三菱電機の暗号アルゴリズム開発 —MISTY，KASUMI，Camellia—

松井　充*
時田俊雄*
反町　亨*

要　旨

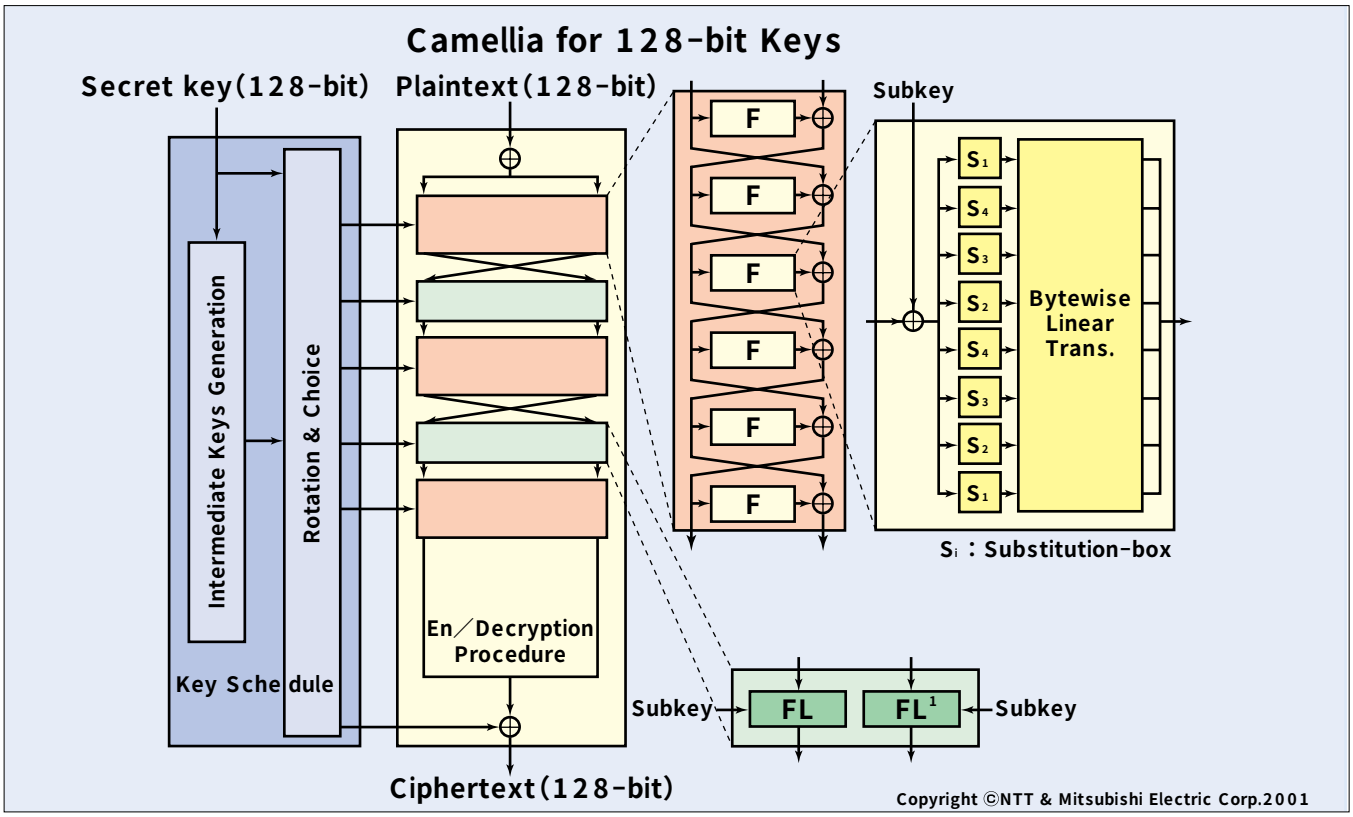
三菱電機の暗号評価技術を基に設計された三つの共通かぎ(鍵)ブロック暗号アルゴリズム“MISTY”“KASUMI”“Camellia”を紹介する。暗号アルゴリズムの設計においては，その安全性はもちろんのこと，速度性能や実装時のサイズ，又は応用の広さなど実用面からの検討が不可欠である。すなわち，安全性と実装性のバランスをどうとるかが，暗号を設計する上において最も困難な部分であると言ってよい。

MISTYは，当社が1996年に発表した64ビットブロック暗号である。MISTYは，ソフトウェアでの高速性だけでなく，ハードウェアでの小型化をも設計目標とした点で，当時としては珍しい方式であった。

その後2000年になって，第三世代携帯電話(W-CDMA)世界標準暗号にMISTYをベースとして欧州で開発された64ビットブロック暗号KASUMIが採用されたが，MISTYがそのベースとなるに至った大きな理由の一つは，MISTYがハードウェアで優れた性能と低消費電力を実現することにあった。

Camelliaは，2000年にNTT㈱と当社が共同で設計した次世代128ビットブロック暗号であり，両社の持つ世界トップレベルの暗号強度評価技術と暗号実装技術を結集して実現されたものである。Camelliaは，次世代暗号にふさわしい高い安全性と，あらゆるプラットフォームで高い性能と小型化が両立できるよう設計されている。

これらの暗号方式はいずれも国内外の研究者から高い評価を得ており，我々は積極的な標準化活動を行っている。今後，これらマルチプラットフォーム共通鍵暗号のニーズはますます拡大していくものと考えられる。



ブロック暗号アルゴリズムCamellia

Camelliaは，米国政府標準暗号AESと同じく３種類の鍵サイズ(128ビット，192ビット，256ビット)をサポートする。図は，このうち128ビットの鍵サイズを持つCamelliaの全体図を示したものである。フェイステル型と呼ばれる構造と，鍵によって形が変化する線形関数を組み合わせることによって，高い安全性と小型化を両立させている。

*情報技術総合研究所