# 審 査 の 結 果 の 要 旨

氏　名　　石 坂　理 人

本論文は、「Public-Key Cryptosystems Resilient to Computationally Hard-to-Invert Leakage（計算量的逆変換困難漏洩耐性を持つ公開鍵系暗号技術）」と題し、実在する脅威であるサイドチャネル攻撃等に起因する秘密情報漏洩に関して、強力な漏洩の理論的モデル化である計算量的逆変換困難漏洩に対して安全な、種々の公開鍵系暗号技術の構成法を提案している。論文の構成は、「Introduction」と「Preliminaries」を含め、6章から成る。

第1章は「Introduction（序論）」で、本研究の背景や動機、加えて本研究の貢献について述べている。具体的には、秘密情報漏洩への耐性を考慮しない安全性モデルは現実の脅威を捉え切れていない点を指摘し、考えられる限りのあらゆる対策を施したとしても全ての秘密情報漏洩を完全に防ぐことは困難であるが故に漏洩耐性は実用面で重要であると指摘している。加えて、数ある漏洩耐性安全性モデルの中で、逆変換困難漏洩（HL）に対する耐性を考慮するモデルは、実用的観点及び理論的観点から特に重要であることを説明し、本研究の意義を明らかにしている。

第2章は「Preliminaries（準備）」と題し、本論文において使用される計算量的困難性仮定を導入している。また、公開鍵暗号、ID ベース暗号（IBE）、電子署名、ID ベース署名（IBS）、属性ベース署名（ABS）を含む種々の暗号要素技術の標準的な安全性要件及び機能的要件を記述し、漏洩耐性を考慮しない場合の理論的枠組みをまとめている。

第3章は「IBE with Hard-to-Invert Leakage-Resilience（逆変換困難漏洩耐性を持つ ID ベース暗号）」と題し、HL 耐性を持つ ID ベース暗号方式の具体的構成法を提案している。ID ベース暗号は、任意の ID 情報（電話番号等）を公開鍵として使用可能な公開鍵暗号である。また、通常の公開鍵暗号単体では実現不可能な高度な機能を実現できる、いわゆる高機能公開鍵暗号として、最も基本的なものの一つである。そのため、本研究のように暗号要素技術への新たな脅威に対する耐性を持たせて安全性を高める研究をする場合、ID ベース暗号に関する研究は実用的及び理論的に重要であるとされる。本章では、HL 耐性を持つ ID ベース暗号構成法を提案するのみならず、暗号分野の最高峰の学術会議の一つである EUROCRYPT において提案され HL 耐性を持つ ID ベース暗号方式として唯一知られていた方式について、その安全性証明が誤りであることを指摘している。

第4章は「Digital Signatures with Hard-to-Invert Leakage-Resilience（逆変換困難漏洩耐性を持つ電子署名）」と題し、多項式的逆変換困難漏洩の生起する状況におい

て、実用的に必須とされる強偽造困難性と呼ばれる安全性を達成する電子署名の一般的構成法を提案し、標準的な計算量的仮定の下で安全性を証明している。この一般的構成法に基づいて得られる具体的方式は、標準的な仮定の下で多項式的逆変換困難漏洩耐性を達成する世界初の方式であるだけでなく、HL 耐性の考慮された強偽造困難性の安全性モデルにおいて安全性が証明された最初の方式であり、その価値は大きい。

第 5 章は「ABS/IBS Schemes with Hart-to-Invert Leakage-Resilience（逆変換困難漏洩耐性を持つ属性ベース署名及び ID ベース署名方式）」と題し、HL 耐性を持つ属性ベース署名と ID ベース署名の構成法を提案している。ID ベース署名は、任意の文字列を署名検証鍵として使用可能な電子署名である。属性ベース署名は、ID ベース署名の一般化であり、署名者の匿名性が特徴である。本章の成果により得られる具体的方式は、標準的な仮定の下で HL 耐性を持つ世界初の方式であるだけでなく、広義に捉えれば標準的な仮定の下で漏洩耐性を持つ初めての方式であり、本成果の意義は大きい。

最後に第 6 章は「Conclusion（結論）」で、本研究の総括を行い、併せて将来展望について述べている。

以上これを要するに、本論文は、実用的観点及び理論的観点から特に重要とされる種々の公開鍵系暗号技術について、計算量的逆変換困難漏洩耐性を持つ世界で最初の一般的構成法や具体的方式を、厳密な証明可能安全性の枠組みで示した論文であり、電子情報学、特に情報セキュリティ工学上貢献するところが少なくない。

よって本論文は博士（情報理工学）の学位請求論文として合格と認められる。