

# 楕円暗号コプロセッサ内蔵FRAM搭載マイコン MB89R905

モバイル端末などのセキュリティをサポートするセキュアプロセッサです。楕円曲線暗号コプロセッサ，4KバイトFRAM等を内蔵し，チップ内部で高速・低消費電流の暗号処理と署名処理が可能です。

## 概要

このたび当社は，株式会社富士通研究所と共同で，楕円曲線暗号<sup>\*1</sup>コプロセッサと大容量FRAM<sup>\*2</sup>を世界で初めてワンチップ化したセキュアプロセッサMB89R905を開発しました。

本製品は，当社8ビットマイクロコントローラとともに，楕円曲線暗号コプロセッサと大容量FRAMをワンチップ化したものです。コプロセッサにより，ソフト処理に比べて1000倍以上の高速処理が可能です。またFRAMの採用により，セキュリティチップに不可欠なセキュリティ関連情報の書換えが，従来のEEPROMなどに比べて高速・低消費電力で可能であり，書換え可能回数も飛躍的に多くなります。

近年，インターネットの急激な普及に伴い，電子商取引やバーチャルショップでの新ビジネス，バーチャルオフィス等が注目を集めています。これらの実用化に際しては，情報の暗号化や個人認証など，基礎技術として公開鍵暗号が必須です。

現在，標準的な公開鍵暗号としてはRSA暗号<sup>\*3</sup>が主流ですが，次世代の公開鍵暗号として楕円曲線暗号が注目を浴びています。楕円曲線暗号はRSA暗号と比べて，短い鍵長で同程度の安全性を実現できます。例えば，鍵2048ビットのRSA暗号と同程度の安全性は，鍵211ビットの楕円曲線暗号で実現できます。鍵長が短ければ，処理量も少なくなり高速処理が可能で，かつそれを実現するハード規模も小さくなります。

本製品では，秘密情報をチップから外部に出すことなく暗号/署名処理が可能のため，安全なシステムが容易に実現できます。したがって，今後のモバイル端末やデジタル家電，スマートカードでのセキュアシステムの実現に大きく貢献すると予想されます。

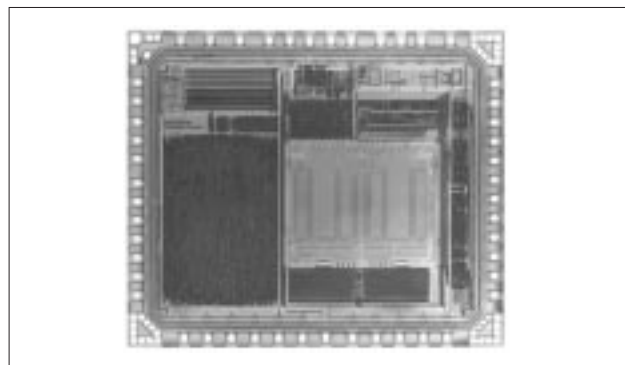


写真1 チップ

## 特 長

本製品は、次の回路で構成されています。

- 8ビットCPUコア
- 4KバイトFRAM... (データメモリ)
- 16Kバイト マスクROM... (プログラムメモリ)
- 1Kバイト SRAM... (ワークメモリ)
- 楕円曲線暗号コプロセッサ
  - ・ 2の拡大体上の楕円曲線演算の基本演算を高速に行います。
  - ・ 最大239ビット以下の任意のビット長、任意の既約多項式に対応できます。

なお、本コプロセッサを用いれば、ファームウェア (ライブラリ) にて暗号化 / 復号処理 (ECAES)、署名作成 / 確認処理 (ECDSA)、鍵交換処理 (ECDH) 等の楕円曲線暗号を構成できます。

表 1 に主な仕様を示します。

本製品には次の特長があります。

- 最大鍵長239ビットまで、任意のビット長の楕円曲線暗号に対応可能
- 楕円曲線暗号での署名処理・暗号化処理・鍵交換に必要な、標準的な暗号関数をフルサポート
- 任意の楕円曲線パラメータに対応可能
- 高速・大容量・低消費電力の不揮発性メモリであるFRAM (最大4Kバイト) を内蔵

- \* 1 : 楕円曲線暗号 (ECC : Elliptic Curve Cryptosystem) : Koblitz, Millerらが発明した公開鍵暗号方式。
- \* 2 : FRAM (Ferroelectric Random Access Memory) : 強誘電体材料を利用した不揮発性メモリ。FRAMはラムトロン社の登録商標です。
- \* 3 : RSA暗号 : Rivest, Shamir, Adlemanらが発明した公開鍵暗号方式。

表 1 主な仕様

項 目		仕 様	
CPU機能		基本命令数:136命令 命令ビット長:8ビット 命令長:1~3バイト データビット長:1, 8, 16ビット長 最小命令実行時間:0.28μs(3.58MHz時) 割込み処理時間:2.5μs(3.58MHz時)	
周 辺 機 能	ポート	汎用入出力ポート (CMOS) 汎用出力ポート (CMOS) 合計	:30本 : 8本 :38本(最大)
	タイムベースタイム	21ビット 割込み周期 メインクロック 3.58MHz時 (0.57ms, 2.29ms, 18.3ms, 292.9ms)	
	ウォッチドッグタイム	リセット発生周期 メインクロック 3.58MHz時 (最小585.8ms)	
	UART/SIO	UART/SIOでのデータ転送可能 可変データ長(7, 8ビット), ボーレートジェネレータ内蔵, 転送レート(874bps-223.75Kbps@3.58MHz時), ダブルバッファ内蔵 全二重, NRZ方式転送フォーマット, エラー検出機能, クロック同期(SIO)・クロック非同期(UART)のデータ転送可能	
	8/16ビットタイマカウンタ	8ビットタイマ×2チャンネル/16ビットタイマ×1チャンネルとして使用可能)	
	FRAM	不揮発性メモリ(4Kバイト)	
	SIO	8ビット長 LSBファースト/MSBファースト選択可 転送クロック(外部, 0.8μs, 3.2μs, 12.8μs)	
	楕円曲線暗号コプロセッサ	最大239ビットまでの楕円曲線暗号に対応	
	スタンバイモード	スリープモード・ストップモード	