AES

TMCは数学的手法を駆使した独自のコンピュータアルゴリズム
[**DMNA**]を用いて高品位なソリューションを提供します

1 概要

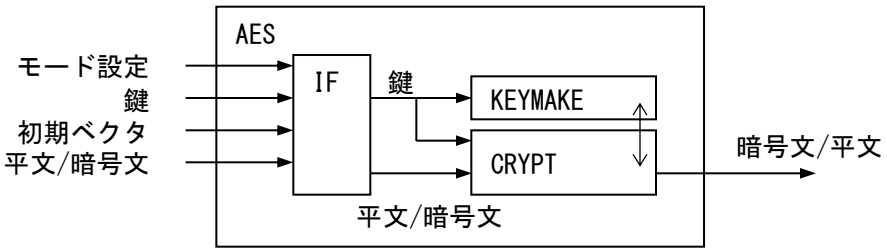
AES暗号/復号 IPコアは、NIST CAVP認証取得済みです。
高速処理が可能ですので、高速LANシステム等の分野に利用可能です。

2 特長

◆超高速動作
・1ラウンドを1クロックで処理
・ 処理能力 1 Gbps（動作周波数100MHz時）
・ FPGAへの搭載も可能

AES DMNA

3 ブロック図



4 仕様

◆各モード対応
NIST FIPS PUB 197 ECB/CBC/OFB/CFB1/CFB8/CFB128モードに対応
NIST AES Algorithm Validation Cert. #3875
・平文： 128bit、 暗号文： 128bit、 鍵長： 128/192/256bit
（CTRモード：オプション対応）
◆１ラウンドを１クロックで処理
・(例) 鍵長128bit、周波数100MHzで動作させた場合、1Gbpsで暗号が可能となります。
※最高動作周波数はプロセス/使用FPGA等により異なります。詳細はお問い合わせ下さい。

製品の仕様は予告なく変更することがあります。詳しくは弊社までお問い合わせください。

問い合わせ先
〒141 - 0031 東京都品川区西五反田2丁目12番19号　五反田NNビル7階
株式会社テクノマセマティカル
電話:03 - 3492 - 3633 FAX:03 - 3492 - 3631
email: info-sales@tmath.co.jp URL: https://www.tmath.co.jp