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)	論文要旨
Type(English)	Summary

（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 数理・計算科学　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	吉田 雄祐	指導教員（主）： Academic Supervisor(main)	田中 圭介
		指導教員（副）： Academic Supervisor(sub)	

要旨（和文 2000 字程度）
Thesis Summary（approx.2000 Japanese Characters ）

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二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 Encryption(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望ましい安全性である．マルチパーティ計算全体の通信量に直接影響する NCE の暗号文拡大率,すなわちメッセージ 1bit 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されていた．

本論文では暗号方式の使用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，NCE 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 NCE 方式を二種類，Decisional Diffie-Hellman (DDH) 問題と Learning with Errors(LWE)問題の困難性に基づいてそれぞれ構成している．

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 NCE 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，一般的に，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．次に具体的に公開鍵暗号と Non-Committing 安全な公開鍵暗として NCE の定義を与えている．

第 3 章「NCE with O(λ) 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(λ)である NCE を構成している．具体的にはまず，NCE の正当性と安全性を弱めた Weak NCE の定義を提案し，紛失サンプル可能な鍵カプセル化メカニズム(KEM)から暗号文拡大率が O(λ)である Weak NCE 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 Weak NCE を NCE 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，DDH 問題と LWE 問題に基づいた構成をそれぞれ与えている．次に，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 Weak NCE 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 NCE を構成している

第 5 章「Conclusion」では本論文の総括を行なう．

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).

（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 数理・計算科学 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	吉田 雄祐	指導教員（主）： Academic Supervisor(main)	田中 圭介
		指導教員（副）： Academic Supervisor(sub)	

要旨（英文 300 語程度）
Thesis Summary (approx.300 English Words)

Public-key encryption is a cryptographic primitive used for establishing a secure channel between two parties. Depending on the situation and purpose, public-key encryption scheme must satisfy appropriate security requirements.

Non-committing encryption (NCE) is a public-key encryption scheme which satisfies a security notion essential to establish a secure channel in adaptively secure multi-party computation (MPC) protocols. Informally, NCE can generate a dummy ciphertext. The dummy ciphertext is indistinguishable from the real ciphertext. Moreover, we can explain the dummy ciphertext as encryption of an arbitrary message by producing consistent randomness.

It has been a challenge in the theory of adaptively secure MPC to find an NCE scheme with small ciphertext expansion (required ciphertext length per bit of message).

This thesis proposes the first NCE schemes with constant ciphertext expansion in the standard model (i.e., without assuming the randomness used in cryptosystem can be securely erased or use of the random oracle). We show two instantiations of the scheme, one from the Decisional Diffie-Hellman (DDH) problem and another from the Learning with Errors (LWE) problem.

Before constructing the constant ciphertext expansion scheme, we demonstrate the new approach to construct NCE through the construction of a simpler NCE scheme based on obliviously samplable key-encapsulation mechanism (KEM). The ciphertext expansion of this simpler scheme is $O(\lambda)$ for security parameter λ. In detail, we use KEM to construct a weak NCE scheme with $O(\lambda)$ ciphertext expansion. Weak NCE is NCE where its correctness and security requirements are weakened. Then weak NCE is amplified to full-fledged NCE scheme using information theoretical primitive called wiretap codes. This amplification increase the cipher text expansion only by a constant factor.

The constant ciphertext expansion scheme is obtained by using a primitive called obliviously samplable chameleon encryption, instead of KEM in the above construction. We show instantiations of obliviously samplable chameleon encryption based on the DDH and the LWE problems.

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).