論文 / 著書情報
Article / Book Information

題目(和文)	代理人再暗号化方式に対する概念と構成
Title(English)	Notions and Constructions on Proxy Re-Encryption
著者(和文)	ｸﾞｴﾝﾏｲﾝ ﾊｰ
Author(English)	Manh Ha Nguyen
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9613号, 授与年月日:2014年9月25日, 学位の種別:課程博士, 審査員:田中　圭介,小島　定吉,渡辺　治,鹿島　亮,脇田　建
Citation(English)	Degree:, Conferring organization: Tokyo Institute of Technology, Report number:甲第9613号, Conferred date:2014/9/25, 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

専攻： Department of	数理・計算科学　専攻	申請学位（専攻分野）： Academic Degree Requested	博士 Doctor of　（　理学　）
学生氏名： Student's Name	MANH HA NGUYEN	指導教員（主）： Academic Advisor(main)	田中　圭介
		指導教員（副）： Academic Advisor(sub)	

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

Public-key encryption is a fundamental cryptographic primitive with which we can communicate securely over possibly insecure network without shared secret information in advance. Proxy re-encryption (PRE) extends the traditional public key encryption to support the delegation of the decryption rights, in which a proxy is allowed to transform ciphertexts computed under the public-key of the delegator into other ciphertexts for the delegatee. The proxy, however, learns nothing about the underlying messages encrypted, and has no knowledge of the secret keys of the delegators and the delegatees.

PRE schemes have many applications in encrypted email forwarding, distributed file storage systems, law enforcement, digital rights management (DRM), and outsourced filtering of encrypted spam. For PRE schemes, security against chosen ciphertext attacks (CCA security) is nowadays considered as a standard security notion needed in most practical applications/situations where PRE schemes are used. There are many notions of CCA security for PRE proposed so far. However, these notions do not capture all of the essential aspects of the CCA security. In this thesis, we focus on CCA security notions for PRE and constructing schemes, which are secure in the sense of these security notions.

We begin with Chapter 1 providing some backgrounds and our contributions on PRE. Going on, in Chapter 2, after introducing notations used in the whole thesis, we review the factoring assumption, the properties of bilinear maps and the intractability assumptions that our schemes rely on. Next, we review the definitions on public key encryption, symmetric key encryption, signature, and target-collision resistant hash function, which are the main tools in our constructions.

According to the direction of transformation, PRE can be classified into two types: unidirectional and bidirectional. In unidirectional PRE, the proxy can only transform ciphertexts from the delegator to the delegatees. While in bidirectional PRE, the proxy can transform ciphertexts in both directions. PRE can also be categorized into multi-hop PRE, in which the ciphertexts can be transformed from Alice to Bob and then to Charlie and so on, and single-hop PRE, in which the ciphertexts can only be transformed once.

In Chapter 3, we first recall the concepts and the security notions of bidirectional multi-hop, bidirectional single-hop, and unidirectional single-hop PRE. We then present new CCA security definitions for both bidirectional single-hop, and unidirectional single-hop PRE by extending those of the previous works. In order to point out why our security models are stronger than those of the previous works, we present concrete PRE

schemes, which are secure in their model, but are not secure in our models. In this chapter, we also review the model and security definitions of conditional PRE (CPRE), which is a variant of proxy re-encryption, where only the ciphertext satisfying one condition set by the delegator can be transformed by the proxy and then decrypted by the delegatee.

In Chapter 4, we focus on constructing PRE schemes, which are based on the hardness of the factoring problem. In particular, we present three PRE schemes. The first is a CPA-secure bidirectional multi-hop PRE scheme. The second is a CCA-secure bidirectional single-hop PRE scheme. The last is a CCA-secure unidirectional single-hop PRE scheme. The first is in the standard model, and the others in the random oracle model. In order to construct the second and the third schemes, we propose a new factoring-based strong signature scheme which is a variant of the Schnorr signature scheme.

In Chapter 5, we first show that the PRE scheme proposed by Shao, Liu, and Zhou in the Journal of Systems and Software 85(3) is vulnerable to chosen-ciphertext attack. We then propose a unidirectional single-hop PRE scheme which is secure in the full CCA security model. Our scheme relies on mild complexity assumptions in bilinear groups without random oracles.

In Chapter 6, we first show that the CPRE scheme proposed by Liang, Liu, Tan, Wong, and Tang in ICISC2012 is vulnerable to chosen-ciphertext attack. We then propose two CPRE schemes which are secure against the selective and adaptive condition chosen-ciphertext attack, respectively. These schemes are extended from the CCA-secure PRE scheme proposed in Chapter 5. Our schemes are the first CPRE schemes which are secure against condition chosen-ciphertext attack without random oracles.

We conclude the thesis and give several open problems in Chapter 7.