ISDN マルチメディア通信用ワンチップ暗号プロセッサ†

小柳津 育郎†† 松本 博幸†† 石井 晋司††

メモリに格納された大量の文書データやファイルデータの暗号ならびに音声，映像を含むマルチメディアデータをリアルタイムで高速に暗号処理できるワンチップ暗号プロセッサを開発した．この暗号プロセッサは，全二重のビットシリアルデータを最大5Mビット/秒の速度で暗号化と復号を実時間で同時に処理することができる．また，メモリに格納された文書データやファイルデータの暗号処理に適用した場合，最大 10M バイト/秒の処理性能が得られる．この論文は，主に，音声等の上位プロトコルを持たないストリームデータの暗号通信に必要な送信側と受信側の暗号同期のプロトコル，全二重通信における送信データの暗号化と受信データの復号を1つの暗号演算器を用いて効率よく行うパイプライン処理方式および音声 CODEC との接続機能等とこれらの実現方法について述べている．また，本プロセッサのディジタル電話機等への適用例についてもあわせて述べている．

1. はじめに

ISDN を利用した新サービスやパーソナル通信サービスの発展には，音声，映像データを含むマルチメディアデータをリアルタイムで高速に暗号化，復号する技術を確立することが極めて重要である．NTT では，1987 年に高速データ処理に適した FEAL (Fast Data Encipherment Algorithm) を開発している[1]．FEAL は DES (Data Encryption Standard) と同様に暗号アルゴリズムが公開の共通鍵暗号方式である．われわれは，FEAL を用いて，メモリに格納された大量の文書データやファイルデータを一括して暗号化，復号処理するだけでなく，音声，映像等を含むマルチメディアデータをリアルタイムで高速に暗号化，復号処理するワンチップ暗号プロセッサを開発した．本暗号プロセッサにはマルチメディア通信用の機能として，音声等，上位プロトコルを持たないストリームデータの暗号通信に必要な送信側と受信側の暗号同期のプロトコル，全二重通信における送信データの暗号化と受信データの復号を1つの暗号演算器を用いて並列処理を行うプロセッサ構成および音声 CODEC との接続機能等を新しく導入している．

本論文は，これらのマルチメディア通信用機能を中心に暗号プロセッサの開発条件とその実現方法を述べる．あわせて本暗号プロセッサの ISDN ディジタル電話機等への適用例について述べる．

† The One-chip Encryption Processor for ISDN Multi-media Communications by IKURO OYAIZU, HIROYUKI MATSUMOTO and SHINJI ISHII (NTT Communications and Information Processing Laboratories).

†† 日本電信電話(株) NTT 情報通信処理研究所

2. 開発条件

2.1 設計コンセプト

本暗号プロセッサの主な適用領域を ISDN 用通信機器とし，ディジタル電話機およびファクシミリ，データ端末等に容易に組み込めるように設計する．すなわち，(a)小型で低価格であること，(b)各種機器との接続のための周辺回路を LSI に内蔵し使いやすさを実現することに，重点をおいて設計する．

2.2 要求機能

2.1 節の設計コンセプトにもとづき，ISDN を利用したマルチメディア通信に適用するワンチップ暗号プロセッサへの要求機能をつぎのように定めた．

(1) 音声等のレイヤ2以上の通信プロトコルを持たないストリームデータの暗号化，復号を実時間で行えること．

(2) 全二重通信における送信データの暗号化と受信データの復号を同時に実行できること．

(3) ISDN 1次群速度インタフェースの H_{11}/H_{12} チャネル (1.5 Mbps/2 Mbps) のビットシリアルデータの暗号化，復号に適用できること．

(4) 音声，音声映像等の PCM CODEC (8ビット単位のフレーム同期信号があるシリアルインタフェース) に直接接続できること．

(5) 産業標準のマイクロプロセッサ・バスに直接接続できること．

(6) パラレルデータを高速に転送する DMA (Direct Memory Access) インタフェース機能を持つこと．

3. プロセッサ機能

3.1 暗号方式

3.1.1 FEAL

FEAL の暗号処理部は，DES の構造[2]を基本にして初期変換と最終変換および暗号関数 f を別の方法で置き換えた構造をしている（図1参照）．暗号処理の最初と最後に DES では転置が行われるが，FEAL では転置の代わりに 64 ビットのデータの右半分と左半分の排他的論理和がとられ，さらに全データと拡張鍵のサブセットとの排他的論理和がとられる．DES の f 関数が排他的論理和と換字表（Sボックス）の組み合わせで構成されているのに対して，FEAL の f 関数はバイト加算とバイトローテーションの2つの基本オペレーションの組み合わせで構成される．FEAL は換字表を用いないで，論理演算だけで暗号処理が行える点が特長であり，高速データ処理に適した暗号アルゴリズムである[1]．FEAL は暗号強度を高めるために，暗号処理の内部段数と鍵の長さをオプションとして拡張できる[3]が，本プロセッサではファクシミリ装置や IC カード等に適用され，利用実績がある FEAL-8 アルゴリズムを搭載する．

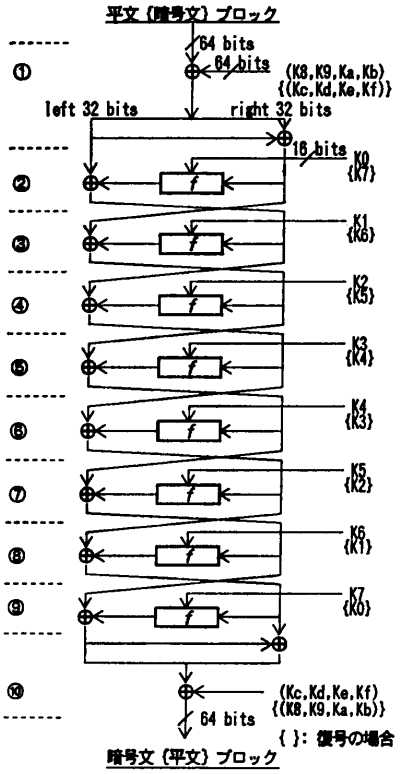


図 1 FEAL-8（暗号処理部）の構造
Fig. 1 The structure of FEAL-8.

3.1.2 暗号利用モード

FEAL-8 のような 64 ビットブロック暗号については，暗号アルゴリズムの利用法が ISO, JIS で標準化されている[4]．暗号アルゴリズムをそのまま利用する ECB (Electronic Codebook) モード，入力ブロックを1つ前の暗号文ブロックと排他的論理和の操作を行ったうえで暗号化する CBC (Cipher Block Chaining) モード，暗号の出力データに再度の暗号化と排他的論理和の操作を行う CFB (Cipher Feedback) モードおよび OFB (Output Feedback) モードが規定されている．また，CFB, OFB モードでは，暗号処理の入力データ幅を1から 64 ビットの任意のビットを選択できるようになっている．CBC, CFB または OFB モードを選択することによって，暗号アルゴリズムの適用範囲を広げることができる．例えば OFB モードは，暗号文が伝送路上でビット誤りを起こしても復号結果による誤り伝搬が入力データ単位外に拡大しないことから，主に音声や映像の伝送に適し

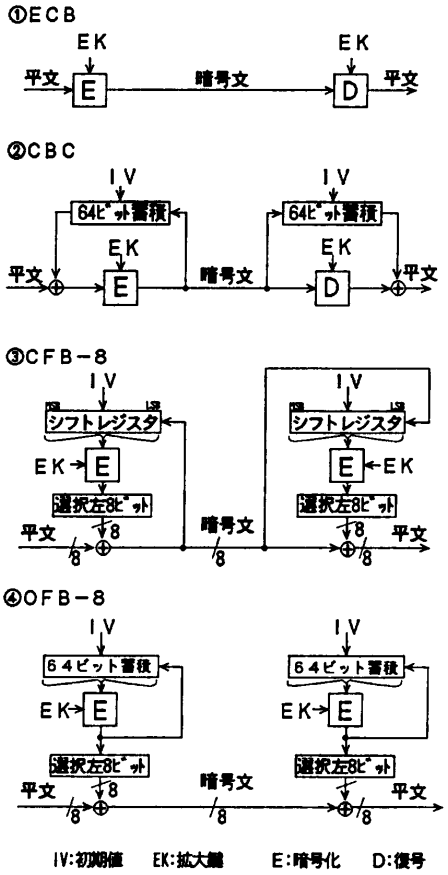


図 2 本プロセッサの暗号利用モード
Fig. 2 Cipher modes installed in the processor.

ている．

本プロセッサは上記すべての暗号利用モードを搭載する．また，CFB，OFB モードの入力単位については，①マルチメディア通信では8ビット（1バイト）単位でデータ伝送が行われること，②ファクシミリやデータ端末等の通信機器に搭載されている各種の LSI チップの処理単位がバイト単位であることから，8ビットにすることとした．すなわち，CFB-8 モード，OFB-8 モードをサポートすることにした（**図2参照**）．

3.1.3 鍵の拡大処理

FEAL-8 では，与えられた 64 ビット長の鍵データを暗号処理部と類似の構造の鍵処理部に入力してかき混ぜ，長さを 256 ビットに拡大した鍵（拡大鍵）を作成し，この拡大鍵を用いて入力データの暗号化と復号を行う[1]．このような鍵の拡大処理をハードウェアで実現する場合，約 4.5 K ゲートの回路が必要であり，暗号プロセッサのゲート数が約 30% 増加する．一方，プログラムで鍵の拡大処理を行うと，16 ビット・マイクロプロセッサのアセンブラ記述のプログラムの場合で，メモリ占有量は 0.2 KB 程度，処理性能は 120 Kbps が実現できることが確認されている[1]．

鍵の拡大処理が必要になるのは，鍵の変更時やセッション鍵を受信した場合であり，その頻度は高くなく，要求される性能もプログラム処理で得られる性能で十分と考えられる．鍵の拡大処理をプログラムで行う場合，一般には安全上拡大処理プログラムを実行するマイクロプロセッサを暗号機構の一部として保護されたエリアに置くように設計しなければならない欠点があるが，逆に，電話機のように ROM しか搭載されない通信機器では外部から侵入の機会は少なく，端末制御と鍵の拡大処理を共通のマイクロプロセッサで行うことができる利点がある．また，後述のようにマルチプレックス機能による暗号処理操作を行うことができる等の利点が得られる．

以上のような利害得失があるが，本暗号プロセッサでは，暗号プロセッサ本体の回路規模を小さくできる点を最重視し，外部の制御用マイクロプロセッサで拡大鍵を作成し，暗号プロセッサ内のレジスタに拡大鍵を外からセットする方法を採用することとした．

3.2 上位プロトコルを持たないデータの暗号

一般に，データ端末装置では，ISO，CCITT で標準化されている OSI プロトコル[5),6)] を用いてデータ伝送を行う．この場合，通信文が暗号化されたものかどうかはレイヤ間で取り決められた制御情報を通信文のヘッダに付与することによって容易に区別ができる．しかし，物理レイヤのプロトコルしか持たない音声コード，例えば μ 法則符号化法で符号化されたディジタルコード[7)] の暗号通信を行うためには，送信側で暗号化された音声コードの先頭位置を受信側で実時間で確実に検出し復号を開始する方式を開発する必要がある．このために，**図3**に示す暗号通信プロトコルを考案し，本プロトコル処理機能を暗号プロセッサに搭載した．

[送信側]：暗号化を開始する場合，音声コードの代わりに，1バイトの特定コード（IDL コード）を連続 M 回送信し，次に1バイトの特定コード（EOC コード）を1回送信し，以後の音声コードを暗号化して送信する．

[受信側]：受信データから IDL コードを連続 N 回（$N \leqq M$）検出すると外部割り込みを発生するとともに，EOC コード待ち状態になり，EOC コードを検出すると外部割り込みを発生し，以後の受信データ（暗号化された音声コード）から復号を開始する．

同様に，暗号通話から通常通話への切り替えは次のように行う．

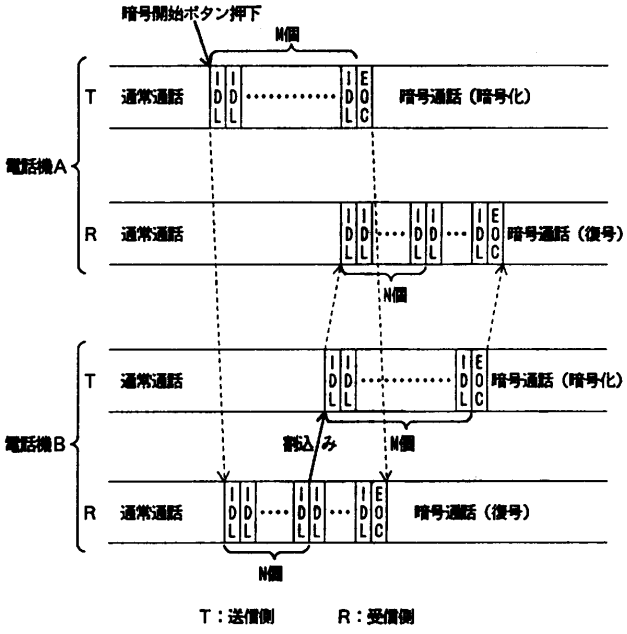


図3 音声コードの暗号通信プロトコル（暗号化開始の場合）
Fig. 3 Encryption transmission protocol for voice data.

[送信側]：暗号化された音声コードの代わりに，連続M個の IDL コードを暗号化して送信し，次に EOC コードを1個暗号化して送信し，以後の音声コードは暗号化せずに送信する．

[受信側]：復号後のデータ列から IDL コードを連続N個（$N \leqq M$）検出すると，外部割り込みを上げるとともに EOC コード待ちとなり，EOC コードを検出すると外部割り込みを上げ，以後の受信データから復号動作を停止する．

IDL, EOC はマイクロプロセッサ等により外部から任意のコードを設定でき，またM, Nは 1～255 の範囲の値の中から任意の値を設定できるようにした．本機能は音声と同様に上位プロトコルを持たない音声映像データの暗号化，復号にも適用可能である．

4. ハードウェア設計

4.1 プロセッサの構成

全二重通信では，送信データの暗号化と受信データの復号を並行に処理する必要がある．このため，**図4**のブロックダイヤグラムに示すように，プロセッサを1つの暗号演算部とチャネルAとチャネルBの2系統の入出力バッファ部で構成し，演算実行中に2チャネルのデータ入出力を独立に実行するパイプライン処理方式を採用した．これによって，プロセッサのゲート数削減と性能向上を図っている．以下にプロセッサ各部の構成法について述べる．

4.1.1 入出力インタフェース

（1） 外部データバス：汎用マイクロプロセッサに接続可能な8または 16 ビットの双方向バスとした．32 ビットバスにした場合には，ECB, CBC モードの処理性能が 16 ビットバスの場合の約 1.4 倍になる（4.2.1 項参照）．しかし，(a)マルチメディア通信における暗号利用モードは CFB, OFB モードが主な利用モードであること，(b)ピン数増により LSI 価格が上昇すること，(c)通信機器で利用されるマイクロプロセッサは 8/16 ビットが主流であることから，ECB, CBC モードの性能アップよりも LSI の経済化を優先し，16 ビットバスを採用することとした．また，外部データバスにはチャネルAとチャネルBの入出力が独立に行えるよう4組の DMA 転送機能を設けた．

（2） ビットシリアルインタフェース：音声等の PCM CODEC（8ビット単位のフレーム同期信号があるシリアルインタフェース）に直接接続するシリアルインタフェースを2組（送信側と受信側）設けた．また，ディジタル PBX 等の時分割多重通信システムにも適用可能にするため，1フレーム期間だけ出力をローインピーダンスにし，それ以外はハイインピーダンスにする仕様にしている．本インタフェースは，CFB, OFB モードで利用可能である．

4.1.2 入出力バッファ部

入力，出力バッファ部にそれぞれチャネルA，チャ

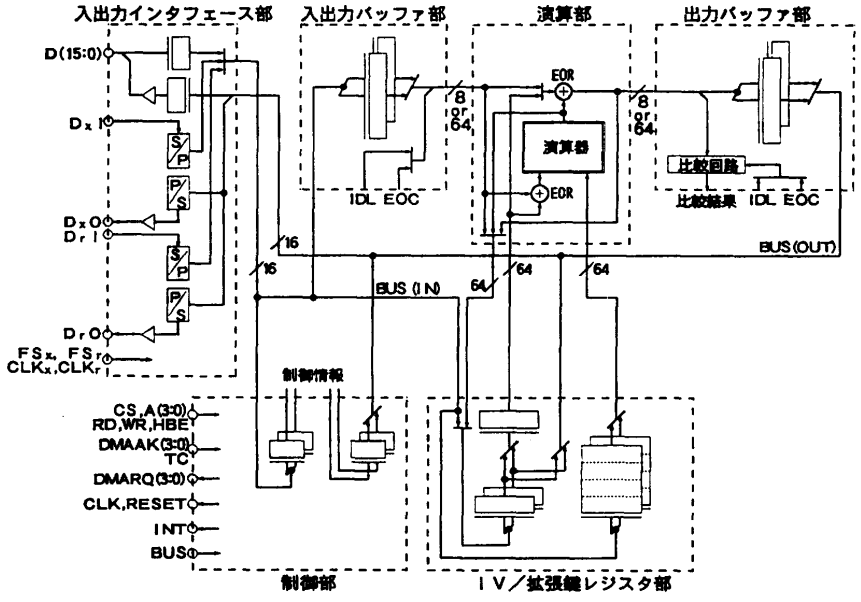


図 4 本暗号プロセッサの回路構成
Fig. 4 The structure of the encryption processor.

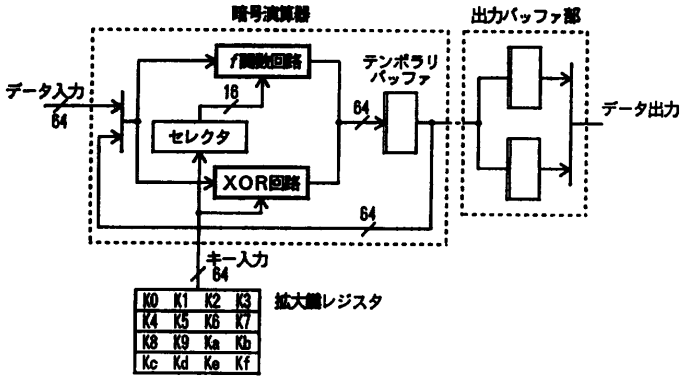


図 5 暗号演算器の構成
Fig. 5 The encryption arithmetic unit.

ネルBの2組の8バイトバッファを用意している．入力バッファ部はビットシリアルデータの暗号化開始/終了時における IDL, EOC コードの送信機能を持つ．出力バッファ部には，受信チャネルの IDL, EOC コードをモニタする比較回路が接続され，同コードの検出機能を持たしている．

4.1.3 暗号演算器

暗号演算器は図5に示すように f 関数回路と排他的論理和回路で構成される．

4.1.4 IV/拡大鍵レジスタ部

A，B両チャネルに対応する2組の IV レジスタ（8バイト）と2組の拡大鍵レジスタ（32 バイト）で構成される．

IV レジスタは，CBC, CFB および OFB モードの初期値およびフィードバックデータを格納し，プロセッサ外部から書き込みと読み出しの両操作ができる．拡大鍵レジスタはプロセッサ外部から書き込み操作ができる．これにより，LSI のチャネルA，Bを時分割で共用し外部のサブチャネルメモリとの間でデータ入出力操作を行うこと（マルチプレクス機能）により多数のチャネルの同時暗号処理ができるようにしている．

以下にマルチプレクス機能による暗号処理の操作手順を示す．

（1） 暗号利用モード，転送方法等を制御レジスタにセットする．

（2） 拡大鍵を外部のサブチャネルメモリから拡大鍵レジスタに転送する．

（3） 初期値（IV）またはフィードバックデータをサブチャネルメモリから IV レジスタに転送する．

（4） 暗号化または復号するデータを入力バッファに転送する．

（5） 暗号化または復号されたデータを出力バッファから外部メモリへ転送する．

（6） フィードバックデータを IV レジスタからサブチャネルメモリに出力する．

（7） (1)～(6)を繰り返す．

本暗号プロセッサは，フィードバックデータの読み出しができるので，データの改ざん検出を行うメッセージ認証用としても使用できる．

4.2 パイプラインの動作

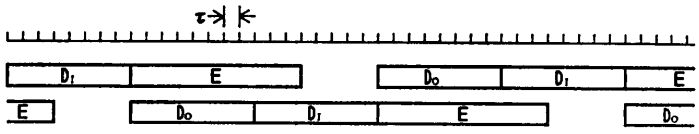
4.2.1 バイトパラレル処理

パイプライン処理のタイムチャートを図6に示す．

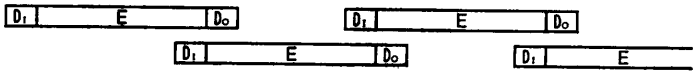
（1） データ書き込み (D_I)：書き込み信号を検出しデータと該当のレジスタアドレスをラッチするのに最小1クロック，プロセッサ (LSI) の内部バスを開けて入力バッファ部の該当チャネルのバッファに転送するのに1クロック，最小2クロックで動作する．

（2） データ読み出し (D_O)：読み出し信号とアドレスの取り込みに最小1クロック，LSI のシステムクロックに同期して該当レジスタから内部バスを経由して入出力インタフェースのバッファに格納するのに1クロックが必要であり，最小で2クロックで動作する．

（3） 演算実行（E）：演算実行サイクルを次の 11



（a） ECB, CBC モードの場合
（a） In the case of ECB and CBC modes.



（b） CFB-8, OFB-8 モードの場合
（b） In the case of CFB-8 and OFB-8 modes.
D_I：データ入力　D_O：データ出力　E：暗号演算実行
τ：暗号プロセッサの内部クロック

図 6 バイトパラレル処理の動作
Fig. 6 Encryption processing in byte parallel data.

クロックで動作する．

（a） 最初に，入力データを排他的論理和回路に送り，結果をテンポラリバッファに格納する（図1の①を実行）．

（b） テンポラリバッファの出力データを f 関数回路に帰還し，結果をテンポラリバッファに格納する．この操作を8回繰り返す（図1の②～⑨を実行）．

（c） テンポラリバッファの出力データを排他的論理和回路に帰還し，結果をテンポラリバッファに格納する（図1の⑩を実行）．

（d） 最後に，テンポラリバッファのデータを出力バッファに格納する．

ECB, CBC モードでは，4回のデータ入力（16 ビットバス利用）で入力バッファ部に8バイトのデータが格納される．入力チャネルと同じチャネルの出力バッファ部に8バイト分の空きがあれば暗号演算の実行を開始する．演算実行が終わると，4回のデータ出力で8バイトを外部データバスに出力する．ECB, CBC モードでは，2回のデータ入出力の間に演算実行を1回行う．以上のように，ECB, CBC モードの場合は外部データバスのデータ転送能力でプロセッサの処理性能が決まる．

OFB-8, CFB-8 モードでは入力バッファ部に1バイト以上のデータが格納されると，同じチャネルの出力バッファ部に1バイト以上の空きがあれば暗号演算実行を開始する．演算実行時間は，ECB, CBC モードと同じである．この場合には，1バイトのデータの暗号演算実行中に前の演算結果のデータ出力と次の演算の入力データをプレフェッチすることができ，演算部をフル稼働の状態にして処理可能である．

4.2.2 ビットシリアル処理

入力がビットシリアルデータの場合，外部からの非同期信号をサンプリングするために，プロセッサのクロック周波数（f）とシリアルデータのビットレート（v）との間に，

$$4v \leqq f$$

の条件が必要である．したがって，1バイトのデータ入力時間は最小で 32 クロック必要である．プロセッサ性能は，ビットシリアルデータのデータ入出力処理に要する時間で決まる（図7）．

4.3 デバグ機能

暗号演算部をトランスペアレント状態にして，プロセッサ外部からの入力データがそのままプロセッサ外部に出力されるかをチェックするデータパス系の診断機能，および本プロセッサを外部から制御するハードウェア，ソフトウェアの設計バグを容易に発見するために，エラーが発生したチャネル番号と詳細なエラー内容をエラー表示レジスタに表示する機能をプロセッサに搭載した．

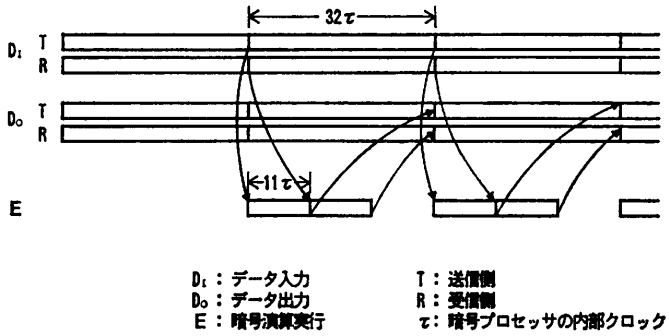


図7 ビットシリアル処理の動作
Fig. 7 Encryption processing in bit serial data.

5. 実現結果と性能

本暗号プロセッサは，1ミクロンルール，メタル3層配線の CMOS ゲートアレイを用いて設計し，コンパクトな 60 ピンのプラスチック・フラット・パッケージに収容した（図8参照）．使用ゲートは 13.5 キロゲートである．入出力端子を付表に示す．

本プロセッサをシステムクロック 20 MHz で動作させた場合，ECB, CBC モードでは最大で 10 M バイト/秒，CFB-8, OFB-8 モードでは 1.8 M バイト/秒の処理性能が得られる．また，全二重のビットシリアルデータを最大 5 M ビット/秒の速度——ISDN の1次群速度インタフェースのデータ伝送速度を越え

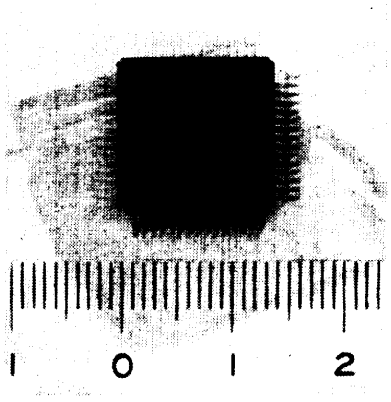


図8 本暗号プロセッサの外観
Fig. 8 The single-chip encryption processor.

る——で暗号化と復号を同時に行う処理性能がある．チップ消費電力は，200 ミリワットである．

6. 利 用 例

6.1 ISDN ディジタル電話機

ISDN ディジタル電話機に適用した例を図 9 に示す．音声 CODEC と ISDN レイヤ 1 処理 LSI の間の入出力信号を中継する位置に本暗号プロセッサを実装し，ディジタル電話機の MPU とバス接続する．MPU がバスを通して暗号プロセッサの内部レジスタに拡大鍵や初期値等の制御情報をセットすることにより暗号化の開始，終了の制御を行う．このように既存のディジタル電話機のハードウェアに本暗号プロセッサを追加するだけで秘話機能付きの電話機が実現できる．図 10 は，本プロセッサを搭載した盗聴防止型ディジタル電話機の外観である．本機では左下の暗号ボタンを押下して通常通話，暗号通話の切り替えを行う．切り替えは，2～3 ミリ秒 (15～25 個程度) の IDL コードの送出で可能であり，音声 CODEC のローパスフィルタを通過した音がわずかにクリック音

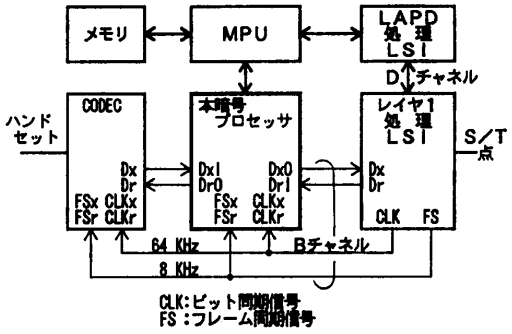


図 9 ディジタル電話機への適用例
Fig. 9 An example of the applications to ISDN digital telephones.

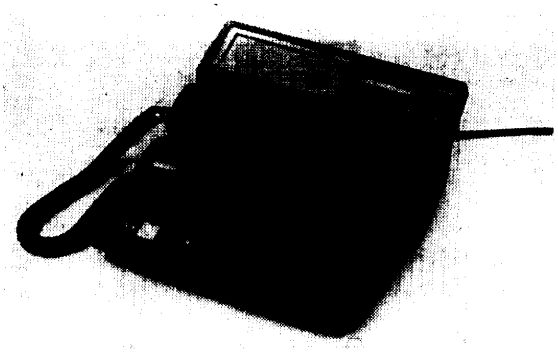


図 10 盗聴防止型ディジタル電話機
Fig. 10 The ISDN digital telephone set capable of cipher communications.

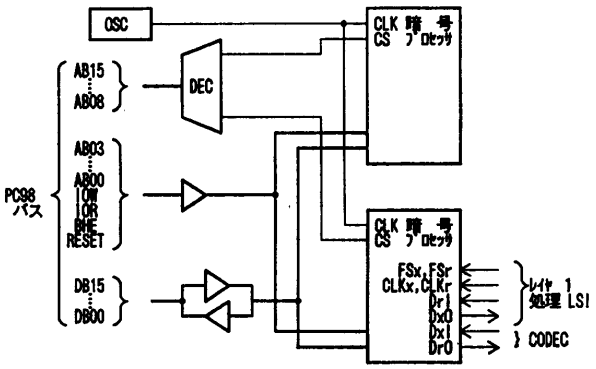


図 11 パソコン用暗号処理ボードの構成例
Fig. 11 An example of encryption plug-in expansion board for personal computer.

となって聞こえるだけである．

6.2 パーソナルコンピュータ用暗号処理ボード

PC 9801 シリーズパーソナルコンピュータ用の暗号処理ボードの一構成例を図 11 に示す．この暗号処理ボードは本暗号チップ 2 個とアドレスデコード，PC 98 バスのドライブ回路の IC，計 7 チップと水晶発振子から構成でき，音声の実時間暗号処理と並行してファイルデータの暗号処理ができる．本暗号処理ボードの制御プログラムは C 言語等の高級言語で容易に作成できる．すなわち，暗号 LSI の処理時間がパソコンの汎用ポートへのデータ入出力命令時間より高速であるため，Out 命令と In 命令を繰り返し実行するだけで，ファイルデータの暗号処理を実行することができる．本ボードを PC-9801 RA に収容し，C 言語で制御プログラムを記述した場合，2.2 Mbps のスループットが得られている[8]．

7. おわりに

開発した暗号プロセッサは，ファイルデータの一括暗号処理だけでなく，高速のビットシリアルデータの実時間暗号処理に適用でき，現在知られている暗号 LSI の中で最もコストパフォーマンスが優れたワンチッププロセッサである．本プロセッサはディジタル電話機，ファクシミリ，テレビ会議装置などの各種のマルチメディア通信機器に搭載でき，ISDN を利用した新しいアプリケーションサービスやパーソナル通信サービスの発展に寄与するものと期待される．

謝辞 本研究の機会を与えてくださった NTT 情報通信処理研究所 石野福彌所長，FEAL 暗号アルゴリズムについてご指導いただいた同研究所情報システム研究部 栗原定見主席研究員に感謝いたします．

参考文献

1) 宮口，白石，清水：FEAL-8暗号アルゴリズム，研実報，Vol. 37, No. 4/5, pp. 321-327 (1988).
2) 小山：情報セキュリティ，pp. 76-88，電気書院東京 (1989).
3) 宮口，栗原，太田，森田：FEAL 暗号の拡張，NTT R & D, Vol. 39, No. 10, pp. 1439-1450 (1990).
4) ISO 8372, Information Processing—Modes of Operation for a 64-bit Block Cipher Algorithm (1987).
5) ISO 7498-1, Information Processing Systems—Open Systems Interconnection—Basic Reference Model (1984).
6) CCITT Recommendation X. 200, Reference Model of Open Systems Interconnection for CCITT Applications (1984).
7) CCITT Recommendation G. 711, Pulse Code Modulation (PCM) of Voice Frequencies (1972).
8) 小柳津，松本，石井：パソコン間暗号通信方式の一検討，情報処理学会研究会報告，91-DPS-50-2 (1991).

小柳津育郎（正会員）

1968年名古屋大学工学部電気学科卒業．1970年同大学院工学研究科修士課程修了．同年日本電信電話公社（現 NTT）に入社．現在 NTT ヒューマンインタフェース研究所第四プロジェクトチームにおいて ISDN を利用したマルチメディア通信システムの研究・開発に従事している．主幹研究員（プロジェクトチームリーダ）．電子情報通信学会会員．

松本 博幸（正会員）

1972年東京電機大学工学部電気通信工学科卒業．同年日本電信電話公社（現 NTT）に入社．現在 NTT ヒューマンインタフェース研究所第四プロジェクトチームにおいてネットワークセキュリティおよび画像処理に関連した研究開発に従事．主幹研究員．電子情報通信学会会員．

付表 1 入出力端子

端子名	入出力	機能
Vdd	—	+5 ボルト電源
Vss	—	グランド
CLK	I	システムクロック入力
RST*	I	リセット入力
CS*	I	チップセレクト信号
WR*	I	書き込み動作指定
RD*	I	読み出し動作指定
UBE*	I	上位バイト/下位バイト指定
A3-A0	I	内部レジスタ指定アドレス
D15-D0	I/O	双方向3ステートデータバス
INT	O	CPU への割り込み要求
DMARQ 3*-0*	O	DMA 転送要求
DMARK 3*-0*	I	DMA コントローラからの応答信号
TC*	I	DMA コントローラからの転送終了信号
FSx, FSr	I	8ビット単位のフレーム同期信号
CLKx, CLKr	I	ビット同期信号
DxI	I	音声 CODEC 等からのビットシリアル入力
DxO	O	Sインタフェースへの3ステートビットシリアル出力
DrI	I	Sインタフェースからのビットシリアル入力
DrO	O	音声 CODEC 等への3ステートビットシリアル出力
BUS	I	8/16 ビットのデータバス幅の選択
TEST	I	テスト指示，通常は“0”にする．

注）端子名の後の * は負論理であることを示す．
I：入力端子，O：出力端子

（平成3年 5 月 29 日受付）
（平成3年12月 9 日採録）

石井 晋司（正会員）

1987年職業訓練大学校電子科卒業．1989年埼玉大学大学院工学研究科電気工学専攻課程修了．同年日本電信電話株式会社に入社．NTT ヒューマンインタフェース研究所第四プロジェクトチームにおいて ISDN 端末のデータセキュリティに関する研究開発に従事．電気学会会員．