博士（工学）　森　田　　光

学位論文題名

A Study on Test Method, Arithmetic Algorithms, and Hardware Implementation of Cryptography

（暗号記述におけるテスト法，高速計算法，ならびにハードウェア化に関する研究）

学位論文内容の要旨

正当な通信者間の安全な情報伝達を可能とし，不正な第三者への情報もれを排除する手段として発展してきた暗号は，近年の公開鍵暗号の概念の創出に伴い，理論および実用化の両面から精力的に研究が進められている。公開鍵暗号は，従来の秘密鍵暗号と異なり，通信相手への秘密鍵配送を不要とするばかりでなく，相手確認機能およびデータ確認（署名）機能が新たに加わったため，電子契約・電子決済など，多方面での利用が期待されている。一方，最近の通信と計算機技術の進歩に伴い，あらゆる機能を電子化された通信手段と計算機で高速かつ安全に処理するシステムの重要性が高まっており，IC カードのような小型化システムへの適用など，暗号の実用面における技術確立が強く望まれている。

ところで，公開鍵暗号の安全性は，離散対策問題，または素因数分解問題の困難性と密接な関係がある。安全性の向上のためには，データサイズが500ビットから1,000ビット程度の多倍長演算が必須となり，一般的な単精度演算の単純な組み合わせだけでは高速処理を達成できない。このため，秘密通信では，各データを乱数化する秘匿処理に従来と同じ秘密鍵暗号を利用し，通信相手との鍵共有には公開鍵暗号，または公開鍵配送を使う併用方式が実用的であるとされてきた。しかしながら，公開鍵暗号を鍵共有機能に限定したとしても，安価な汎用マイクロプロセッサで処理するには不十分な処理速度であり，ハードウェアによる高速化が必要であった。また，秘密鍵暗号の100Mb／s～1 Gb／s 程度の高速処理を実現するにも専用ハードウェアが必要とされた。

本論文は，こうした状況の中で，公開鍵暗号ならびに秘密鍵暗号のハードウェア化を実現するための計算法と設計方法，公開鍵暗号技術を利用した署名方式を IC カード上のプログラムにより実用的な時間内で処理する計算法，さらに秘密鍵暗号の代数的な構造の有無を確かめることにより暗号の安全性を検証するテスト法に関する研究成果をまとめたものである。具体的には，秘

密鍵暗号の安全性検証のためのスイッチ型閉構造テスト法，公開鍵暗号用ハードウェア化のための高速剰余乗算法，公開鍵暗号用プログラム処理のための高速剰余乗算法，秘密鍵暗号用ハードウェア設計方法を新たに提案し，それらの高速性，有効性，適用性を明らかにしている。以下に本論文の概要を示す。

第1章では，本論文の背景，目的，および構成について述べる。

第2章では，本論文が前提とした用語と技術を紹介する。

第3章では，閉構造を検出するためのスイッチ型テスト法について述べる。秘密鍵暗号の安全性の根拠は，公開鍵暗号に比べ定量的には表現し難い。しかしながら，各種暗号攻撃法に対する暗号の強度を測定することは可能である。閉構造は暗号解読を容易にする代数的構造の代表的なものの一つであり，暗号に閉構造があれば暗号化関数で定義される関数は群をなす。この結果，暗号解読に必要な探索量が鍵空間Kのサイズ|K|からその平方根$\sqrt{|K|}$まで縮退し，暗号解読が容易になる。

本章では，従来のCCT（Cycling Closure Test）法がDES（Data Encryption Standard）暗号のみに適用可能であったのに対し，全ての暗号に適用可能なSCT（Switching Closure Test）法を提案する。SCT法はCCT法が前提としていた条件（暗号化関数における乱数性の仮定など）を不要とするばかりでなく，高速かつ小メモリ量で実現できる。SCT法は暗号の関数を組み合わせたスイッチ型関数を周期性検出手法に拡張して実現する。従来に比べ，所要メモリ量を3桁以上削減することを可能とするとともに，膨大なメモリアクセス時間を削減する。さらに，確率に基づく安全性評価尺度を与える。

第4章では，産業上重要となっている512ビット規模のRSA暗号(Rivest−Shamir−Adleman scheme）またはDH法（Diffie−Hellman scheme）を対象に，LSI一個程度でディジタル通信の基本通信単位である64Kb／sを越えるべき乗剰余演算法について述べる。特に，べき乗剰余を構成する剰余乗算の高速化法を提案する。関連する研究は既に多くなされているが，大規模ハードウェア，あるいは大容量メモリを前提とするものが多く，実用的に満足できるものは従来なかった。本章の提案手法では，高基数の採用と，除算に必要な試行演算を不要とする近似算法の提案により高速化を達成する。具体的には1.5μmゲート長CMOSにより80Kb／sのRSA暗号用LSIが作製可能となった。

第5章では，ソフトウェアによる剰余演算の高速化法について述べる。FS法（Fiat−Shamir scheme），ESIGN法（Efficient digital SIGNature scheme）などの高速署名方式は，発表当初から，ICカードなどの小規模システム上のプログラムによる実現が期待されてきたが，目標とする数秒程度の署名は困難であった。本章では，乗余乗算法の高速化手法を提案し，8ビッ

,トマイクロプロセッサが搭載されている市販 IC カード上に適用した結果，FS 法が 3 秒以下，ESIGN 法が0.5秒以下で処理され，実用レベルとして利用できることを初めて示す。従来に比べ 1 桁程度高速であり，小容量の内蔵メモリでも実現できる。この理由は，計算機の処理単位に適した先行制御法と乗余乗算における除算を効率化する近似算法による。また，拡張ユークリッド互除法による剰余除算にも，剰余乗算に使用した近似算法と同様の手法を適用して高速化する。

第 6 章では，小規模・低速応用において有効な秘密鍵暗号を高速領域に適用するための暗号 LSI の構成法について論ずる。本章では，特に既存マイクロプロセッサをベースに小規模・低速応用において多用されている FEAL（East data Encipherment Algorithm）暗号を高速化するため，基本デバイスである暗号 LSI（FEAL-LST）の構成法について論ずる。

第 7 章では，複数の暗号 LSI を組み合わせることで高速性と高信頼性を同時に満たす，1 Gb／s の処理速度まで適用可能な装置構成法を提案する。また，将来の大容量通信時代への対応と基幹回線の暗号化ニーズに対応できる基本技術として，並列処理における高速性と高信頼性を目的に研究された結果を述べる。

第 8 章では，結論を述べる。

学位論文審査の要旨

主　査　　教　授　　小　柴　正　則
副　査　　教　授　　伊　藤　精　彦
副　査　　教　授　　小　川　吉　彦
副　査　　教　授　　永　井　信　夫

正当な通信者間の安全な情報伝達を可能とし，不正な第三者への情報もれを排除する手段として発展してきた暗号は，近年の公開鍵暗号の概念の創出に伴い，理論および実用化の両面から精力的に研究が進められている。最近の通信と計算機技術の進歩に伴い，あらゆる機能を電子化された通信手段と計算機で高速かつ安全に処理するシステムの重要性が高まっており，暗号に対する要求は処理の高速化にとどまらず，適用性の拡大，さらには多用なニーズに対応することが必要になってきている。

本論文は，こうした状況の下で，公開鍵暗号ならびに秘密鍵暗号のハードウェア化を実現する

ための計算法とその設計方法，公開鍵暗号技術を利用した署名方法をICカード上のプログラムにより実用的な時間内で処理する計算法，さらに秘密鍵暗号の代数的な構造の有無を確かめることにより暗号の安全性を検証するテスト法に関する研究成果をまとめたものである。

まず，閉構造を検出するためのスイッチ型テスト法について述べ，従来テスト法，いわゆるCCT（Cycling Closure Test）法がDES（Data Encryption Standard）暗号のみに適用可能であったのに対し，全ての暗号に適用可能なテスト法として，SCT（Switching Closure Test）法を新たに提案している。SCT法はCCT法が前提としていた暗号化関数における乱数性の仮定などの条件を不要とするばかりでなく，高速かつ小メモリ量で実現でき，具体的には，暗号の関数を組み合わせたスイッチ型関数を周期性検出手法に拡張して実現している。さらに，確率に基づく安全性評価尺度を与えている。

次に，産業上重要となっているRSA暗号（Rivest-Shamir-Adleman scheme）およびDH法（Diffie-Hellman scheme）の512ビット規模のべき乗剰余のハードウェア化に利用でき，LSI一個程度でディジタル通信の基本通信単位である64Kb／s　以上の処理速度を達成する方法について述べている。特に，べき乗剰余を構成する剰余乗算の高速化に新規性があり，高基数の採用と，除算に必要な試行演算を不要とする近似算法の提案により高速化を達成している。

さらに，ソフトウェアによる剰余演算の高速化法について述べている。FS法（Fiat-Shamir scheme），ESIGN法（Efficient digital SIGNature scheme）などの高速署名方法は，発表当初から，ICカードなどの小規模システム上のプログラムによる実現が期待されてきたが，目標とする数秒程度の署名は困難であったのに対して，ここでは，剰余乗算の高速化手法を提案し，実用レベルで利用できることを示している。

また，小規模・低速応用において有効な秘密鍵暗号を高速領域に適用するための暗号LSIの構成法についても論じ，具体的に，基本デバイスであるFEAL（Fast data Encipherment ALgorithm）－LSIの実現に成功している。

最後に，複数の暗号LSIを組み合わせることで，高速性と高信頼性を同時に満たす1Gb／sの処理速度まで適用可能な装置構成法を示している。

以上のように本論文は，公開鍵暗号を高速化する計算手法，秘密鍵暗号の高速設計法，暗号の安全性検証方法を開発し，暗号の実用的な課題の多くを解決しており，通信工学，情報工学の進歩に寄与するところが大きい。よって，著者は，博士（工学）の学位を授与される資格あるものと認める。