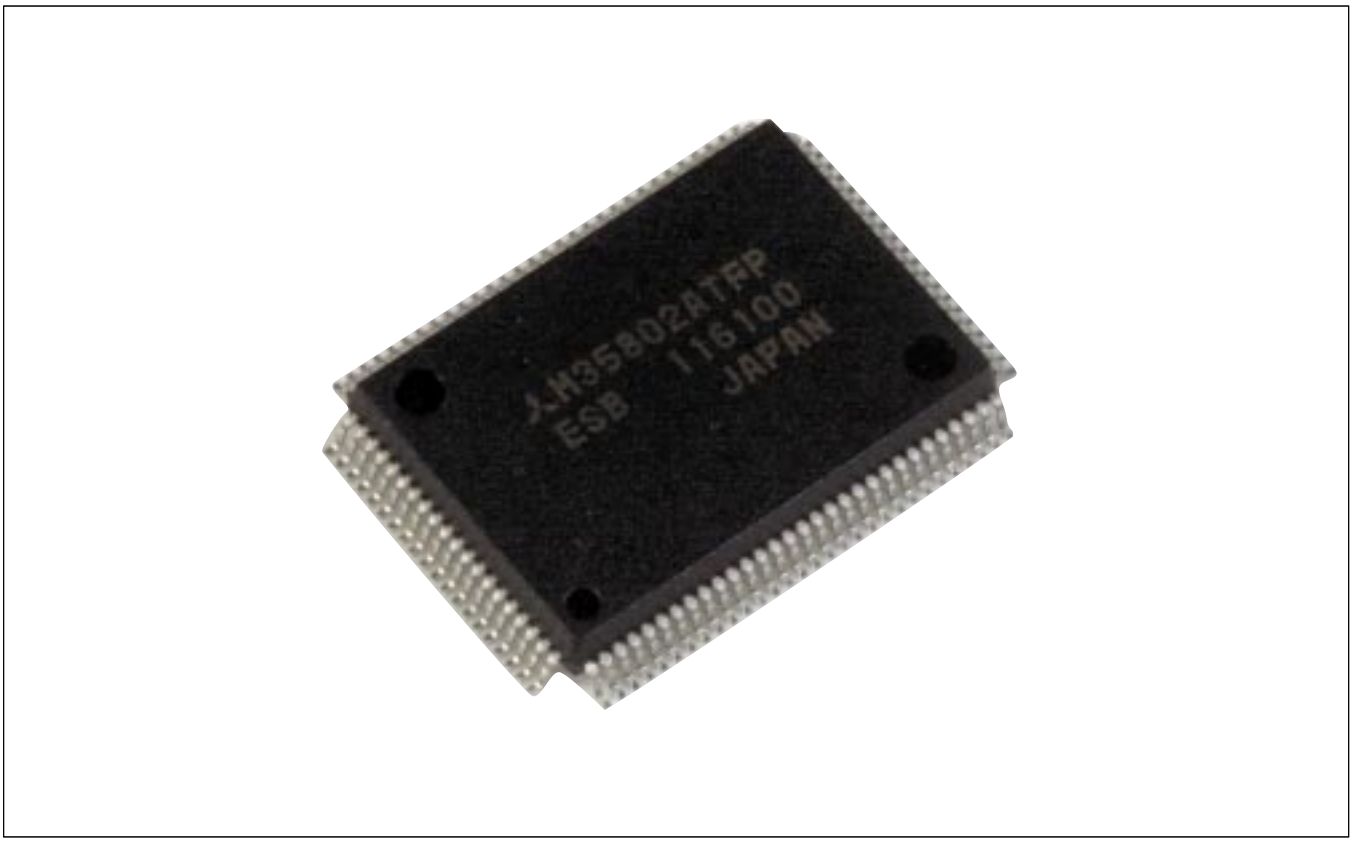
暗号アルゴリズムの実装

中嶋純子*　山岸篤弘*
市川哲也**
粕谷智巳*

要　旨

インターネットの普及に伴い，ネットワークにおける安全性の確保に注目が集まっている。安全性を確保するための中核技術である暗号アルゴリズムに関する研究開発は，米国のAES，我が国のCRYPTRECや欧州のNESSIEといったプロジェクトの影響もあり，新しい暗号技術（アルゴリズム）の提案が盛んに行われている。これらのプロジェクトで特徴的なことは，暗号の安全性（強度）を評価するだけでなく，実用化を視野に入れた評価も行われている点にある。つまり，暗号技術（アルゴリズム）を実際に使用する場合には，実装設計という過程を経てソフトウェア，ファームウェア（マイクロコンピュータ（以下“ マイコン ”という。）上での実装）やハードウェアという形態をとる必要があるため，高速実装法や小型化という実装面での研究開発も重要になりつつある。この実装技術の研究開発に当たっては，実装規模と処理性能のバランスをとることが重要となる。

本稿では，ソフトウェア，ハードウェアそれぞれの実装技術について述べる。特にハードウェアで実現する場合には，他の機能と組み合わせた暗号モジュール（暗号機能付きのASIC）として実現されることが多い。このような暗号モジュールを設計するための暗号機能の再利用可能な設計資産（Intellectual Property）についても触れる。



暗号アルゴリズムを実装した１チップLSIの例

RSA暗号やMISTY等の暗号技術をマイコンチップと組み合わせて実装した暗号LSIの実装例である。このLSIチップには，暗号アルゴリズムがハードウェア，ソフトウェア又はハードウェアとソフトウェアを組み合わせて実装されている。実装に当たっては，この暗号LSIが適用されるシステムの要求に合わせて，コストと性能の最適化を図った。

*三菱電機㈱情報技術総合研究所　**三菱電機エンジニアリング㈱