T2R2 東京科学大学 リサーチリポジトリ
Science Tokyo Research Repository

論文 / 著書情報
Article / Book Information

題目(和文)	実演に適したカードベースプロトコルの構成について
Title(English)	On the Construction of Easy to Perform Card-Based Protocols
著者(和文)	品川和雅
Author(English)	Kazumasa Shinagawa
出典(和文)	学位:博士(理学), 学位授与機関:東京工業大学, 報告番号:甲第11391号, 授与年月日:2020年3月26日, 学位の種別:課程博士, 審査員:渡辺 治,田中 圭介,伊東 利哉,尾形 わかは,西崎 真也,縫田 光司
Citation(English)	Degree:Doctor (Science), Conferring organization: Tokyo Institute of Technology, Report number:甲第11391号, Conferred date:2020/3/26, Degree Type:Course doctor, Examiner:,,,,,
学位種別(和文)	博士論文
Category(English)	Doctoral Thesis
種別(和文)	論文要旨
Type(English)	Summary

Powered by T2R2 (Science Tokyo Research Repository)

（博士課程）
Doctoral Program

論 文 要 旨

THESIS SUMMARY

系・コース： Department of, Graduate major in	数理・計算科学 系 コース	申請学位（専攻分野）： Academic Degree Requested	博士 Doctor of 理学
学生氏名： Student's Name	品川 和雅	指導教員（主）： Academic Supervisor(main)	渡辺 治
		指導教員（副）： Academic Supervisor(sub)	田中 圭介

要旨（英文 800 語程度）
Thesis Summary（approx.800 English Words ）

Secure computation enables a set of players holding secret inputs to compute a joint function of the inputs without revealing the inputs. Although secure computation is usually achieved by the use of computers over a network, secure computation can also be done using a deck of physical cards. This research area is called card-based cryptography. In card-based protocols, input information is encoded by a sequence of face-down cards, which is called a commitment. Then, operations are applied in front of all players to the sequence of commitments produced by the players. These operations include a permutation, turning, and a shuffle. The goal of card-based protocols is either to publicly reveal the output value or to produce a commitment to the output value without revealing the inputs. Protocols of the former type are called non-committed format protocols, while protocols of the latter type are called committed format protocols. Since the output commitment of a committed format protocol can be used to the input commitment of another protocol, to compute any Boolean circuit, it is sufficient to construct committed format protocols for the NOT, AND, and COPY functions.

In the first part of this dissertation, we study card-based protocols using a small number of shuffles restricted to uniform closed shuffles, which are shuffles whose permutation set is closed and in which each permutation is chosen uniformly and randomly. To the best of our knowledge, there is no general protocol in the literature that uses a constant number of shuffles even with the use of non-uniform or non-closed shuffles. In this work, we construct a general protocol with a single uniform closed shuffle. This protocol achieves the minimum number of shuffles, as it is impossible to securely compute any non-trivial function without shuffles (i.e., with permutations and turnings only). In addition, the proposed protocol only requires 24q+2n cards, where n is the input length and q is the number of cards in a circuit computing the function. This is achieved by introducing a card-based variant of the garbled circuit methodology. We also construct a general protocol with two pile-scramble shuffles, which are uniform closed shuffles that are easy to perform. This is accomplished by introducing a parallel batching technique, which combines multiple pile-scramble shuffles in parallel into one pile-scramble shuffle using a relatively small number of additional cards.

In the second part of this dissertation, we study card-based protocols using private permutations instead of shuffles. A private permutation is an operation that covertly applies

a permutation chosen by a player according to the player's input bit. A private permutation is considered easier to perform than a shuffle since every private permutation can be easily physically performed while it is not known how to physically perform certain shuffles. However, since private permutations are necessarily performed at a physically isolated location so as not to reveal the chosen permutation, protecting against malicious attacks in private permutations is difficult. Thus, protocols with private permutations are considered easier to perform but less secure than protocols with shuffles. We solve this dilemma by defining a new security notion called active security that captures malicious attacks in private permutations. Furthermore, we construct several protocols with active security. In particular, for any Boolean function that maps n bits to one bit, we construct a general protocol with n private permutations, which has the minimum number of private permutations. We also construct a general protocol with 2n+7 cards, which is optimized in terms of the number of cards. In addition, we construct several protocols for concrete functions that are efficient with a small number of cards and private permutations.

In the third part of this dissertation, we study card-based protocols based on polygon-shaped cards. Suppose that we wish to compute a multi-valued function. Although a protocol for any Boolean function implies a protocol for any multi-valued function, this conversion usually increases the number of cards and shuffles. To circumvent this inefficiency, we introduce two types of polygon-shaped cards possessing a rotational symmetry: cyclic cards and dihedral cards. Based on cyclic cards, we construct efficient protocols for concrete functions such as addition, subtraction, copy, and multiplication. It is also possible to construct a protocol for any function multi-valued function based on our new technique, oblivious conversion; however, a large number of cards is required. Based on dihedral cards, we construct efficient protocols for interesting predicates such as a carry predicate, equality predicate, and greater than predicate. Because every protocol based on cyclic cards also work based on dihedral cards, by combining the addition protocol and the carry protocol, we can efficiently compute addition and subtraction over large integers.

備考 ： 論文要旨は、和文 2000 字と英文 300 語を 1 部ずつ提出するか、もしくは英文 800 語を 1 部提出してください。
Note : Thesis Summary should be submitted in either a copy of 2000 Japanese Characters and 300 Words (English) or 1copy of 800 Words (English).

注意：論文要旨は、東工大リサーチリポジトリ(T2R2)にてインターネット公表されますので、公表可能な範囲の内容で作成してください。
Attention: Thesis Summary will be published on Tokyo Tech Research Repository Website (T2R2).