

AES128-IP コアのご紹介

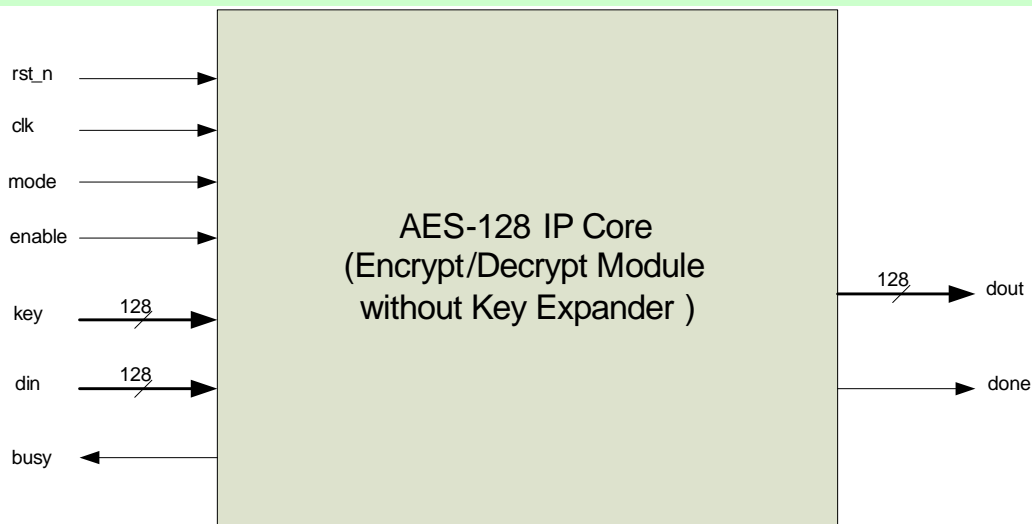
IP コア概略

DesignGateway 社の AES128-IP コアは、FIPS 197 ドキュメントの AES(Advanced Encryption Standard)に準拠し、暗号化および復号化の両方をサポートします。

特長

- 128bit データブロック暗号化/復号化
- EBC モードオペレーション
- 11 サイクルで 暗号化/復号化を実行
- 外部 Key Expander 使用
- シンプルな外部インタフェース
- スマートカード等のアプリケーション用 任意の CBC モード

ブロック図



使用リソース

本 IP を単体で FPGA に実装した場合、以下のリソースを必要とします。

Altera Cyclone II の場合

- ロジックセル数： 780
- メモリビット数： 65,536 (S-BOX の ROM テーブル用 M4K 使用の場合)
- クロック： 100MHz 以上