マルチメディア通信と分散処理　48－10
（１９９１．１．２４）

マルチメディア通信用暗号ＬＳＩ

小柳津　育郎　　松本　博幸　　石井　晋司

ＮＴＴ情報通信処理研究所

ＮＴＴが開発したＦＥＡＬ－８暗号アルゴリズムを採用し，メモリに格納されたデータの暗号処理だけでなく，音声，映像等のリアルタイムで発生するデータの暗号処理に適用できる小型で低価格なマルチメディア通信用暗号ＬＳＩを開発中である．本報告では，主に，プロトコルを持たないストリームデータの暗号化開始と復号開始の同期機能の提案とその実現方法，全二重通信のための送信データの暗号化と受信データの復号の同時動作を効率良く行うＬＳＩ構成法，音声，映像コーデックの直接接続方法についてを述べる．本ＬＳＩはＥＣＢ，ＣＢＣモードで５３Ｍビット／秒，ＣＦＢ，ＯＦＢモードで１５Ｍビット／秒，ビットシリアルで５Ｍビット／秒の処理速度を実現できる見通しを得た．

THE FEAL ENCRYPTION PROCESSOR FOR MULTIMEDIA COMMUNICATIONS

Ikuro Oyaizu　　Hiroyuki Matsumoto　　Shinji Ishii

NTT Communications and Information Processing Laboratories.

The single chip FEAL encryption processor has been developed which is not only capable of encryption in bulk text data and file data contained in storage but can also handle the encryption of multimedia data, including voice and audiovisual data in real time.

The following new techniques installed in the encryption processor for multimedia communication usage are mainly discussed in this paper.

(1) The encryption transmission protocol to encipher stream data which has only physical layer protocol of data transmission, such as voice or audiovisual data.

(2) Pipeline processing to handle the enciphering of transmitted data and deciphering of receiving data in full duplex mode, by sharing one encryption arithmetic unit.

１．まえがき

ＩＳＤＮの普及により，本格的なマルチメディア通信の時代が始まった．一方，企業秘密や個人のプライバシ保護のためのデータ・セキュリティの必要性が強く要求されている．データ・セキュリティの技術的対策として「データの暗号(*)処理」は最も有力な手段である．我々は，ＮＴＴが開発した秘密鍵暗号方式で暗号アルゴリズムを公開したＦＥＡＬ（Fast Data Encipherment Algorithm）暗号アルゴリズム[1]を採用し，メモリ上に格納されたデータの暗号化／復号処理だけでなく，音声，映像等のリアルタイムで発生するデータの暗号化／復号処理に適用できるマルチメディア通信用暗号ＬＳＩを開発中である．本資料は，このＬＳＩの技術的課題，構成，性能，およびディジタル電話機等への適用例等について述べる．

２．技術的課題

マルチメディア通信用暗号ＬＳＩの開発における主な技術的課題は，以下のような機能を経済的に実現することである．

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開始と復号開始の同期確立．

②全二重通信を可能にするための送信データの暗号化処理と受信データの復号処理の同時動作．

③ＩＮＳネット１５００のH0チャネル（1.5Mbps）にも適用可能な高速ビットシリアルデータの暗号処理．

④汎用マイクロプロセッサ（８／１６ビット）バスインタフェースとの直接接続．

⑤音声・映像等のＰＣＭコーデック（８ビット単位のシリアルインタフェース）との直接接続．

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．

⑦暗号処理はＩＳＯ，ＪＩＳ仕様に準拠．

３．機能条件の検討

３．１　暗号方式

暗号方式は表１に示す様に，暗号化鍵を公開するかどうかで秘密鍵暗号方式（慣用暗号方式）と公開鍵暗号方式に大別され，さらに前者は暗号アルゴリズムを公開にするものと，秘密にするものがある[2]．

本ＬＳＩは暗号処理速度が高速で，暗号アルゴリズムを公開しているＦＥＡＬ暗号アルゴリズムを採用する．ＦＥＡＬ暗号アルゴリズムは暗号処理の内部処理段数と鍵の長さが利用者のオプションとして指定できるが[3]，本ＬＳＩではファクシミリ装置やＩＣカード等で実績のあるＦＥＡＬ－８暗号アルゴリズム(以下，ＦＥＡＬ－８と略す)を適用する．

ＦＥＡＬ－８のような６４ビットのブロック暗号アルゴリズムは，以下の暗号利用モードがＩＳＯ，ＪＩＳで標準化されており[4,5]，本ＬＳＩはこれら全ての暗号利用モードを搭載する．各暗号利用モードの特徴を表２に示す．

①ＥＣＢ（Electronic Codebook）モード

②ＣＢＣ（Cipher Block Chaining）モード

③ＣＦＢ（Cipher Feedback）モード

④ＯＦＢ（Output Feedback）モード

ここで，ＣＦＢ，ＯＦＢモードでは任意ビット単位の暗号化または復号が可能であるが，データ通信，音声等は８ビット（１バイト）単位である

表１　暗号方式の分類

項目＼暗号方式	秘密鍵暗号		公開鍵暗号
暗号鍵の関係	暗号化鍵＝復号鍵		暗号化鍵≠復号鍵
暗号化鍵	秘密		公開
復号鍵	秘密		秘密
暗号ｱﾙｺﾞﾘｽﾞﾑ	秘密	公開	公開
代表例	ﾊﾞｰﾅﾑ、ｼｰｻﾞｰ	ＦＥＡＬ、DES	RSA、ｴﾙｶﾞﾏﾙ
暗号化速度	速い		遅い

(*)本資料では平文を暗号文に変換することを「暗号化」といい，暗号文を平文に変換することを「復号」といい，暗号化と復号の総称を「暗号」という[5]．

表2　各暗号利用モードの特徴

モード	特　　徴
ＥＣＢ	• 1ﾌﾞﾛｯｸ(64ﾋﾞｯﾄ)単位の暗号。 • 同一内容のﾌﾞﾛｯｸは同一の鍵に対して同一の暗号文となるため暗号強度は弱い。 • 主に鍵、IVを相手側に送信するときに使用する。
ＣＢＣ	• 複数ﾌﾞﾛｯｸからなるﾃﾞｰﾀの暗号。 • 暗号処理結果と次の入力ﾃﾞｰﾀと演算し、更に暗号処理するので暗号強度は強い。 • 主にﾌｧｲﾙの伝送、蓄積時に使用する。 • ﾃﾞｰﾀ長は64ﾋﾞｯﾄの倍数でなければならない。 • 演算単位が64ﾋﾞｯﾄ単位であるため演算効率が良い。 • 一つの暗号文ﾌﾞﾛｯｸ内のﾋﾞｯﾄ誤りはそのﾌﾞﾛｯｸおよび次のﾌﾞﾛｯｸの復号に影響を及ぼす。
ＣＦＢ	• 任意ﾋﾞｯﾄ長(一般には8ﾋﾞｯﾄ)単位の暗号。 • 暗号化演算と復号演算は同じである。 • 1文字(8ﾋﾞｯﾄ)単位の暗号で一つの暗号文字内のﾋﾞｯﾄ誤りはその文字および以降の8文字の復号に影響を及ぼす。 • 主にﾃﾞｰﾀ通信に使用する。 • 暗号強度はOFBﾓｰﾄﾞより強い。
ＯＦＢ	• 任意ﾋﾞｯﾄ長(一般には8ﾋﾞｯﾄ)単位の暗号。 • 暗号化処理と復号処理は同じである。 • 1文字単位の暗号で一つの暗号文字内のﾋﾞｯﾄ誤りはその文字の復号にのみ影響を及ぼす。 • 主に音声、映像等の伝送に使用する。

こと，本ＬＳＩが適用されると考えられるファクシミリ，データ端末等の装置に採用されている各種のＬＳＩは1バイト単位でデータを処理していることより８ビットのみを採用した．（以下ＣＦＢ－８モード，ＯＦＢ－８モードと略す）

本ＬＳＩに搭載した暗号利用モードの構成を図1に示す．

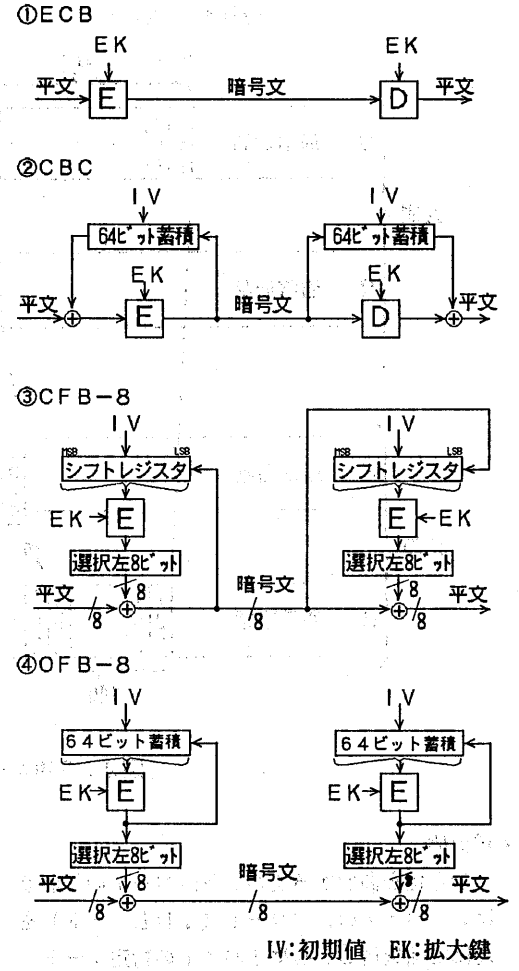

図1　本ＬＳＩの暗号利用モード

３．２　プロトコルを持たないデータの暗号

一般にデータ端末等で使用されるデータ通信のプロトコルは，ＩＳＯ，ＣＣＩＴＴで標準化[6,7]されているＯＳＩ（Open Systems Interconnection）プロトコルに準拠しており，通信内容を暗号処理する場合，ＯＳＩプロトコルレイヤに対応したＬ－Ｌ（Link by Link）暗号方式と，Ｅ－Ｅ（End to End）暗号方式の形態が考えられる[8,9]．一方，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[10]）の通信ではデータ通信の様なプロトコルを持たないため，新たな方法を用いて以下の機能を実現しなければならない．

- 送信側

　音声コードの暗号化を開始するとともに，暗号化を開始した音声コードを受信側に知らせる機能．

- 受信側

　暗号化が開始された音声コードを検出し，その音声コードから復号を開始する機能．

上記機能を実現するために次の手段を考案した．（図２参照）

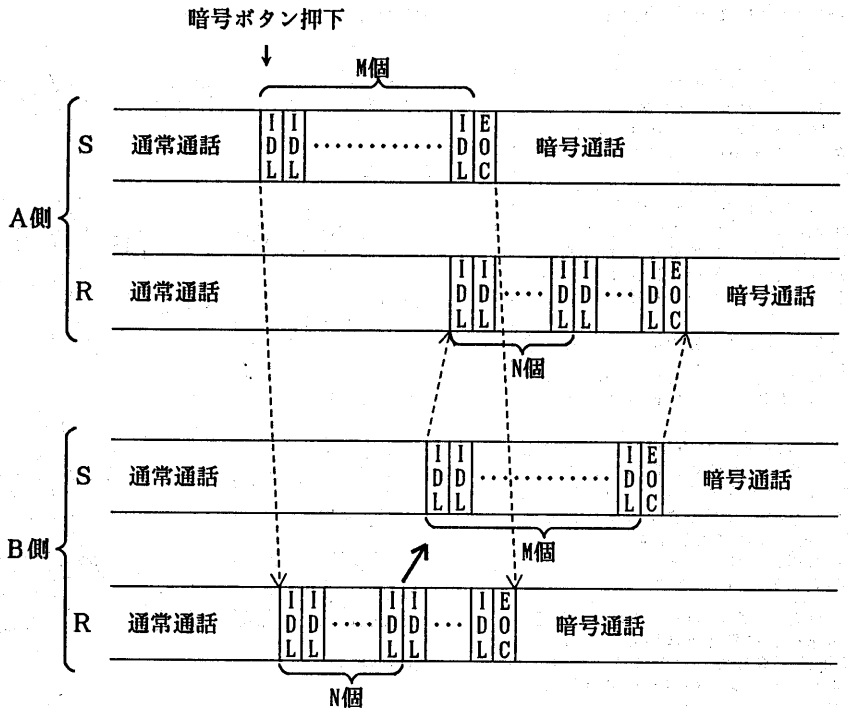

図2．音声コードの暗号化手段

• 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≦M）検出すると割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，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．

本機能は，PCMコーデックインタフェース（4．4章で説明）使用時に動作し，IDL，EOCコードは任意のコードを設定可能に，M，Nの値は1～255を設定可能にした．

本機能は音声と同様にプロトコルを持たない画像データの暗号化および復号にも適用可能である．

4．LSIの構成

4．1　パイプライン構成

全二重通信を可能にするため，暗号化処理と復号処理の同時処理が必要となる．ここで外部バスからのデータ転送時間（TI），暗号化または復号の処理時間（TE），外部バスへのデータ転送時間（TO）についてみると（TI，TE，TOの値は5章を参照），ECB，CBCモード（8バイト処理）では

$$TE < TI + TO$$

CFB－8，OFB－8モード（1バイト処理）では

$$TE > TI + TO$$

となるが，マルチメディア通信で扱うデータ長は１バイト単位が主であるため，暗号化処理と復号処理を行う暗号化／復号処理部を１組，入力バッファ部，出力バッファ部をそれぞれ２組（Ａ系，Ｂ系）から成る構成にし，暗号化／復号処理部，入力バッファ部，出力バッファ部はそれぞれ独立に動作するパイプライン構成にし，ＬＳＩのハードウェア削減と性能向上を図った．

動作は入力バッファ部のバッファに演算対象分（ＥＣＢ，ＣＢＣモードでは８バイト，ＯＦＢ－８，ＣＦＢ－８モードでは１バイト）以上のデータが格納され，かつ出力バッファ部のバッファが演算対象分以上空になれば演算を開始し，演算結果を出力バッファ部のバッファに格納する．

なお全二重通信では暗号化処理と復号処理が同時に行われるが，本ＬＳＩの適用範囲を拡大するために，Ａ系，Ｂ系とも独立に暗号化処理または復号処理の何れでも選択可能とした．

４．２　鍵の拡大処理

ＦＥＡＬ－８は６４ビット長からなる鍵の各ビットを混ぜ合わせ，その長さを２５６ビットに拡大した鍵（拡大鍵）を用いて，入力データを暗号化処理または復号処理する[1]．ここで鍵の拡大処理についてみると，

①鍵の変更は頻繁に行われない．鍵を変更しない限り鍵の拡大処理は必要ない．

②鍵の拡大処理は高速性を必要としない．

③鍵の拡大処理を本ＬＳＩ上で実現する場合約４．５Ｋゲートの回路規模を必要とし，ＬＳＩの回路規模が大幅に増加する．

等より鍵の拡大処理は本ＬＳＩを制御するマイクロプロセッサ等で行い，拡大鍵をＲＯＭまたはＲＡＭ等の外部メモリ上に格納しておく．電源投入時，或いは鍵を変更したときにこの拡大鍵を本ＬＳＩ内の拡大鍵レジスタ（２５６ビット）にセットする方法を採用した．

なお拡大鍵レジスタはＡ系用，Ｂ系用と独立に持ち，外部メモリとの間の転送を高速に行うためにデータ転送と同様にＤＭＡ転送も可能にした．

４．３　マルチプレックス機能

ＣＢＣ，ＣＦＢ－８，ＯＦＢ－８モードにおけるフィードバックデータ（８バイト）をＬＳＩ外部への読みだしと，ＬＳＩ外部から書込みを可能にし，Ａ系，Ｂ系とも多チャネルの同時暗号処理（マルチプレックス機能）を可能にした．以下にマルチプレックス機能を用いた該当チャネルの暗号処理の操作方法を示す．

①暗号利用モード，転送方法等をモードレジスタにセット．

②拡大鍵を外部メモリより拡大鍵レジスタに転送．

③初期値（ＩＶ）またはフィードバックデータを外部メモリよりＩＶレジスタに転送．

④暗号化または復号するデータをデータレジスタに転送．

⑤暗号化または復号されたデータをデータレジスタから外部メモリに転送．

⑥フィードバックデータをＩＶレジスタからメモリ素子に転送．

ここでＩＶレジスタもＡ系用，Ｂ系用と独立に持ち，外部メモリとの間の転送を高速に行うためにＤＭＡ転送も可能にした．

またフィードバックデータの読みだしが可能なことにより，データの改ざん検出を行うメッセージ認証[11]にも本ＬＳＩを利用可能である．

４．４　ＰＣＭコーデックインタフェース

音声等のＰＣＭコーデックに直接接続する８ビット単位のシリアルインタフェースを２組（送信側と受信側）設け，本ＬＳＩをディジタル電話機，ＩＳＤＮ端末等に容易に適用可能とした．またディジタルＰＢＸ等の時分割多重ＰＣＭ通信システムにも対応可能とするために，１フレーム期間だけ出力をロー・インピーダンスにし，それ以外では出力をハイ・インピーダンスにするようにした．

本インタフェースはＣＦＢ－８，ＯＦＢ－８モードで使用可能で使用可能である．

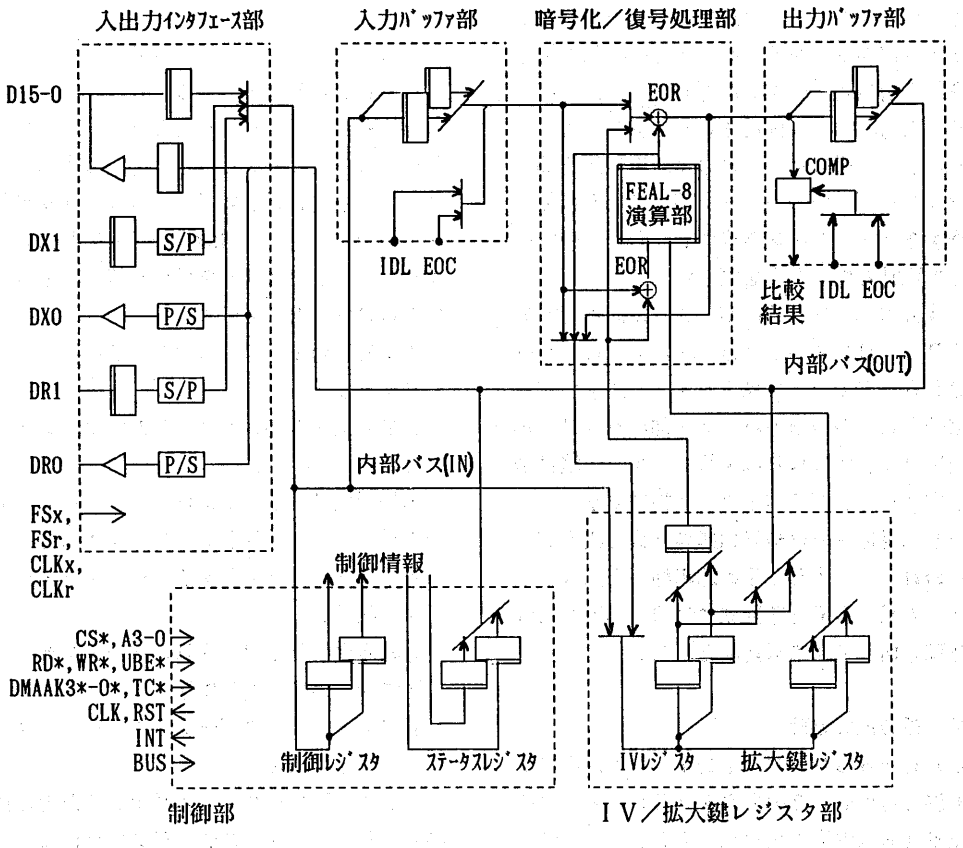

図３　本ＬＳＩの構成図

４．５　デバグ機能

ＦＥＡＬ－８演算部をトランスペアレント状態にして，入力データがそのまま出力されるかをチェックするデータパス系の自己診断機能，および本ＬＳＩを制御するハードウェア，ソフトウェアの制御ミスを容易に発見するために，制御ミスによってエラーが発生したチャネル番号と詳細なエラー内容を表示するようにした．

図３に本ＬＳＩの構成図を示す．

５．性能

５．１　パラレル転送

４．１章で述べたＴＩ，ＴＥ，ＴＯの値は以下のようになる．

$TI=3\tau$，$TE=11\tau$，$TO=3\tau$

ここでτは１クロックサイクル時間である．

各暗号利用モードの暗号化または復号の処理時間，外部バスとのデータ転送の総和時間を算出した結果を表３に示す．

表３よりバス幅＝２バイト，ＥＣＢ，ＣＢＣモードについてみると，

$TE(11\tau)<4\times(TI+TO)=24\tau$

またバス幅＝１バイト，ＣＦＢ－８，ＯＦＢ－８モードについてみると，

$TE(11\tau)>TI+TO=6\tau$

以上より，ＥＣＢ，ＣＢＣモードでは外部バスとのデータ転送がネックになって処理性能が抑え

表3　暗号モードと処理時間，データ転送時間

暗号モード / 項目		ECB，CBC	CFB－8，OFB－8	
		8ﾊﾞｲﾄ当たり	2ﾊﾞｲﾄ当たり	1ﾊﾞｲﾄ当たり
暗号処理		11τ	2×11τ	11τ
データ転送	1B	8×3τ	——	3τ
	2B	4×3τ	3τ	——

τ：1クロックサイクル時間

表4　本LSIの性能　(Mbit/s)

暗号モード / ﾊﾞｽ幅	ECB、CBC	CFB－8、OFB－8
1バイト	A＋B≦26.7	A≦14.5 B≦14.5
2バイト	A＋B≦53.3	A≦14.5 B≦14.5
シリアル	——	A≦5 B≦5

A：A系　　B：B系

られ，CFB－8，OFB－8モードでは演算部がフル稼働状態である．

性能は，例えばクロック周波数＝20MHzの場合，ECB，CBCモードでは6．7Mバイト／S，CFB－8，OFB－8モードでは3．6Mバイト／Sとなり，高機能16ビットマイクロプロセッサによるプログラム転送，またはDMAコントローラによるDMA転送の転送速度と同等かそれ以上である．

なお，性能はクロック周波数と比例関係にある．

5．2　シリアル転送

PCMコーデックインタフェース使用（シリアル転送）ではLSIのクロック周波数（F）とシリアルデータの通信速度（V）との関係は，外部からの非同期に変化するデータの同期化等より，

$$4V \leqq F$$

となり，1バイト当たりのデータ転送速度（TS）は最高32τとなる．よって全二重動作時でも

$$TS > 2TE$$

となり，シリアルデータ転送がネックになって処理性能が抑えられている．

表4に本LSIの性能を示す．

6．適用例

本LSIは情報の送受信または蓄積を行うエレクトロニクス製品に適用可能である．代表的適用例として以下のようなものが考えられる．

①ディジタル電話機．
②ファクシミリ装置．
③モデム．
④ワークステーション（LAN，ISDN等）．
⑤パソコン（パソコン通信，ISDN等）．
⑥ディジタルPBX．
⑦守秘性の高いデータのバックアップ用光磁気ディスク，DK，MT，FD等．

7．あとがき

本LSIはパラレルデータの暗号化／復号処理および，通信プロトコルを持たないシリアルデータの暗号化／復号処理を高速に行う．また，FEAL－8はマイクロプロセッサ等でのプログラム処理向き暗号アルゴリズムであり，市販の8ビットマイクロプロセッサ（Z80，クロック周波数＝4MHz）でもECB，CBCモードで50Kbps程度の処理速度が達成できる[12]．ここでこのマイクロプロセッサ,ROM，RAM等を用いて専用の暗号処理モジュールを実現した場合のハードウェアコストと本LSIのコスト比較しても同程度である．これより低速な暗号処理を要求する分野においても本LSIの適用範囲となる．

表5に本LSIの仕様概略を示す．

表5　本ＬＳＩの仕様概略

項目＼品名			本ＬＳＩ	参考（現在国内で入手可能な代表的製品）	
				NLC5001F	CRY12C102
製造メーカ			NEL	NEL	Cryptech (ﾍﾞﾙｷﾞｰ)
暗号アルゴリズム			FEAL−8	FEAL−8	DES
暗号モード			ECB,CBC,OFB-8,CFB-8 (*1)	ECB,CBC,CFB-1 (*2)	ECB,CBC,OFB,CFB,OFB-8,CFB-8
ﾒｯｾｰｼﾞ認証機能			有り	無し	有り
最大ｸﾛｯｸ周波数			20MHz	12MHz	16MHz
最大演算処理速度			128Mbps(8ﾋﾞｯﾄ)	96Mbps(8ﾋﾞｯﾄ)	32Mbps(8ﾋﾞｯﾄ)
同時動作ﾁｬﾈﾙ数			2	1	
ﾏﾙﾁﾌﾞﾚｯｸｽ機能			有り	無し	
データ転送	ﾊﾟﾗﾚﾙ	バス幅	1B,2B(双方向)	1B(IN),1B(OUT)	1B,2B,4B(双方向)
		DMA転送	可能	不可	可能
	ｼﾘｱﾙ	ｲﾝﾀﾌｪｰｽ	8ﾋﾞｯﾄｼﾘｱﾙ(IN,OUT)(CODECｲﾝﾀﾌｪｰｽ)	1ﾋﾞｯﾄｼﾘｱﾙ(IN,OUT)	
		暗号同期	有り	無し	
ピン数	信号ピン		45	31	44
	電源		12	20	4
	計(ﾊﾟｯｹｰｼﾞ)		60(QFP)	128(QFP)	48(DIP)
テクノロジ	プロセス		CMOS	CMOS	
	配線ルール		1.0μm	1.5μm	3.0μm
	回路規模		13Kｹﾞｰﾄ	10Kｹﾞｰﾄ	――――
備考				[13]	[14]

*1:ECB,CBC,CFB-8,OFB-8ﾓｰﾄﾞ(ﾊﾟﾗﾚﾙ転送時). CFB-8,OFB-8ﾓｰﾄﾞ(ｼﾘｱﾙ転送時).
*2:ECB,CBCﾓｰﾄﾞ(ﾊﾟﾗﾚﾙ転送時). CFB-1ﾓｰﾄﾞ(ｼﾘｱﾙ転送時).

謝辞
本ＬＳＩの開発にあたり，御指導頂いた当所，情報システム研究部の栗原定見主幹研究員に感謝致します．

[参考文献]

(1) 宮口・白石・清水，ＦＥＡＬ−８暗号アルゴリズム，研実報，37，4/5，pp.321-327 (1988)
(2) 小山，情報セキュリティ，４章 暗号化技術，㈱電気書院 (1989)
(3) 宮口・栗原・太田・森田，ＦＥＡＬ暗号の拡張，NTTR&D vol.39 No.10 pp.1439-1450 (1990)
(4) ISO 8372,Information processing−Modes of operation for a 64-bit block cipher algorithm
(5) JIS X 5052,６４ビットのブロック暗号アルゴリズムの利用モード (1990)
(6) ISO 7498-1,Information processing systems - Open Systems Interconnection - Basic Refernce Model
(7) CCITT勧告X.200,REFERENCE MODEL OF OPEN SYSTEMS INTERCONNECTION FOR CCITT APPLICATIONS
(8) ISO 7498-2,Information processing systems - Open Systems Interconnection - Basic Refernce Model − Part2:Security Architecture
(9) 辻井・笠原，暗号と情報セキュリティ，７章 通信における情報セキュリティ，㈱昭晃堂(1990)
(10) CCITT勧告G.711,PULSE CODE MODULATION(PCM) OF VOICE FREQUENCIES
(11) 辻井・笠原，暗号と情報セキュリティ，６章 認証とディジタル署名，㈱昭晃堂(1990)
(12) 宮口，秘密鍵暗号による情報セキュリティ，ﾃﾚﾋﾞｼﾞｮﾝ学会誌 Vol.42,No.12,pp.1314-1318 (1988)
(13) 森田・山根・篠岡，高性能ＦＥＡＬ−８暗号ＬＳＩの設計，情処学会第３６回全国大会4C-5 (1988)
(14) I.Verbauwhede,F.Hoornaert,and J.Vandewalle:Security and Performance Optimization of a New DES Data Encryption Chip,IEEE J. Solid-State Circuits,vol.23,no.3,pp.647-656,(June 1988)