JAIST Repository
https://dspace.jaist.ac.jp/

Title	現実的な電子署名の設計と解析
Author(s)	岡本，健
Citation	
Issue Date	2002-03
Type	Thesis or Dissertation
Text version	author
URL	http://hdl.handle.net/10119/916
Rights	
Description	Supervisor:宮地 充子，情報科学研究科，博士

JAIST
JAPAN
ADVANCED INSTITUTE OF
SCIENCE AND TECHNOLOGY

Japan Advanced Institute of Science and Technology

学位論文の概要

電子署名とは，署名者固有の情報を用いて電子的なデータを変換することにより作成されたデータであり，ユーザ認証，メッセージ認証，否認防止という機能を実現できる．近年，インターネットを利用した情報通信の急速な普及に伴い，電子商取引や企業間通信の実現等，社会において重要な役割を果たすようになってきた．その一方で，このような通信は実際の当事者と会わずに情報のやりとりが成されるため，通信者の「なりすまし」や情報の「改ざん」というような情報セキュリティの問題が存在する．このような課題に対応するため，電子署名は情報の正当性を確保するための必要不可欠な技術として位置付けられている．

電子署名の研究を理論的な側面から考えた場合，数論上に基づく新しい問題を定義し，それらの問題の帰着関係を調べるという研究が挙げられる．現在のところ署名方式の安全性は，解くことが計算量的に難しいとされる問題に依存している．このため問題の帰着関係を明らかにすることは，署名方式に関して厳密な安全性を与えるという点で価値を与える．

次に現実的な側面から考えた場合，電子署名の高速化に関する研究は最も重要な研究課題の一つである．これは，現在の電子署名方式がいずれも署名の作成や検証の際に指数演算を必要とするため，共通鍵暗号系のデータ認証と比較した場合，公開鍵暗号系の署名は計算処理速度が遅いという短所があるためである．計算処理速度の向上のためには効率的なアルゴリズムを発見したり，演算の種類を削減する等の取り組みが不可欠である．さらに，現実的な社会の要求に対応するため，従来の署名方式には有していない特徴を持つ署名技術の開発も不可欠である．

本研究では，従来の署名方式を改良することによって，高い実用性を有するとともに，数学的に定義された署名の安全性に対して，証明が可能な電子署名システムの構築を目的としている．具体的には，以下に示す 3 種類の課題について研究を行なった．

数論に基づく新しい問題の提案とその応用 実社会では素因数分解問題に基づく署名方式が主流を占めている．また素因数分解系の問題に関して，これまでに多くの新しい問題が提案されており，それらの問題に基づく有益な署名方式が構築されている．本研究では，これらの研究成果をさらに推し進めるため，RSA 問題，位数探索問題という 2 つの素因数分解系の問題に着目し，RSA 問題に変更を加えた 2 つの問題および位数探索問題に変更を加えた問題を新しく定義した．また，これらの問題がどの程度難しいかを，関数間の帰着関係という手法を用いて考察した．さらに，既存方式を改良することにより変形型 RSA 問題に基づく効率的な署名方式を提案した．既存方式の場合，安全性を証明するためには，利用するハッシュ関数に関してある種の強い仮定が必要であった．一方，提案方式にはこれらの仮定を必要とせず，実装環境下において，より厳密な安全性の考察が可能になった．

電子署名の高速化に関する研究 電子署名の作成に必要な計算は，メッセージが与えられる以前から計算可能な「off-line 計算」と，メッセージが与えられてはじめて計算が可能となる「on-line 計算」の 2 種類に分類できる．ここで，on-line 計算は off-line 計算と異なり，リアルタイムの処理時間に影響を与えるため，on-line 計算の効率化は電子署名の高速化を実現する．本研究はこの点に注目して，高速な 2 種類の署名方式を提案した．2 つの方式のうち，一方は on-line 計算において剰余を，他方は乗算を削除することによって高速化を実現している．また，前者は既存方式が有していた秘密鍵の構造に関する問題点を改善することによって得られた方式であるのに対し，後者は既存方式となる方式は存在せず，on-line 計算において乗算を削除した高速化手法の提案は今回が初めてとなる．さらに，変形型位数探索問題に関する研究成果を用いることによって，off-line 計算が高速化された方式に関する厳密な安全性の考察を実現した．

メッセージ復元に基づく新しい委任署名方式 委任署名とは，署名者が署名の権限を第 3 者に委任し，委任された機関が署名を行う方式である．従来の委任署名に関する研究では，代理署名者による署名権限の逸脱を防ぐため，署名依頼者が署名作成の期限や，署名できるメッセージの種類等が記載された保証書を発行し，検証時に，検証者がこの保証書の正当性を確認する方式が提案されている．しかしながら，この方式の場合，検証者は検証時に代理署名者から保証書を送ってもらう必要があり，このことは伝送量の増大を伴うという短所が存在した．本研究では，この問題を克服するため，従来の委任署名を拡張した新しい概念を提案した．この概念の特徴は署名検証時において，検証者は署名依頼者が意図したメッセージが復元さ

れた場合に限り署名文を受理するというものであり，これにより検証者は署名検証時に必要な通信情報量を軽減することができる．また，上記の概念を満たす 2 種類の委任署名方式を提案した．2 つの方式のうち，一方は RSA 問題に，他方は離散対数問題に基づく方式である．