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)	審査の要旨
Type(English)	Exam Summary

（博士課程）

論文審査の要旨及び審査員

報告番号	甲第　　号		学位申請者氏名		品川 和雅	
論文審査 審査員		氏　名	職　名		氏　名	職　名
	主査	渡辺 治	教授	審査員	西崎 真也	教授
	審査員	田中 圭介	教授		縫田 光司	東京大学 准教授
		伊東 利哉	教授			
		尾形 わかは	教授			

論文審査の要旨（2000 字程度）

本論文は「On the Construction of Easy to Perform Card-Based Protocols（実演に適したカードベースプロトコルの構成について）」と題し，英文 6 章よりなる。カードベースプロトコルとは，入力情報に対応するカード列を与えられたとき，計算結果に対応するカード列を得るための手続きのことである。計算結果の正しさ（正当性）と，手続きを観測した場合でも入力情報が漏れない性質（安全性）が要求される。計算手続き（特にシャッフル）が複雑な場合，プロトコルを実演することは難しくなる。本論文は，実演に適したプロトコルを構成するために，(I)単純なシャッフルのみを用いる設定でシャッフル回数の少ないプロトコルの構成，(II)シャッフルの代わりに秘匿置換（別の単純な操作）を用いるプロトコルの構成を行う。また，既存研究はブール関数に特化しているが，(III)多値を自然に扱うことのできるカードを用いるプロトコルの構成を行う。

第 1 章「Introduction」では，本研究の背景及び成果の概要を述べ，論文の構成を示している。

第 2 章「Preliminaries」では，本研究で用いる概念や用語を定義している。

第 3 章「Protocols with Uniform Closed Shuffles」では，上述の(I)について述べている。任意の関数を計算する際のシャッフル回数について，既存研究では回路の素子数という自明な上界しか知られていなかった。本研究では，1 回のシャッフルのみを用いるプロトコルを構成した。ここで，そのシャッフルは uniform closed という良い性質を持っている。なお，シャッフルが 0 回だと非自明な関数は計算できないため，この結果はシャッフル回数について最適である。この結果に加えて，2 回のパイルスクランブルシャッフルを用いたプロトコルも構成した。パイルスクランブルシャッフルは，極めて単純なシャッフルであるため，実演に適している。

第 4 章「Protocols with Private Permutations」では，上述の(II)について述べている。秘匿置換とは，ある特定のプレイヤーが自身の入力に従って，並び替えをするか否かを秘密裏に選択するという操作である。この操作は，シャッフルと比べて手操作が簡単であるが，悪意のあるプレイヤーは入力に従わずに秘匿置換を実行する可能性がある。本研究では，悪意のあるプレイヤーに対しても秘密情報が漏れない性質（active 安全性）を定義し，この安全性を満たすプロトコルを構成した。具体的には，任意の関数（入力数 n）に対して，2n+7 枚の active 安全なプロトコルを構成した。この構成は，カード枚数は十分に少ないが，秘匿置換の回数は n の指数関数である。別の構成として，秘匿置換 n 回，カード枚数 2^n の active 安全なプロトコルも構成した。この構成は，秘匿置換の回数について最適である。さらに，具体的な関数に対するより効率的な active 安全なプロトコルも構成している。

第 5 章「Protocols Based on Polygon-Shaped Cards」では，上述の(III)について述べている。通常のブール値用のプロトコルで多値の演算を行う場合，カード枚数およびシャッフル回数の増加が避けられない。そこで本研究では，多値を自然に扱うことのできる多角形形状のカードとして，巡回カード（cyclic card）と二面カード（dihedral card）を導入した。巡回カードを用いて，多値の加算・減算・コピー関数に対する効率的なプロトコルを構成した。入力数 n の指数関数枚のカードを許せば，任意の多値関数を n 回のシャッフルで計算することも可能である。二面カードは，巡回カードの上位互換であり，上記のプロトコルに加えて，加算のキャリービット，等号判定，大小判定といった述語計算を効率的に実現できる。特に，加算のキャリービットが計算できるようになったので，大きな整数の加算が効率的に実現できるようになった。

第 6 章「Conclusion」では，今後の研究課題について述べている。

本論文で提案されたモデルはカードベース暗号のみならず今後の情報セキュリティ技術の設計と解析の進展に寄与することも期待できる。以上をまとめると，本論文はカードベース暗号ならびに情報セキュリティ技術の基本的理解に大きく貢献しており，博士（理学）の学位論文として十分な価値があるものと認められる。