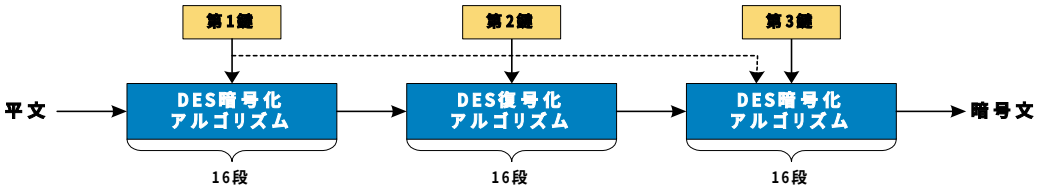
TECHNO CREATE

DES・Triple-DES 暗号/復号エンジン

本 IP は、64bit データを処理単位とした共通鍵暗号 DES の暗号/復号エンジンです。
外部制御回路も含め、お客様のご要望にあわせてカスタマイズ・最適化を行い
ご提供することが可能ですので、全体の回路規模を抑えることができます。

■特長

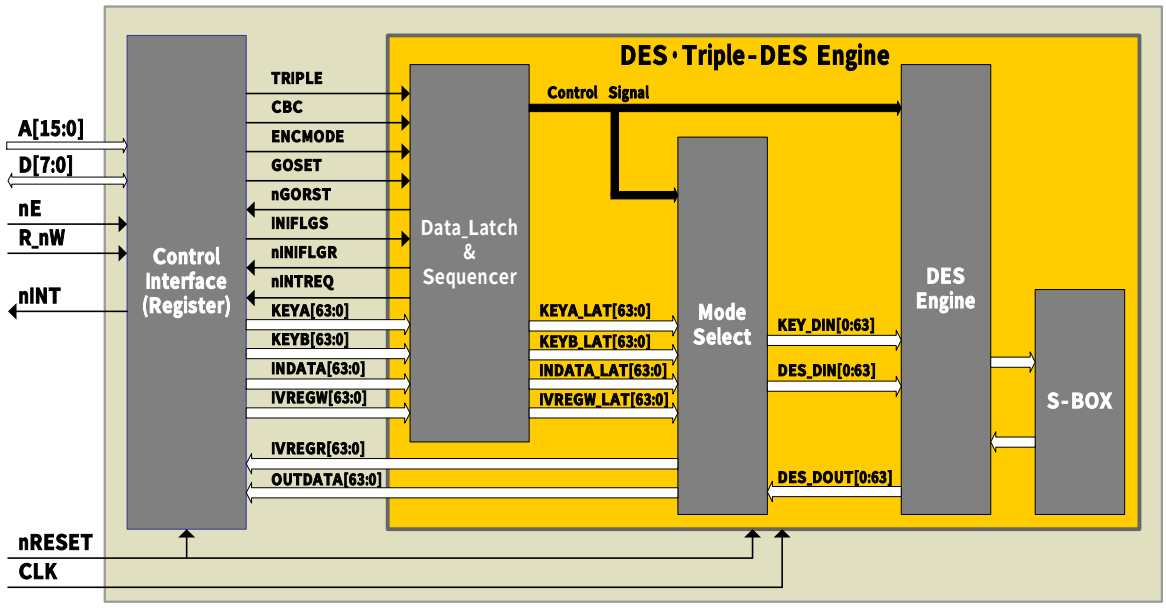
- アルゴリズムは米国規格協会 (ANSI X3.92) 規格に準拠
- DES の利用モードは米国規格協会 (ANSI X3.106) 規格の ECB、CBC モードに準拠
- Triple-DES の利用モードは米国規格協会 (ANSI X9.52) 規格の TECB、TCBC モードに準拠
- Triple-DES は 2key/3key の暗号鍵を選択可能
- DES /Triple･DES による暗号/復号エンジンを1パッケージにて実現



【Triple-DESの暗号化アルゴリズム】

56bit の暗号鍵を利用する DES、および DES の
アルゴリズムを3回繰り返し 112bit (2key) /168bit
(3key) の暗号鍵を利用する Triple-Des。

●ブロック図 (CPU I/F カスタム設計例)



DES･Triple-DES エンジン部

CPU 接続用 I/F をお客様のご要望に合わせてカスタム設計して
ご提供することにより、外部制御が容易になります。

アーキテクチャ面においては、各種データを内部レジスタに設定することにより、DES/Triple-DES、ECB/CBC モード、暗号化/復号の組み合わせにて８通りの動作を可能としております。
また CPU バスと DES エンジン・インタフェースが非同期の場合にも安定動作を実現しております。

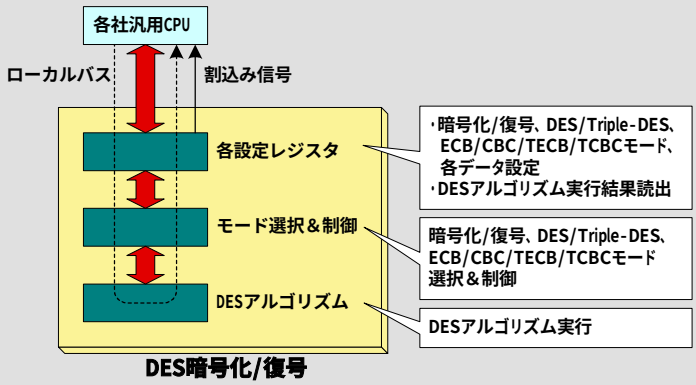
- **シンプルな I/F により簡易手順にて制御可能**
- **処理サイクルは DES：16 クロック、Triple-DES：48 クロック**
- **完全同期設計（エンジン部）**

【規模と速度(参考)】

デバイス	： ALTERA 製 Cyclone（EP1C3）
使用 LE 数	： 約 2,700LEs（CPU I/F 含む、DES エンジン部のみ約 2,200LEs）
必要 Memory 空間	： 0kbit
最大動作速度	： 80MHz

【記述言語】 Verilog-HDL（※VHDL での対応も可能です。詳細はお問合せください。）

【使用構成例】



≪制御手順≫

1) ブロック暗号の利用モードを設定する
2) ブロック暗号の利用モードに応じて、イニシャルベクタ/キーデータ等を設定する
3) 入力データを設定する
4) 暗号化/復号動作開始を指示する
5) 割込み信号等により、暗号化/復号動作終了を確認する
6) 割込みをクリアして、出力データを読み出す

※64bit を越えるデータを暗号化/復号するときは、上記の 3) ～6) を繰り返し、64bit 毎に実行する

外部制御を容易にする CPU 接続用 I/F 制御部を、CPU の種類やお客様のご要望にあわせてカスタム設計してご提供することもできます。

- ご要望により IP のカスタマイズおよび機能追加してのご提供も可能です。
- 外部制御回路等の周辺回路のカスタム設計も承りますので、ご相談ください。
- HDL 言語で設計していますので、様々な FPGA や ASIC デバイスへ対応出来ます。
- マクロ（ネットリスト）によるご提供や ROM 形式でのご提供も可能です。

通信機器･画像処理関連ハードウェア、ファームウェアの受託開発も承ります。

株式会社テクノクリエート
【本社】〒980-0801 仙台市青葉区木町通１－８－２８ 武山興産ビル
【東京技術センター】〒206-0014 東京都多摩市乞田１２８４ 永山Ｕビル

■お問い合わせはこちら
0120－733－606（お問い合わせセンター）
E-mail：info@techno-create.com
http://www.techno-create.com