(Greece)

⑩ Takuya Ibaraki and Yoshifumi Manabe: ``A More Efficient Card-Based Protocol for Generating a Random Permutation Without Fixed Points,'' Proc. of 3rd International Conference on Mathematics and Computers in Sciences and Industry (MCSI 2016), pp.252-257 (Aug. 2016). **査読有** Crete(Greece)

⑪ Tsuyoshi Komatsubara and Yoshifumi Manabe: ``Game-theoretic Security of Commitment Protocols under a Realistic Cost Model,'' 30th IEEE International Conference on Advanced Information Networking and Applications(AINA 2016), pp.777-783 (March 2016). **査読有** Crans-Montana(**スイス**)

⑫ **久保光毅,真鍋義文**: ``**途中退出を許容したオンラインケーキ分割プロトコル**,'' 2016 **年電子情報通信学会総合大会** D-1-3(Mar. 2016) **九州大学（福岡市）**

⑬ **清水航平,真鍋義文**: ``**分割不可能な財のオンライン配分方式**,'' 2016 **年電子情報通信学会総合大会** D-1-4(Mar. 2016). **九州大学（福岡市）**

⑭ **朝比奈佑馬**, **真鍋義文**: ``**秘匿回路計算のゲーム理論的安全性**,'' **暗号と情報セキュリティシンポジウム** SCIS2016 3A2-5(Jan. 2016) ANA **クラウンプラザホテル熊本ニュースカイ（熊本市）**

⑮ Yuta Urushiyama and Yoshifumi Manabe: ``A Double-Private epsilon-fuzzy Matching Protocol,'' 5th International Conference on Workshop on IT Convergence and Security (ICITCS2015), pp.348-351 (August 2015). **査読有** Kuala Lumpur(**マレーシア**)

⑯ Yuji Mochizuki and Yoshifumi Manabe: ``A Privacy-Preserving Collaborative Filtering Protocol Considering Updates,'' 10th Asia-Pacific Symposium on Information and Telecommunication Technologies(APSITT2015), RS-5-3, pp.1-3 (August 2015) **査読有** Colombo(**スリランカ**)

⑰ Kohei Shimizu and Yoshifumi Manabe:

``An Allocation Algorithm of Indivisible Goods," 10th Asia-Pacific Symposium on Information and Telecommunication Technologies(APSITT2015), RS-3-3, pp.1-3 (August 2015). 査読有 Colombo(スリランカ)

⑱ 稲永隆大,真鍋義文: ``ブロックごとに分かれた利用時間の希望割り当て問題," 2015 年電子情報通信学会総合大会 D-1-7(Mar. 2015). 立命館大学（草津市）

⑲ 清水航平,真鍋義文: ``分割不可能な財に対する配分方式," 2015 年電子情報通信学会総合大会 D-1-6(Mar. 2015). 立命館大学（草津市）

〔図書〕（計　0　件）

〔産業財産権〕

○出願状況（計　0　件）

○取得状況（計　0　件）

〔その他〕
ホームページ等
http://www.ns.kogakuin.ac.jp/~wwa1056/

６．研究組織
(1)研究代表者
真鍋　義文（MANABE, Yoshifumi）
工学院大学・情報学部・教授
研究者番号：８０４６６４０８