論文 / 著書情報
Article / Book Information

題目(和文)	暗号文拡大率が定数である Non-Committing 暗号の構成
Title(English)	Constructions for Non-Committing Encryption with Constant Ciphertext Expansion
著者(和文)	吉田雄祐
Author(English)	Yusuke Yoshida
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12169号, 授与年月日:2022年9月22日, 学位の種別:課程博士, 審査員:田中 圭介,伊東 利哉,尾形 わかは,鹿島 亮,安永 憲司
Citation(English)	Degree:Doctor (Science), Conferring organization: Tokyo Institute of Technology, Report number:甲第12169号, Conferred date:2022/9/22, 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		吉田 雄祐	
論文審査 審査員		氏　名	職　名		氏　名	職　名
	主査	田中 圭介	教授	審査員	安永 憲司	准教授
	審査員	伊藤 利哉	教授			
		尾形 わかは	教授			
		鹿島 亮	准教授			

論文審査の要旨（2000字程度）

本論文は「Constructions for Non-Committing Encryption with Constant Ciphertext Expansion（暗号文拡大率が定数であるNon-Committing暗号の構成）」と題し，英文で全5章から構成されている．

公開鍵暗号は事前に鍵共有を行なっていない送信者と受信者が，攻撃者にメッセージを盗聴されることなく安全に通信するために使用される暗号技術である．公開鍵暗号は用いられる状況と目的によって適切な安全性を満たすことが求められる．本論文の主題である Non-Committing 暗号（NCE）とは，適応的安全なマルチパーティ計算においてメッセージを送信するために必要な安全性を満たす公開鍵暗号である．マルチパーティ計算は暗号理論における中心的なテーマの一つであり，その中でも適応的安全性は攻撃者が任意のタイミングで参加者のもつ秘密情報を入手できることを想定した非常に強力な安全性である．マルチパーティ計算全体の通信量に直接影響する Non-Committing 暗号の暗号文拡大率，すなわちメッセージ1ビットあたりに必要な暗号文長を削減することは，適応的安全なマルチパーティ計算の理論において重要な課題として研究されてきていた．

本論文では送信者が用いた乱数を確実に消去することや，ランダムオラクルの存在を仮定しない標準モデルにおいて，Non-Committing 暗号の新しい設計方針を示すとともに，初めて暗号文拡大率が定数である Non-Committing 暗号方式を二種類構成している．ひとつは Decisional Diffie-Hellman 問題の困難性に基づいて構成しており，もうひとつは Learning with Errors 問題の困難性に基づいて構成している．

第1章「Introduction」では本論文の背景であるマルチパーティ計算と既存の Non-Committing 暗号方式，関連研究について振り返り，論文全体の概要について述べている．また論文中で用いる表記を導入している．

第2章「Basics and Definitions of NCE」ではまず，シミュレーションによる安全性定義の拡張として Non-Committing 安全性と紛失サンプル可能性が定義できることを示している．つぎに Non-Committing 安全性を満たす公開鍵暗号として Non-Committing 暗号の定義を与えている．

第3章「NCE with $O(\lambda)$ Ciphertext-Expansion」では本論文で提案する NCE を構成するための新しい設計方針を示すため，セキュリティパラメータ λ に対して暗号文拡大率が $O(\lambda)$ である Non-Committing 暗号を構成している．具体的にはまず，Non-Committing 暗号の正当性と安全性を弱めた弱 Non-Committing 暗号を新たに定義し，紛失サンプル可能な鍵カプセル化メカニズムから暗号文拡大率が $O(\lambda)$ である弱 Non-Committing 暗号を構成している．次に，ワイヤタップ符号と呼ばれる情報理論的技術を用いて暗号文拡大率を定数倍より大きく増長させることなく弱 Non-Committing 暗号を通常の Non-Committing 暗号に変換できることを示している．

第4章「NCE with Constant Ciphertext-Expansion」ではまず，紛失サンプル可能なカメレオン暗号という中間の暗号技術を導入し，Decisional Diffie-Hellman 問題と Learning with Errors 問題に基づいた構成をそれぞれ与えている．つぎに，第3章と類似した構成方法によって紛失サンプル可能なカメレオン暗号から暗号文拡大率が定数である弱 Non-Committing 暗号を構成し，ワイヤタップ符号を用いて変換することで本論文の主成果である暗号文拡大率が定数である Non-Committing 暗号を構成している．

第5章「Conclusion」では本論文の総括を行なっている．

以上のように本論文では適応的安全なマルチパーティ計算において基礎的役割を果たす Non-Committing 暗号について，標準モデルで最も暗号文拡大率が小さな方式を提案するだけでなく，紛失サンプル可能なカメレオン暗号や弱 Non-Committing 暗号，ワイヤタップ符号など，Non-Committing 暗号の構成における有用な技術の安全性定義，構成，安全性証明を与えるなど多くの知見を与えており，理学上貢献するところ大である．よって，本論文は博士(理学)の学位論文として十分価値があるものと認める．