RSA暗号・高速処理LSI

鍵長1024-bit 対応

LSI 仕様

◎鍵長1024bitのRSA暗号化／復号化処理では現在最高速のLSIです。
◎遠隔医療システムで稼働中です。
◎現在、性能評価用LSIを提供中です。
◎処理速度よりも回路規模縮小を重視したコンパクト版も現在開発中です。
◎ユーザーのシステムLSI向けに、IPコアでの提供も可能です。

■特徴

●RSA公開鍵暗号方式対応暗号化・復号化処理LSI
●信州大学／シーデックス方式の高速アルゴリズムを採用
●CPUバス接続可（アドレスデコーダーが必要）
●パラレル動作対応（2chip搭載で処理速度が2倍）
●1024bitまでの鍵長に対応
●CMOSプロセス（0.18μmASIC）

●電源電圧：<I/O>3.3V±0.3V
　　<コア>1.8V±0.15V
●Clock周波数：75MHz（MAX）
●入出力信号：3.3V　CMOSレベル
●消費電力：0.73W（MAX）（75MHz動作時）
●処理速度：42.1kbit/sec（1024bit鍵）

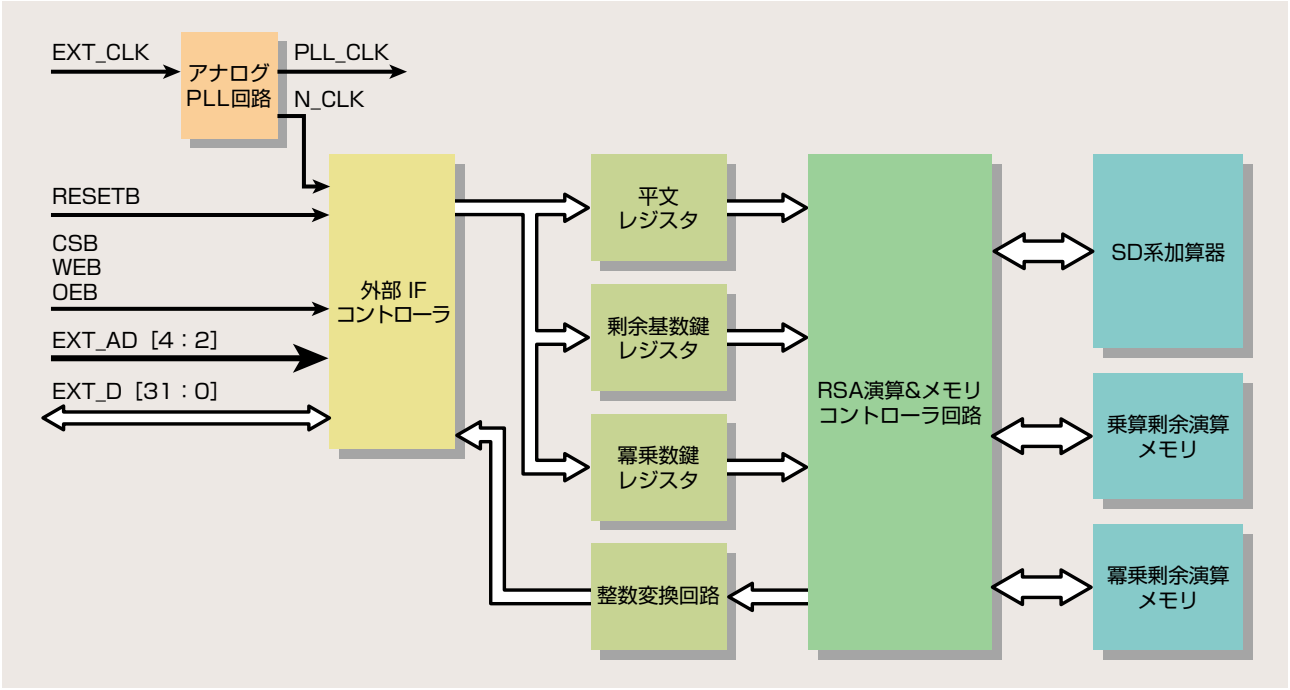
アプリケーション例

◎公開電子認証CAサーバーの認証高速化
◎SSLサーバーの認証高速化
◎ホームサーバーの認証高速化
◎各種端末の認証高速処理化

製品ラインナップ

◎高速版：評価chipは現在提供中
◎コンパクト版：速度よりも価格を重視（現在開発中）
◎2048-bit版も開発中
◎IPコアでの提供も可能

RSA1024A-LSI ブロック図



RPCIボード 仕様

◎RSA1024Aを最大6個同時に並列処理可能な、PCIバス対応のボードです。
◎認証処理がボトルネックになるCAサーバー／SSLサーバーに最適です。

■特徴

●PCIバスインターフェイス
●Linux上で動作（Windowsも対応可）
●暗号化／復号化GUIインターフェイス
●RSA1024Aを複数chip搭載可能（Max.6個）

■電気的特性

●電源電圧：5.0V（PCIバスから供給）
●消費電力：～4W（1chip実装、75MHz動作時）
●処理速度：42.1kbit/sec（RSA1024A 1個実装）

■アプリケーション例

●公開電子認証（CA）サーバーの高速化
●SSLサーバーの高速化 他