共通鍵暗号‘ MISTY ’評価用LSI

加藤潤二*　松井　充**
反町　亨**
市川哲也***

要　旨

近年，インターネットの普及，エレクトロニックコマースの実現に見られるように，オープンネットワークの利用が身近なものになってきている。しかしながら，オープンネットワークを利用して個人情報のやり取りや企業間の取引・決済などの電子商取引を行う場合，情報の盗聴，改ざん，成り済まし等が行われる可能性が高く，情報をいかに他者に漏らすことなく安全に送受信するかが最大の課題であり，安全な情報通信を実現するために，暗号技術をシステムに組み込むことが重要である。

その暗号技術を実現する方法として，ソフトウェア又はハードウェアで実装する方法がある。ところが，ソフトウェアでは数十Mbps程度のスループットしか実現できず，高速通信への対応のためには暗号アルゴリズムをハードウェアで実現することが必す(須)となってきている。

今回，三菱電機　が独自開発した秘密かぎ(鍵)暗号アルゴリズム“ MISTY ”の高速・高性能を，客先の評価によって実証し，情報通信システムにおいて暗号アルゴリズムMISTY及び当社暗号LSIを採用してもらうことを目的として，MISTY評価用LSI及びその評価システムの開発を行った。その結果，256Mbpsという世界最高速レベルのLSIを開発したので紹介する。

秘密鍵暗号アルゴリズム評価用LSI
M64409FPの特長

- 三菱電機が開発した高速・高性能な秘密鍵暗号アルゴリズムMISTYを採用
  ブロック長:64ビット　鍵:128ビット
- 208QFP
- ISO規定暗号モード準拠(ECB,CBC,OFB-64,CFB-64)
- 処理速度　256Mbps
- 32ビットI／Oポート装備
- 消費電力　1.5W

M64409FP評価システム

- M64409FPを用い,MISTY高速演算性能の評価を実現
- 5V単一電源のPCI標準長カード
- ソフトウェア(PowerMISTY)とハードウェア(この評価基板)の演算結果の比較及び処理速度の表示が可能
- PCIバスマスタ方式を採用することによるDMA機能

評価用LSI及び評価システムの特長

M64409FPは，三菱電機が開発した高速・高性能秘密鍵暗号アルゴリズム“ MISTY ”をハードウェアで実現した。これを使用して評価システムを構築し，その高速演算性能の評価を実現できる。

*三菱電機　システムLSI事業化推進センター　**同情報技術総合研究所　***三菱電機エンジニアリング(株)