【 7 】

氏名・（本籍）	清水明宏（しみずあきひろ）
学位の種類	工学博士
学位記番号	第 9792 号
学位授与の日付	平成3年5月2日
学位授与の要件	学位規則第5条第2項該当
学位論文名	**高速共通鍵暗号方式に関する研究**
論文審査委員	(主査) 教授 手塚 慶一 (副査) 教授 倉薗 貞夫 教授 北橋 忠宏 教授 森永 規彦

論文内容の要旨

本論文は，コンピュータ通信システムにおける情報セキュリティ対策の中核をなす共通鍵暗号方式について論じたものである。代表的な共通鍵暗号方式であり広く普及しているＤＥＳ暗号方式は，ハードウェアでの実現を想定して設計されており，ソフトウェアでは高速に処理できないという問題がある。

本論文は，ＤＥＳと同等以上の暗号強度を有し，かつ，DESの適用が困難な領域に使用できる共通鍵暗号方式およびそのパスワード認証方法への応用に関する研究をまとめており，緒論，結論を含め6章で構成している。各章の概要は以下の通りである。

第1章では，研究の背景および目的と，本論文の概要を述べている。

第2章では，8・16ビットマイクロプロセッサ上のソフトウェアで高速に処理できる共通鍵暗号方式について論じている。本章の方式が，たとえば16ビットマイクロプロセッサ上のソフトウェアでも，数百バイト程度のプログラム規模で200Kbps をこえる暗号化処理速度を達成できるため，8・16ビットパーソナルコンピュータの蓄積・通信データの暗号化をはじめ，ＩＣカードやファクシミリへの適用が有効であることを示している。

第3章では，32ビットマイクロプロセッサ上のソフトウェアで高速処理が可能な共通鍵暗号方式について論じている。この方式が，32ビットのワークステーション上にＣ言語で実現した場合でも，1 Mbps／MIPS 程度の高速な暗号化処理速度を達成できるため，ＬＡＮ環境におけるマルチメディア蓄積・通信データの暗号化に有効であることを示している。

第4章では，第3章で述べた方式の，高速ハードウェア処理への拡張について論じている。本章の方式のLSI が，汎用のLSI 技術で数百Mbps の暗号化処理速度の性能を実現できるため，B-ISDN や高

速LAN などにおける高速通信データ，あるいは，高精細動画データなどの暗号化・復号処理に有効であることを示している。

第5章では，これまで述べた高速共通鍵暗号方式の応用として，パスワード認証への適用方式について論じている。この章の方式は，従来の方式に比較して数百倍から数千倍の高速処理を実現できるため，一般的なパスワード認証として有用であることはもちろん，セキュリティプロトコルなど，コンピュータ通信システムの様々な資格認証へも応用できることを示している。

第6章は結論であり，上記研究全体についての成果を要約するとともに今後の課題を示している。

論文審査の結果の要旨

情報システムにおけるセキュリティ対策は，高度情報化社会に関わる重要な問題であり，各分野において，活発な研究が行われている。本論文は，このセキュリティ対策の中核の1つと見られている共通鍵暗号方式の高速化に関して，理論と応用の両面からの研究成果をまとめたものであり，主な成果を要約すると次の通りである。

(1) 8, 16, ならびに32ビットマイクロプロセッサ上のソフトウェアで，高速に処理可能なデータ乱数化関数に基づく共通鍵暗号方式を提案し，暗号攻撃に対する安全性，及び暗号化処理速度性能が，従来方式に比べて格段に優れていることを実験的に確かめている。

(2) 本論文で提案されている方式をCMOS ゲートアレイによりハードウェア化し，暗号化速度が数百Mbps に到達しうることを実証するとともに，LSI 化によりLAN 環境やマルチメディア通信環境に適用しうることを示している。

(3) 高速共通鍵暗号方式の応用として，情報通信システムのセキュリティ対策のための動的パスワード認証方式を考案し，安全性並びに処理の高速性が従来方式より向上することを検証している。

以上のように本論文は，種々の計算機環境，通信環境に広範に対応でき，またセキュリティ保護技法にも有用であるシステムの実現に，多くの示唆を与えており，通信工学の発展に寄与するところが大きい。よって本論文は，博士論文として価値あるものと認める。