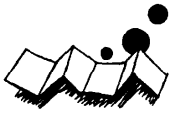
解　説



暗号処理ハードウェア†

秋山良太††　八星禮剛††

1. はじめに

暗号処理専用ハードウェアはプログラムなどのソフトウェアに比べ，情報を保護するしくみが物理的にも論理的にも明確で，しかも高速処理が実現できることから，コンピュータ・通信システムに装置として組込まれ使われている．

本稿では各種暗号処理専用ハードウェアの処理技術で特に通信システム分野で使う暗号処理技術に的をしぼり，このなかで処理技術の要となる各種暗号 LSI や製品化されている各種暗号装置のしくみ及び装置全体に必要な安全対策基準など実践的観点に立った暗号処理技術について解説を行う．

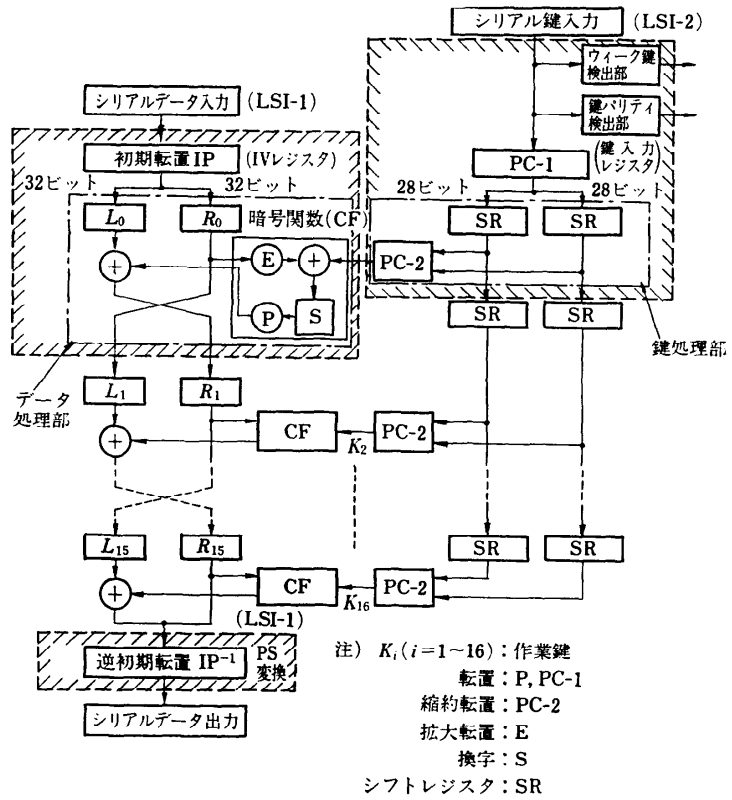


図-1　DES-LSI のしくみ

† Trends on the Hardware Technologies for Data Encryption by Ryota AKIYAMA and Reigo YATSUBOSHI (Digital Network System Laboratory, Fujitsu Laboratories Limited).

†† (株)富士通研究所ディジタル網研究部

2. 暗号処理の LSI

この章では，商用暗号通信に使用される代表的な暗号化アルゴリズムである，DES[1]，RSA 法[2)-4)]，及び DH 法[5),6)] などのハードウェアによる処理技術，LSI 化したハードウェア構成，及び LSI の諸性能について述べる．

2.1 DES アルゴリズムの LSI

(a) CMOS タイプの LSI

富士通で開発した LSI は，CMOS マスタスライス技術を使って，DES アルゴリズムを2チップで構成している（**図-1** 参照）．2チップの1つはデータかく乱部 (LSI-1)，他は鍵かく乱部 (LSI-2) に各々使っている．LSI-1 の構成はシリアル入力データをパラレルに変換する IV レジスタ，データ処理部，パラレル出力をシリアルに変換するレジスタ (PS 変換) 及び制御部などである．このうちデータ処理部の初段部分（図-1 の1点鎖線部）のみが LSI 化され，残り 15 段の処理は初段部分を 15 回繰返し処理することにより達成している．各転置処理部については結線入換によって行っている．一方 LSI-2 の構成は，ウィーク鍵検出部（鍵かく乱の効果のない4組の鍵の除去），鍵パリティ検出部（鍵 64 ビット中8ビットのパリティをチェック），及び鍵データ処理部などである．鍵データ処理部もデータかく乱部と同様，初段部分（図-1 の1点鎖線部）が LSI 化され，残り 15 段の処理は初段部分を繰返し処理している．各転置処理部については，結線入換によって行っている．**図-2** は LSI-1 の各操作内容に対する処理時間とゲート数を示している．LSI-1 のデータ処理部の 16 段処理に要する遅延量は 4 μ 秒以下，また LSI-1，2 総合したゲート数は約 6000 ゲートとなっている．消費電力は 4 MHz 基本クロック動作で LSI-1 は 61 mW，LSI-2 は 23 mW である．インタフェースは両チップとも TTL コンパチブルとなっている．

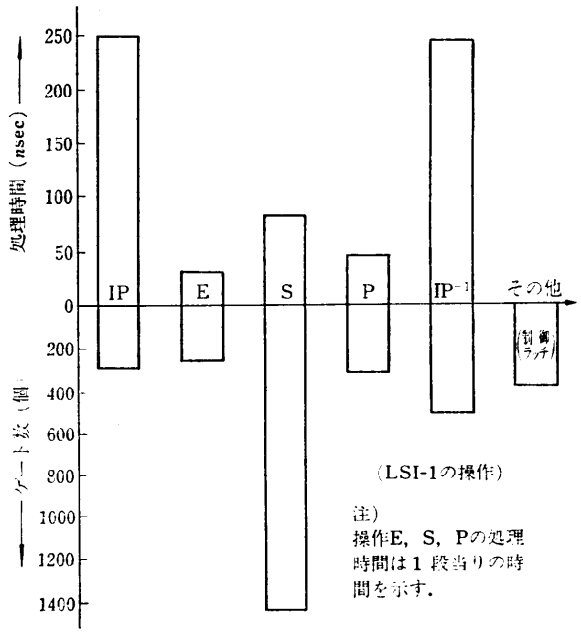


図-2 DES-LSI の処理性能

(b) バイポーラタイプの LSI

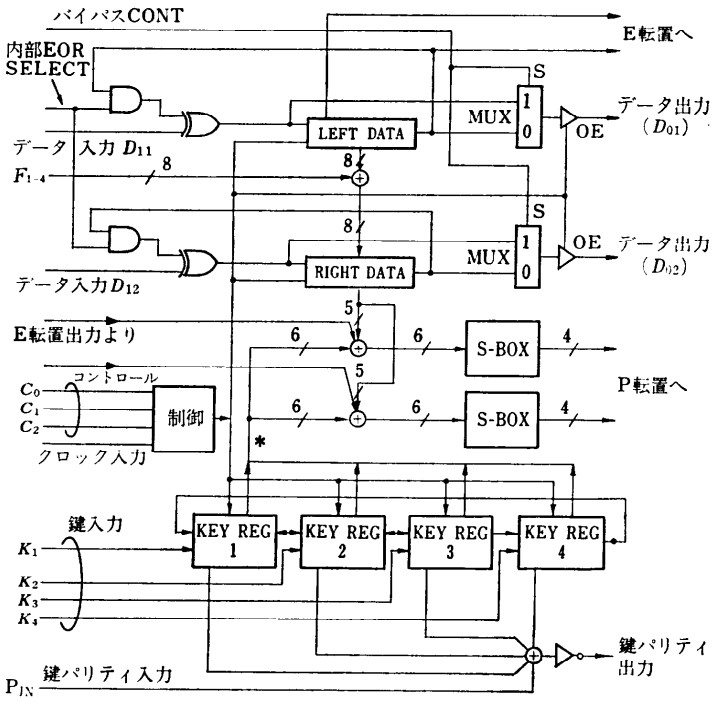


図-3 9414 DES-LSI

米国 Fairchild 社では，I^3L (Isoplanar Integration Injection Logic) 技術を使って，DES アルゴリズムを4チップで構成している．各チップは図-1 に示した LSI-1, 2 を各各縦割りに4等分したデータかく乱部と鍵かく乱部を組合せて1チップとして実現している．**図-3** は4チップのうちの1つを示す．各チップは初めの8クロックで16ビットの鍵データ（2ビットはパリティ）を KEY レジスタにセットし，次の8クロックで16ビットの平文データを LEFT/RIGHT データレジスタにセットした後，次の 16 クロックで DES 演算を実行する．処理出力は最後の8クロックで行われている (**図-4** 参照)．

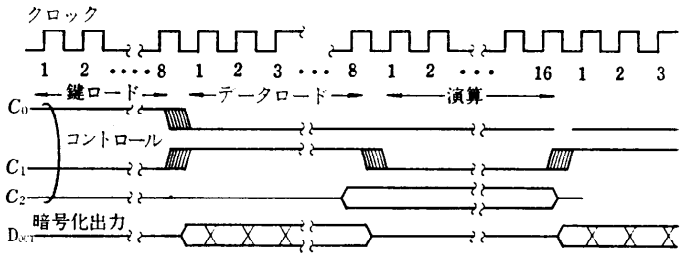


図-4 DES 演算処理タイミング

このチップのE，P転置は各チップ間の結線で行うので，各チップにはE，P転置部が存在しない．また IP 転置はシリアルな入力データをパラレルに変換して各チップに入力するだけで達成している．9414 は発表されて4年以上たち，現在これを上回る性能の LSI が登場しているが，9414 独特の縦割処理構造は今後の高速 DES-LSI を作る上で参考となろう．

（c） 各種の DES-LSI

DES-LSI を製造しているメーカは米国ですでに 10 社以上ある．**表-1** は市販されている代表的な製品例を示している．DES-LSI に関しては μ-CPU などと異なり，セカンドソース製品がないことが特徴となっている．

2.2 その他の暗号処理 LSI

2.2.1 RSA 法 LSI

電電公社横須賀電気通信研究所では公開鍵暗号系の

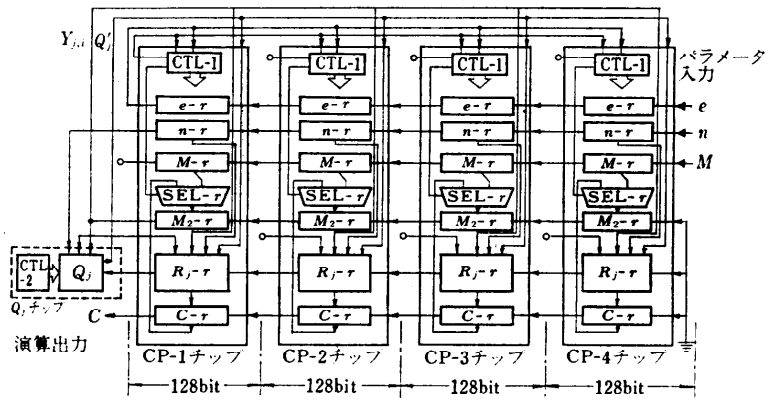


図-5 RSA 法の LSI 化

表-1 各種 DES-LSI

品 名	メーカ（国籍）	仕様 スループット (max)	暗号化モード	チップ数 (LSI 技術)	備 考
Am 9518	AMD (Advanced Micro Devices) (米国)	14 Mbps	ECB, CBC, CFB (プログラム制御)	1 (NMOS)	○ Amz 8000, Amz 8085 ○ インタフェース可能
MC6859	Motorola (米国)	400 kbps	ECB	1 (NMOS)	○ 消費電力 1 W ○ MC6800 ファミリ
9414	Fairchild (米国)	13.3 Mbps	ECB	4 (I^3L)	○ 消費電力 1W/chip
WD-2001	Western Digital (米国)	1.95 Mbps	ECB	1 (NMOS)	8080A インタフェース可能

表-2 RSA-LSI の比較

項目＼方式	Rivest の LSI	宮口の LSI
LSI 技術（ゲート長）	NMOS（2 μm ルール）	CMOS（1 μm ルール）
ハードウェア規模	40 K Tr	LOGIC 部 145K Tr/chip×4 chip ROM 部 2^{11}×9ビット
スループット	1.2 kbps	50 kbps

1種である RSA 法[2]の LSI 化を検討している．RSA 法の基本アルゴリズムは $C \equiv M^e \pmod{n}$（但し，$n = p \times q$；p, q は素数，e；公開鍵，M；メッセージ，C；メッセージ M の暗号化出力）なるベキ乗剰余計算である．同研究所では，ベキ乗計算と剰余計算とを同時に実行できる計算手法を考案し，この計算手法に基づいた高速の LSI を目ざしている．なお，計算手法については文献等[3]を参照されたい．

同研究所の LSI は大規模となるため，4チップに LSI を分割し，512ビットのベキ乗剰余計算を可能にしている（**図-5** 参照）．分割した各 LSI は規則性に優れ，現在の IC 技術なら十分実現できることが報告されている．**表-2** は MIT の Rivest が設計した LSI[4]と新計算手法を用いた LSI の比較である．

2.2.2 DH 法 LSI

米国 HP 社では公開鍵配送に使う DH 法[5]の LSI を実現した[6]．DH 法の基本アルゴリズムは RSA 法同様に，ベキ乗剰余計算である．HP 社の計算方法は，整数計算によらず，多項式計算方法を使ってベキ乗剰余計算を行っている．この方法を使えば，ハードウェアはシフトレジスタと排他的論理和などのロジックで構成でき，LSI 実現が容易である．**図-6** は多項式表現による $A \times B \pmod{p(\alpha)}$ の計算アルゴリズムである．計算手順は，LFSR (Linear Feed back Shift Register) 及びアキュムレータに A をセットしておき，B の第1ビット (LSB) の値に従って，ゲート回路の開閉を行う．この場合，B の値が1のとき，アキュムレータの内容と LFSR の内容と EOR（排他的論理和）して結果をアキュムレータに格納して LFSR を1ビットシフトする．但し，B が0のときはそのまま LFSR を1ビットシフトする．この基本操作を B の第2ビット以降についても繰返し処理して，B の最終ビットまで行うと，A×B の計算が終了する．この基本アルゴリズムを使ってベキ乗剰余計算を行うと，最大 $m \times (m-1)$ のシフト操作が必要となる．（但し m は LFSR の段数）実際のハードウェア構成は（**図-7** 参照）127段の LFSR（図-7 では C の部分）と 127 個の EOR 及び 127 個のレジスタ（図-7 では B の部分）及びゲート制御部である．ハードウェアの特性については **表-3** に示す．

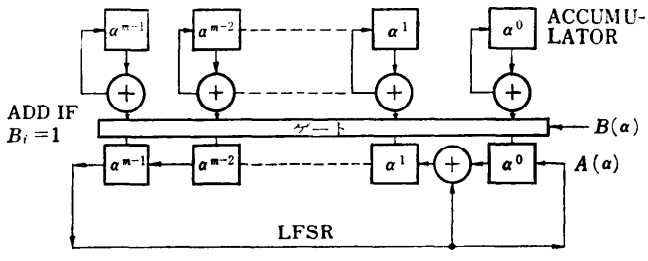


図-6 多項式乗除算器のモデル

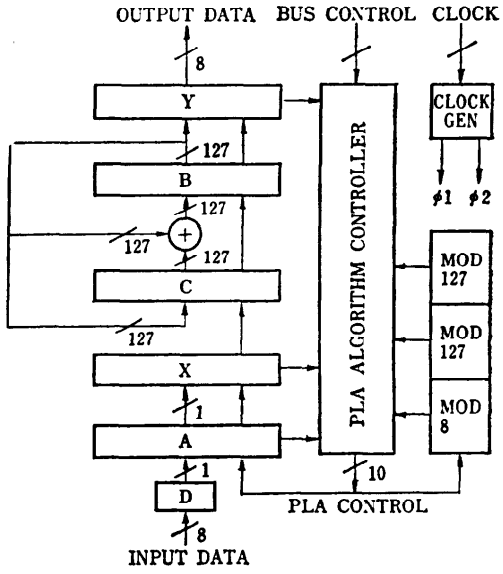


図-7 多項式乗除算器 LSI 構成

表-3 DH 法専用 LSI の特性（n=127ビット）

項　目	仕　様
LSI 技術	NMOS（3 μm ルール）
ハードウェア規模	12 K Tr
基本クロック	4 MHz
チップサイズ	5 mm×5 mm
消費電力	500 mW
スループット	10 kbps（推定）

この LSI は当初見込んでいた安全性より低くなることが最近の研究報告[7]で明らかになったが，鍵の長さ 127 ビット

を例えば 1000 ビット以上にすれば，十分な安全性が得られる[8]．

3. 暗号装置

この章ではいままで述べた暗号処理 LSI を使った製品紹介を中心に暗号装置としてのハードウェア技術について解説する．なお，**表-6** には，現在市販している各種暗号装置の一覧表を示しておいた．今後の暗号システム構築の判断材料の一つとして参考にしていただきたい．

3.1 DES 方式

現在米国では，十数社のメーカが DES アルゴリズムを使った暗号装置を製品化している．製品の多くは端末とモデムとの間に挿入して使うデスクトップタイプである．製品の特長としては，

1) 各社独自に開発した DES-LSI を組込んでいる．

2) 処理遅延が少なく，暗号同期の簡単な CFB (Cipher Feed Back) モードが使われている．

3) 鍵管理方式は IBM 社の2キー方式か又は，paradyne 社，Racal-Milgo社の2階層鍵管理方式[9]を使っている．

4) NBS の安全対策基準 FED-STD 1027[10] に基づく設計．

5) あらゆる通信方式に対し装置を適用させるためのオプションが準備されている．

などがある．また，デスクトップ以外の製品として端末の中に組込んで使う暗号ボードもある．ボード上には DES-LSI の他に暗号化モードを制御する周辺装置が実装されているほか，μ-CPU とのバスインタフェースができるようになっている．

3.2 ハイブリッド暗号装置

3.2.1 DH-DES 方式

富士通で開発した回線暗号装置 FACOM 2151 A は DH 法を使ってセッション鍵（情報暗号化用の使い捨て鍵）の配送を行い，DES を使って情報の暗号化を行うハイブリッド方式である．原理は（**図-8** 参照）通信当事者間の公開鍵 Y_A, Y_B を信頼できるシステム管理者を通じて交換し，通信当事者が各々管理している秘密鍵 S_A, S_B と Y_A, Y_B とから共通なマスタ鍵 Z を作り出している．次にこの鍵 Z と両通信者の装置で発生した乱数 α, β を使って再度 DH 法による鍵配送を行い，両装置で共通のセッション鍵 z を作り，z を DES の鍵としている．富士通の DH 法計算は，米国 HP 社と異なり，整数計算によって行っている．安全性は多項式計算法に比べ高いが，LSI を実現する場合，RSA 法 LSI と同様にハードウェアが大規模となることが予想される．このため同社では LSI の代りに DSP (Digital Signal Processor：専用プロセッサ) を使ってベキ乗剰余計算を行っている．**表-4** には

表-6 各種暗号装置

	装置名	メーカ（国籍）	仕様			
			基本アルゴリズム	使用できる鍵総数（鍵の長さ）	伝送速度	使用回線
DES方式	IBM 3845	IBM（米）	DES	7×10^{16} (56 ビット)	0.3 kbps～19.2 kbps	○ p-p ○ p-mp ○ 交換回線
	Datacryptor II	Racal-Milgo（米）	DES +RSA (option)	〃	0.3 kbps～9.6 kbps	○ p-p ○ p-mp ○ 交換回線
	LC 76 DES	LINKABIT（米）	DES	〃	1.2 kbps～6.5 Mbps	
	FACOM 2151 A	富士通（日）	DES +PKDS	〃	0.3 kbps～19.2 kbps	○ p-p ○ p-mp ○ 交換回線
非DES方式	HC-550	CRYPTO AG（スイス）	3段フォワードシフトレジスタ	10^{28} (アルファベット20字)	100 bps (max)	
	DS-138	datotek（米）	非線形多重レジスタ擬似ランダム発生器使用 bit by bit 方式	10^{12}	19.2 kbps (max)	
	COMCIPHER	日本電気（日）	非線形フィードバックレジスタ	7×10^{16}	2 Mbps (max)	○ p-p ○ p-mp ○ 交換回線

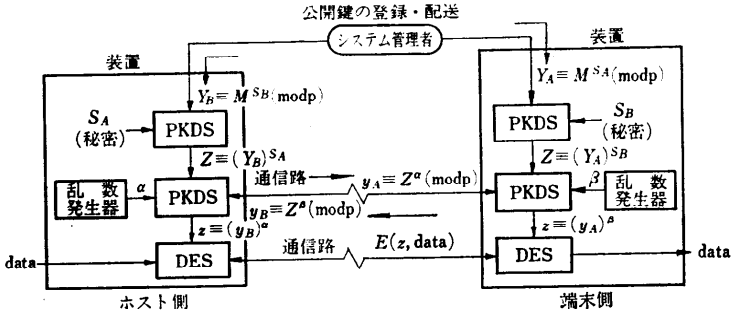


図-8　DH 法-DES ハイブリッド方式

表-4　DSP-2 (MB 8763) の特性

項　目	仕　様
パッケージ	64 ピン RIT
LSI 技術，電源	CMOS，5 V 単一
消費電力	約 150 mW
基本クロック	16.8 MHz
処理速度	5.6M命令/秒(マシンサイクル 180 ns)

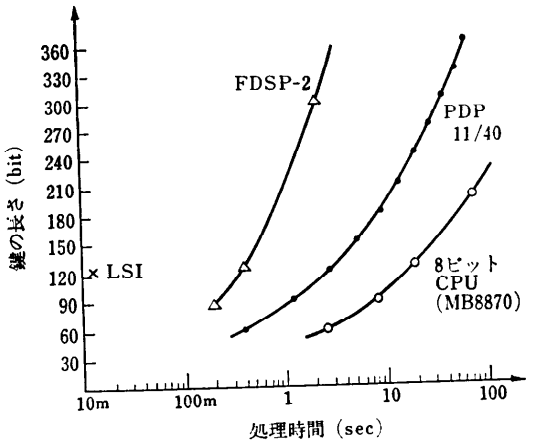


図-10　ベキ乗剰余計算処理時間

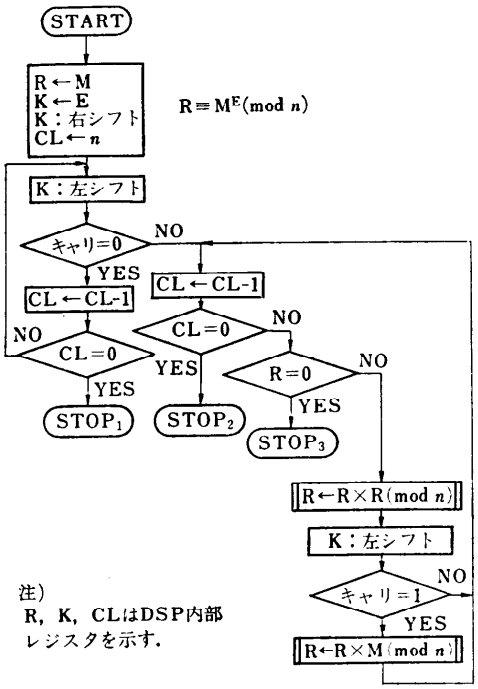


図-9　専用プロセッサによるベキ乗剰余計算フロー

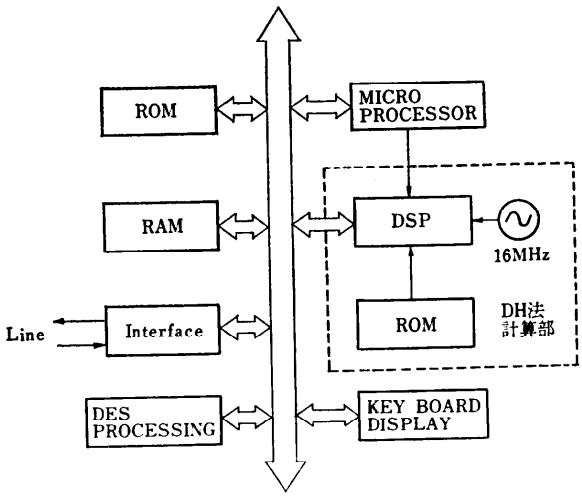


図-11　FACOM 2151 A 回線暗号装置構成

DSP の特性を，また**図-9** にベキ乗剰余計算処理フローを示す．処理方法は秘密鍵Eを DSP 内部レジスタKにセットし，レジスタの値に従って上位ビットから下位ビットまで以下の式に従って計算を行っている．

Eレジスタの内容が0のとき(1)式を計算

$$R_{i+1} \equiv (R_i)^2 \pmod{n} \qquad (1)$$

Eレジスタの内容が1のとき(2)式を計算

$$R_{i+1} \equiv R_i \times M \pmod{n} \qquad (2)$$

但し，$i=1, 2, \cdots,$ CL 1，$R_1 = M$ (M は法 n の原始根)である．**図-10** はベキ乗剰余計算処理時間について，汎用プロセッサ，専用プロセッサ及び DH 法 LSI との比較を示している．DH 法は鍵配送だけに用いるアルゴリズムであるので，数秒程度の処理遅延があっても，通信システムに影響はない．**図-11** 及び **表-5** は装置の構成及び仕様を示す．構成は破線で囲んだ DH 法計算部，DES-LSI と制御回路を実装した DES 演算部，外部から鍵パラメータ及び運用方法を設定するキーボード，装置の状態を表示するディスプレイ，標準的な回線インタフェースを備えたインタフェース部，及び制御用8ビット μ-CPU からできている．**図-12** は暗号装置の外観である．

3.2.2 RSA-DES 方式

米国 Siemens 社ではワークステーションに組込むための暗号ボード，CP (Cryptoprocessor) を開発している[11]．この CP は蓄積又は伝送するメッセージの

表-5 FACOM 2151A の仕様

項目		仕様
暗号アルゴリズム		DES
鍵管理		DH法
装置	通信方式	○同期，調歩同期 ○半2重，全2重
	インタフェース	CCITT V. 24, V. 28
	速度	○同 期……19.2 kbps (max) ○非同期…… 9.6 kbps (max)
	使用回線	○ポイントーポイント ○マルチドロップ ○交換
	保護機能	鍵前の2重化
	RAS 機能	○自己診断テスト ○ループバック ○バイパス
	電源 消費電力	○AC100V ○10W
	サイズ	65(H)×210(W)×300(D)mm

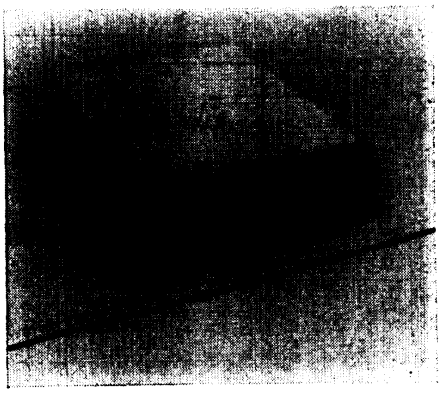


図-12 FACOM 2151 A の外観

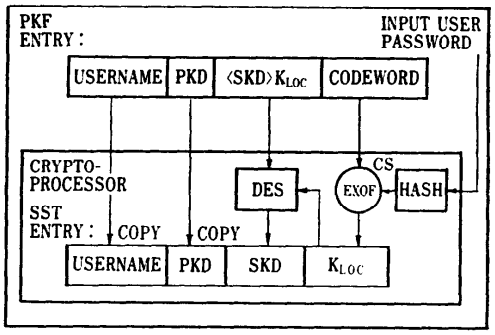


図-13 CP の機能

暗号化に用いている．暗号方式は，RSA 法を使って鍵の管理を行い，DES を使ってメッセージの暗号化を行うハイブリッド方式である．CP の機能は（**図-13** 参照），相手通信者にメッセージを送るとき，中央機関（信頼できる鍵管理機関）に登録してある相手側の一連の情報（公開鍵 PKD，暗号化復号鍵〈SKD〉KLoc，コードワード CW）を中央機関より通信路を通して送ってもらい，これらの情報とメッセージ送信者のパスワード PW 等を CP にセットすることにより，鍵の配送及びメッセージの暗号化さらにはディジタル署名まで実現することができる．この CP 機能のなかに HASH 関数（**図-14** 参照）を使った鍵生成法がある．HASH 関数は原理的にはユーザのパスワードを56ビットのブロックに区切り，DES の鍵部へ入力していく．ここで1ブロック入力するごとに DES を1回フィードバックする．最終ブロックが入力されたときの最終 DES 出力をパスワードから作り出された64ビットの鍵としている．文意のとれる長いパスワードでもすべて HASH 関数によって 64 ビットの

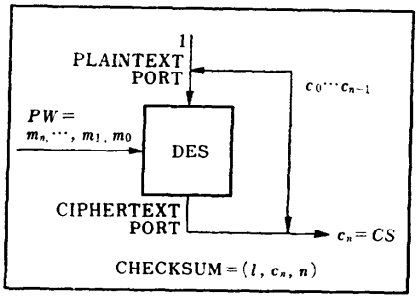


図-14 DES を使った圧縮変換器 (HASH 関数)

領域へ圧縮変換することができる.

CP のハードウェア構成は (図-15 参照) RSA 法の計算, 鍵の管理及び信号制御を 16 ビットの CPU (Intel 8086) を使って処理している. DES 演算処理には Western Digital 社の DES-LSI (WD 2001) が使われている. なお, 図の破線部は RSA 法計算をハードウェアで実現するときのハードウェア組込み位置を示している.

4. 暗号装置の安全対策基準

暗号装置を設計する場合, 装置の物理的安全性及び保全性を考慮した設計が必要となる. 装置の安全性・保全性に関する国際的な基準は現在定められていないが, 目安として NBS (National Bureau of Standard : 米国商務省標準局) が定めた基準 (Federal Standard 1027) がある. この基準は商用暗号装置全般に対し適用するものでなく, 米国政府部門や機関で使用する DES 暗号装置に対し適用される. この基準の骨子は,

1) 操作ミスによる平文伝送の防止.

2) 鍵 (Key Variable) が装置にセットされた状態で盗難されしかも不正使用されることへの防止.

3) セットした鍵 (Key Variable) のコピー又は変更の防止.

4) 鍵設定が簡単で, 政府使用の標準化鍵の設定機構が準備されていること.

5) 危機的状況下のもとでは暗号化出力を停止すると共に装置は警報を鳴らすこと.

が装置に要求される.

これら骨子のうち例えば 2) について実現してみる. 装置には, ユーザ, 保守者等が使用する物理的鍵を使って装置を開いても, あらかじめメモリに蓄積されたユーザの鍵データは消去されないこと. このことは外部電源が供給されない場合も同様に消去されないこと. しかし物理的な鍵なしに不正に装置を開くなら, メモリにセットされた鍵はオール 1 又はオール 0 のコードによってオーバライトされ, もとの鍵は自動消去されることなどの対策がとられている. この他装置の筐体も, 外側から分解されないようにネジなしの機構設計が施されている. この他の骨子については掲載する余白がないので, FED-STD 1027 のマニュアルを参考にしていただきたい.

5. むすび

各種暗号 LSI 及び暗号装置などのしくみを中心に, 最近のハードウェアによる暗号化技術について解説を行った.

本稿では DES と代表的な公開鍵暗号方式について述べたが, 実用化されている DES と検討段階にある

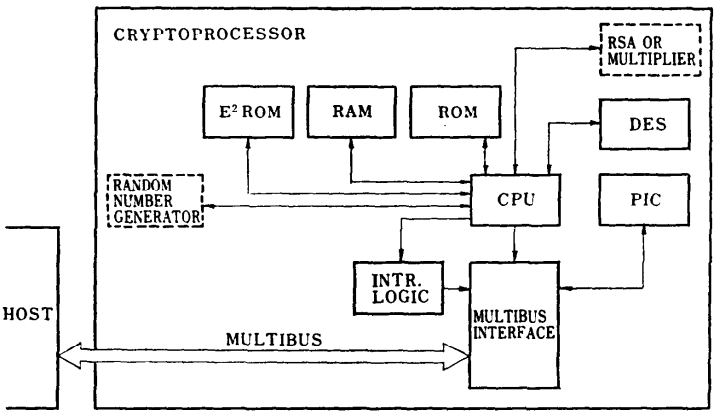


図-15 CP のハードウェア構成

公開鍵暗号方式との技術的開きを今後どのように補っていくかが問題と思われる．また本稿ではふれなかったが，データの暗号化のみならず，音声や画像などの信号波形をそのまま暗号化するアナログスクランブル処理ハードウェア技術もあり，今後の技術動向に期待したい．

参 考 文 献

1) Data Encryption Standard, FIPS PUB 46, NBS (Jan. 1977).
2) Rivest, R., Shamir, A. and Adleman, L.: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, MIT Lab. for Computer Science Technical Report, TM-82 (Apr. 1977).
3) 宮口：RSA 公開鍵暗号の高速計算法と暗号 LSI の構成，情報処理学会論文誌，Vol. 24, No. 6 (Nov. 1983).
4) Rivest, R. L.: A Descryption of a Single Chip Implementation of the RSA Public-Key Cryptosystems, NTC, pp. 49・2・1～49・2・5 (1980).
5) Diffie, W. and Hellman, M. E.: New directions in Cryptography, IE³ Trans. Inform Theory, Vol. IT-22, pp. 644-654 (Nov. 1976).
6) Yiu, K. and Peterson, K.: A Single-chip Implementation of the Discrete Exponential Public Key Distribution System, IE³ GLOBECOM 83, Vol. 1, No. 6 (Dec. 1982).
7) Blake, I., Fuji-Hara, R., Mallin, R. and S. Vanstone: Finite Field Techniques for Shift Registers with Applications to Ranging Problems and Cryptography, Final Report 106-16-02 Dept. of Communication.
8) Odlyzko, A.M.: Discrete Logarithm Algorithms, Bell Lab. Internal Technical Memorandum (May 4, 1983).
9) Orceyre, M. J. and Heller, R. M.: An Approach to Secure Voice Communication Based on the Data Encryption Standard, IE³ Communications Society Magazine, Vol. 16, No. 6 (Nov. 1978).
10) Federal Standard 1027, NBS (Apr. 14, 1982).
11) Müller-Schloer, C. and Wagner, N. R.: The Implementation of Cryptography-based Secure Office System, AFIPS Conf. Proc., Vol. 51, NCC, pp. 487-492 (1982).

（昭和59年3月7日受付）