ブロック暗号アルゴリズム“MISTY”

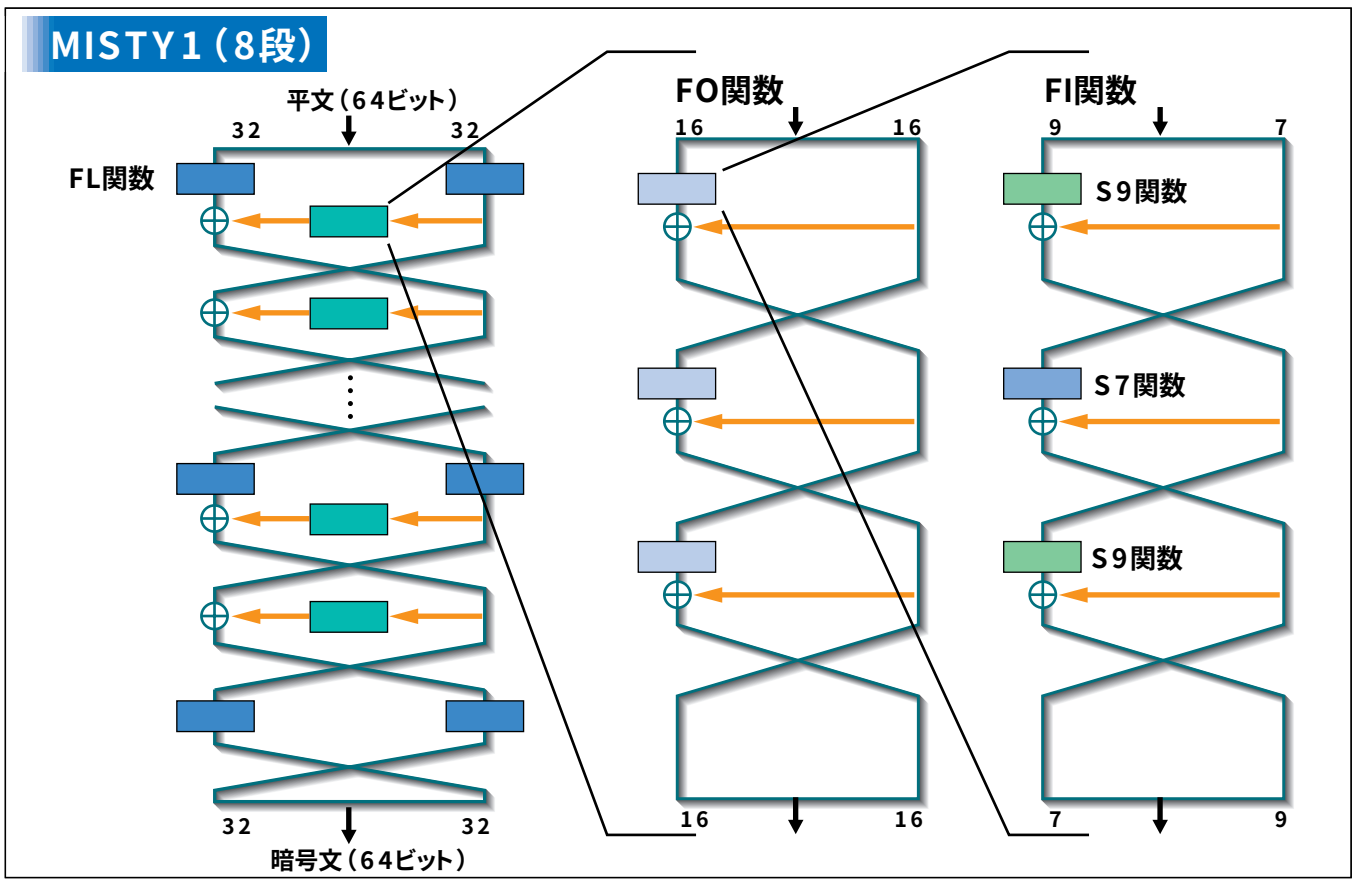
松井　充*
時田俊雄*
反町　亨*

要　旨

“MISTY”は三菱電機が開発した世界最高水準の安全性と実用性を兼ね備えた暗号アルゴリズムであり，その詳細仕様を公開することにより，オープンネットワークにおけるデータ通信やエレクトロニックコマースなどの分野で業界標準となることを目指している。アルゴリズムとしてはMISTY1とMISTY2の二つがあり，共に128ビットの暗号化かぎ(鍵)を持つ64ビットブロック暗号であり，MISTYはこれら二つのアルゴリズムの総称である。またMISTY1は，ISO(国際標準化機構)9979に13番目の暗号アルゴリズムとして登録済みである。

MISTYの特長は安全性と実用性が両立している点にある。安全性としては，ブロック暗号の各種の暗号解読法に対して十分な強度を持っている。特に差分解読法と線形解読法という二大解読法に対しては，その安全性が数学的に証明されている(これを“証明可能安全性”を持つという。)。次に実用性としては，暗号化処理の基本部であるデータランダム化部において，下のイメージ図のような構成とその構造を再帰的に採ることにより，暗号化関数の並列処理が可能となり(高速性)，また，最終的な暗号化関数(S7，S9)のサイズを小さくすることで，ソフトウェア及びハードウェアのテーブル(ロジック)サイズを小さくすること（小型化)が可能となる。例えば，0.8μmCMOSゲートアレーで512Mbpsの暗号化処理が可能であり，Pentium(注)100MHzで20Mbpsの処理速度を達成している。

(注)“Pentium”は，米国Intel Corp. の商標である。



MISTY1の暗号化処理部の基本構造

この図はMISTY1の暗号化処理部の全体構造（左図）とその主要部分であるFO関数の構造（中図），さらにFO関数に用いられるFI関数の構造（右図）を示している。

このようにMISTY1は，主要部分であるFO関数８段で構成され，さらにFO関数２段ごとにFL関数処理が行われ，64ビットの平文データを64ビットの暗号文データに暗号化する。

　*情報技術総合研究所