FEAL-N を適用した汎用暗号 LSI の開発

5H－1

松本　博幸　　小柳津　育郎
NTT ヒューマンインタフェース研究所

1. はじめに

我々は1991年に,メモリに格納された大量のファイルデータや音声等のプロトコルを持たないストリームデータを実時間で高速に暗号処理する FEAL-8 を適用した暗号 LSI を開発した[1]. 本 LSI は PC, ISDN 通信機器等で広く使用されている. その後,より暗号強度の強い FEAL-32 とともに,暗号鍵の不正読みだし防止機能, 勧告 H.233[2]に準拠したテレビ電話/会議用暗号機能等を搭載した暗号 LSI の開発が要求されてきた. そこでこれらの要求に応えるために, 従来開発した上記 LSI の機能と, 上記の要求機能を有する高機能な暗号 LSI を開発した. 本稿では主に上記の要求機能の実現方法および諸元等を報告する.

2. LSI の機能

2.1 従来 LSI の機能

新たに開発した暗号 LSI(以下"本 LSI"と略す)は, 従来開発した暗号 LSI(以下"従来 LSI"と略す)と互換性を図るために以下の機能を継承した.

①FAEL-8 暗号アルゴリズム.
②ECB,CBC,CFB-8, OFB-8 の暗号利用モード.
③音声等の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プロトコル.
④全二重通信のための暗号化と復号の同時動作.

2.2 FEAL-N の構成

NTT では,FEAL-8 を拡張した FEAL-N を提案した[3]. より暗号強度の強い暗号として文献(3),(4)は N≧32 を挙げている. そこで本 LSI では従来 LSI と互換性がある FEAL-8 および FEAL-32 を実現した. FEAL-N は与えられた 8 バイトの暗号鍵を(N/2+4)段の 関数 f_K で演算を行い,(2N+16)バイトの拡大鍵を生成する鍵処理部と,8 バイトの平文(暗号文)を排他的論理和による前処理, 拡大鍵と N 段の関数 f による演算, 排他的論理和による後処理を順に行い, 8 バイトの暗号文(平文)を出力するデータランダム化部から構成される. 以下にそれぞれの実現方法を示す.

鍵処理部は, 関数 f_K 回路および演算結果を一時保持するレジスタを 1 組づつ設け, 8 または 20 回演算を繰り返し, 結果(拡大鍵)を RAM に格納する方法を採用した.

データランダム化部は, 1 組の排他的論理和回路と, 関数 f 回路および演算結果を一時保持するレジスタを 1 組づつ設け, 最初に RAM から読みだした拡大鍵を排他的論理和回路に入力し, 次に RAM から逐次読みだした拡大鍵を関数 f 回路に入力し 8 または 32 回演算を繰り返し, 最後に RAM から読み出した拡大鍵を排他的論理和回路に入力する方法を採用した.

2.3 暗号鍵の不正読みだし/改竄防止

従来 LSI では, LSI 内部に拡大鍵の生成回路を持てば回路規模が増大すること, 拡大鍵の生成は事前処理が可能なこと等より, LSI の経済化を優先して MPU 等で拡大鍵の生成を行いそれを LSI に書き込む方法を採用した. しかしこの方法では暗号鍵が LSI 外部に存在しているため不正に読みだされる可能性がある. そこで本 LSI では暗号鍵の不正読みだし, 改竄の防止策として, マスター鍵の書き込みは専用の装置または特定の人によってのみ行うものとする考えに基づき以下の機能を設けた.

①LSI 内部での拡大鍵生成処理(2.2 参照).

Development of an Encryption Processor using FEAL-N cipher
Hiroyuki Matsumoto　Ikuro Oyaizu
NTT Human Interface Laboratories

②マスター鍵(Km)と2組のセッション鍵(Ks)の値を保持するバッテリバックアップ機能.
③マスター鍵で暗号化されたデータをLSI内部で復号し，セッション鍵として使用する機能.
④マスター鍵変更時はLSIの"マスター鍵書き込み許可"端子がオンの時のみ可能となる機能.

2.4 ITU-T勧告H.233に準拠したテレビ電話/会議用暗号機能

テレビ電話/会議用暗号機能(送信側)の概要を図1に示す. 多重化された映像,音声,データのAV信号をOFB-8モードで暗号化する. OFBモードは伝送路でビットエラーが発生しても他のビットに誤りが波及しないので圧縮された映像データ等の伝送には適しているが，バーストエラー等で同期はずれが生じた場合自己復帰できない. そこで1マルチフレーム(160m秒)毎に暗号演算を初期化して同期の再確立を行う. このとき前のマルチフレームのECSチャネルで送信した初期値を次のマルチフレームの暗号演算の初期値として演算を開始する.しかしLSI外部からのマルチフレーム切り替え指示で瞬時に暗号演算を初期化して暗号化を開始するのは不可能である. そこで本LSIは現在乱数を発生しているパス(図1の実線)の空きを利用して，事前に新たな初期値で乱数を発生しシフトレジスタに蓄積して待機する(図1の波線). マルチフレームの切り替え指示があれば稼働パスと待機パスを切り替へ，以後動作を継続する機能を設けた. なお受信側も同様な機能を設け全二重動作が可能である.

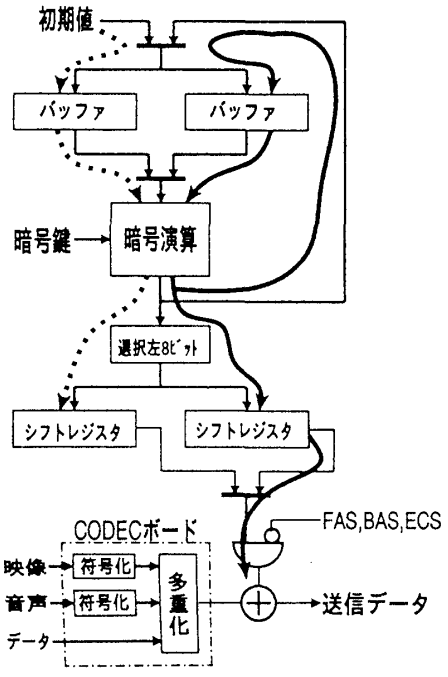

図1　テレビ電話/会議用暗号機能(送信側)

3. 本LSI諸元

表1に本LSIの諸元を示す.

4. まとめ

本LSIは,FEAL-8より暗号強度の強いFEAL-32を採用し,7.6Mバイト/秒の性能を実現した.またファイルデータの暗号処理だけでなく,高速なシリアルデータの実時間処理にも適用でき,今後のセキュリティサービスの発展に寄与するものと期待される.

参考文献

(1)小柳津,松本,石井: ISDNマルチメディア通信用ワンチップ暗号プロセッサ,情処学会論文誌,Vol.33, No.2, pp.204-211, 1992.
(2)ITU-T Recommendation H.233: Confidentiality System for Audiovisual Services.
(3) 宮口,栗原,太田,森田: FEAL暗号の拡張,NTT R&D, 39, No.10, pp.1439-1450, 1990.
(4)Biham, Shamir: Differential Cryptanalysis of Feal and N-Hash, EUROCRYPT91, 1991.

表1　LSIの諸元

項目＼LSI			本LSI	従来LSI (NLC5009)
暗号アルゴリズム			FEAL-32, FEAL-8	FEAL-8
暗号利用モード			ECB,CBC, CFB-8,OFB-8	同左
性能(注)	パラレル	ECB,CBC	7.6MB/s (16.7MB/s)	(10MB/s)
		CFB-8,OFB-8	0.95MB/s (3MB/s)	(1.8MB/s)
	シリアル	ストリーム [CFB-8,OFB-8]	3.8Mb/s×2 (12.1Mb/s×2)	(5Mb/s×2)
		TV電話/会議 [OFB-8]	2.4Mb/s×2 (7.6Mb/s×2)	
暗号鍵の拡大処理			有り	無し
バッテリバックアップ機能			有り	無し
最大システムクロック			33MHz	20MHz
電源電圧			5V/3.3V	5V
ピン数、パッケージ			80ピンQFP	60ピンQFP

(注) ( ) 内はFEAL-8の場合