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)	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		NGUYEN MANH HA	
論文審査 審査員		氏　名	職　名		氏　名	職　名
	主査	田中　圭介	准教授	審査員	脇田　建	准教授
	審査員	小島　定吉	教授			
		渡辺　治	教授			
		鹿島　亮	准教授			

論文審査の要旨（2000字程度）

本論文は、「Notions and Constructions on Proxy Re-Encryption」と題して、 英文７章からなる。

代理人再暗号化方式（Proxy Re-Encryption、PRE）は公開鍵暗号の拡張の一種である。通常の公開鍵暗号の場合、受信者Aの秘密鍵を用いることでのみ復号することが可能である。しかしPREの場合、受信者A宛の暗号文を受信者B宛に変換するための再暗号化鍵を第三者である代理人が用いることにより、 A宛の暗号文を復号することなくB宛に変換することが可能となる。PRE の研究において、暗号文を別の暗号文に変換するという機能を持ちつつ、選択暗号文攻撃（Chosen Ciphertext Attack、CCA）に対して安全な方式の設計を行うことは興味深い研究対象となっており、今までも複数のCCAの概念、およびその安全性を満たす方式が提案されてきた。しかしながら、それらはCCAの本質全体を捉えているとはいえない。本論文では、この安全性概念を再考し、新しいCCA概念を提案する。さらに、この新しい安全性概念を満たす具体的な方式の提案も行っている。

第１章「Introduction」では、代理人再暗号化に関する過去の研究について述べた後、本研究の成果の概要を述べている。

第２章「Preliminaries」では、準備として暗号学的な仮定と本論文で使う基本的なプリミティブを述べている。

代理人再暗号化は再暗号化鍵の性質によって、いくつかのタイプに分類されている。単一の再暗号化鍵でユーザーAからユーザーBへ、ユーザーBからユーザーAへの双方向の暗号文変換ができるなら双方向方式と呼ばれ、どちらか単方向のみ変換出来るなら単方向方式と呼ばれる。また、再暗号化鍵で一度暗号文を再暗号化するとそれ以上再暗号化が不可能になる方式は単一ホップ型方式と呼ばれ、複数回再暗号化が可能な方式は複数ホップ型方式と呼ばれる。

第３章「Models and Security Notions」では、PREの分類について説明し、分類したそれぞれに対して安全性概念を提案する。また、既存研究で提案された概念との比較も行っている。さらに、条件付き代理人再暗号化についても述べ、これに対してのCCA安全性の概念も提案している。

第４章から第６章では、第３章で提案した安全性を満たす具体的な方式を提案し、それぞれの安全性を証明している。

第４章「Schemes Based on Factoring」では、素因数分解問題に基づいて３つの方式を提案している。双方向複数ホップ型の方式はWeeの選択平文攻撃に対して安全な公開鍵暗号を基にして構成されている。残り２つの方式、すなわち双方向単一ホップ型と単方向複数ホップ型のPREを構成するために､Schnorr署名の素因数分解版である新しい電子署名も提案している。これも本論文の１つの成果である。提案された３つの方式は素因数分解問題に基づく代理人再暗号化として初めての方式である。

第５章「A Scheme with Bilinear Maps」では、既存研究としてShao、Liu、Zhouにより提案された方式が、彼らの主張する安全性を満たさないことを具体的な攻撃を行うことで示している。そして、ペアリングを用いた具体的な方式を提案し、第３章で提案したCCA安全性を満たすことを証明している。

第６章「CCA-Secure Conditional Schemes without Random Oracles」では、代理人再暗号化の条件付き版を考察している。条件付き方式では、再暗号化鍵にある条件が付加され、それを使うと同じ条件の付けられた暗号文しか変換できない。既存研究としてLiang、Liu、Tan、Wong、Tangによって提案された条件付き方式が、彼らの主張する安全性を満たさないことを具体的な攻撃を行うことで示している。そして、第５章で提案した方式を基にして２つの具体的方式を提案し、安全性の証明を行っている。提案された方式はランダムオラクルなしでは初めてのCCA安全な条件付き代理人再暗号化方式である。

第７章「Conclusion」では、まとめと今後の課題を述べている。

以上をまとめると、本研究は代理人再暗号化に関する様々な新しい技術を提案するとともに、分野全体を詳しく解説している。提案内容は、今後の代理人再暗号化に関する研究の重要な基礎となる可能性をもち、理学上大きく貢献している。よって、本論文は博士(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。