Vol. 30 No. 11　　情　報　処　理　　Nov. 1989

解　説

2. DSP の応用例

2.5 DSP の秘匿への応用†

岡本栄司††　中村勝洋††

1. まえがき

パソコン通信や UNIX ネットなどの情報ネットワークが全世界的に広まりつつある現在，電子ウィルスやハッカーを始めとするコンピュータ犯罪も地球的規模で多発している．このため，情報秘匿や情報認証などの保護技術が情報ネットワークに適用されるようになってきた．特に国際間の情報のやり取りでは法律などの社会法制度よりも技術に依存せざるを得ない部分が多い．

情報保護技術をインプリメントするには，専用 LSI などのハードウェアによる方法と，マイクロプロセッサや DSP を用いてソフトウェア的に処理する方法がある．従来は処理速度の点からハードウェアが中心であった．特に DES (Data Encryption Standard)[1] などのハードウェア向き暗号アルゴリズムは今後も専用 LSI が主流になると思われる．しかし，高速処理可能な DSP が開発されて，整数演算を利用した暗号アルゴリズムや DFT 処理に基づくスクランブラなどが容易に実現できるようになった．たとえば剰余演算を利用する RSA 公開鍵暗号[2] では専用 LSI が市販されているが，性能的にそれほど見劣りもしないものが DSP で実現可能である．さらに，セキュリティチップは今のところ大量に売れる製品ではないので，なかなか専用 LSI を起こしにくく，可能なら DSP やマイコンで済ましたいという考えもある．そのほか一度専用 LSI を起こすとなかなかバージョンアップができないのに比べ，DSP は短いサイクルでより高性能なチップが開発される点も見逃せない．

以上示したように DSP は情報セキュリティの分野に非常に有用である．そこで本文では DSP を用いたセキュリティ装置／システムについて解説を行う．具体的には，簡単な秘匿技術の解説を行い，ディジタル暗号では RSA 公開鍵暗号系と DES 慣用暗号系を，アナログ秘話については音声秘話装置について説明を行う．

2. 秘匿技術—ディジタル暗号とアナログ秘話—

秘匿技術には，隠語などのように情報の存在そのものをも秘密にする技術から，存在は隠さず意味のみを秘密にする暗号まで多種多様な技術がある．ここではもっともよく用いられる暗号を主に扱う．なお，対象がアナログ情報のときは特にアナログ秘話という．

暗号系を図-1 に示す（アナログ秘話を含む）．送信側で平文 (plaintext) が暗号化鍵をパラメータとして暗号文 (ciphertext) に“暗号化”され，受信側で当該暗号文が対応する復号化鍵をパラメータとしてもとの平文に“復号化”される．このときの暗号化鍵と復号化鍵が同じ場合もしくは，一方から他方が容易に導ける場合を慣用暗号（対称暗号），異なっていて暗号化鍵から復号化鍵を容易に求められない場合を公開鍵暗号（非対称暗号）という．図-2 にさらに詳細な暗号の分類と代表例を示す．慣用暗号ではアメリカの標準である DES (Data Encryption Standard) が有名であ

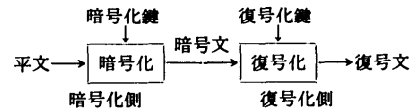


図-1　暗号系

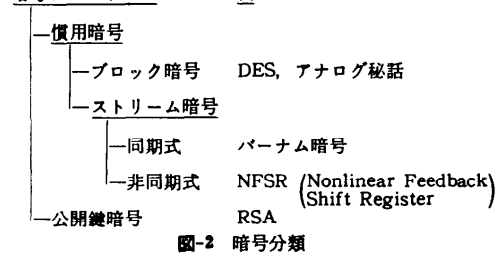


図-2　暗号分類

† The Application of DSP to Cryptography by Eiji OKAMOTO and Katsuhiro NAKAMURA (Information Basic Research Laboratory, C&C Information Technology Research Laboratories, NEC Corporation).

†† 日本電気(株) C&C 情報研究所

り，公開鍵暗号では Rivest, Shamir, Adleman による RSA 暗号が有名である．なお現在用いられているアナログ秘話装置はすべて慣用暗号である．アナログ秘話は厳しい帯域制限があるため，使える手法が限られる．通常なんらかの意味で信号の入れ換えを行うことにより秘話性を出している．

3. DSP を用いたディジタル暗号

ディジタル暗号に DSP を用いた例では RSA 公開鍵暗号と鍵配送のための DH 公開鍵配送方式 (Diffie と Hellman による)[3] が知られている．この両者は演算がほとんど同じなので，ここでは前者だけ扱う．また，慣用暗号では汎用マイクロプロセッサを用いた DES 暗号の例があるので，広い意味で DSP に含めてそれにも言及する．

3.1 公開鍵暗号—RSA 暗号—の実現

公開鍵暗号の概念は 1976 年に Diffie と Hellman によって発表された[3] が，実用的な例は 1978 年に Rivest, Shamir および Adleman が最初に考案した[2]．現在 3 人の頭文字をとって，RSA 暗号と呼ばれる．

RSA 暗号の概略を図-3 に示す．図において整数の組 (E, N) が暗号化鍵で (D, N) が復号化鍵である．平文は整数とみなしたとき N 未満になるようにブロック化される．平文ブロック M は

$$C=M^E \pmod N$$

により暗号化されて暗号文ブロック C になる．暗号文は同じような次の変換によりもとの平文に戻る．

$$M=C^D \pmod N$$

鍵は次のように作る．二つの素数 P と Q を生成して

$$N=P\cdot Q$$

とし，E と D を

$$E\cdot D \pmod{(P-1)\cdot(Q-1)}=1$$

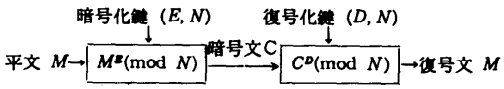


図-3 RSA 暗号

となるように選ぶ．P と Q はたとえばおのおの 256 ビット長程度の整数である．この大きさの素数を見いだすのは容易であり，E と D を見いだすのもユークリッド互除法を用いれば容易である．ところが，E と N を与えられたときに上式を満たす D を見いだすには，N の素因数分解を要するので，困難である．大きな整数に対する素因数分解は今でも困難な問題である．すなわち，RSA 暗号は素数生成の容易さと素因数分解の困難さのギャップを利用した暗号である．

RSA 暗号の主要な演算は

$$Y=X^E \pmod N$$

である．ここで X, E および N は大きな整数なので，演算処理量は多く，今までに多くのベキ乗剰余アルゴリズムが提案されている．ここでは DSP 処理に適した演算アルゴリズムを述べる[4]．

ベキ指数 E の 2 進数展開を

$$E=\sum_i e_i 2^i$$

とすると，

$$Y=\prod_{(e_i=1)} X^{2^i} \pmod N$$

となる．これを図示したのが図-4 である．図中，乗算は，乗数および被乗数を小ブロックに分割して DSP でブロックの乗算を行うことにより，実施できる．また，剰余演算は次のように行う．剰余演算の入力を V とすると，V は N^2 程度の大きさであり，このときの剰余演算

$$W=V \pmod N$$

には剰余テーブルを用いる．剰余テーブルとは N とある整数 q (通常 q は 2 のベキ乗) に対する

$$q^i \pmod N \quad i=n, n+1, \cdots$$

のことで，あらかじめ計算してメモリに格納しておく．ここで，N を q 進数展開したときの桁数を n とした．この剰余テーブルを用いて剰余演算を行う．

剰余アルゴリズム

S_1: V を q 進数展開する

$$V=\sum_i V_i\cdot q^i$$

S_2: n 以上の i に対して $V_i=0$ なら終了

S_3: q^i を $q^i \pmod N$ に置き換えて S_1 へ

$$V=\sum_{i<n} V_i\cdot q^i + \sum_{i\geq n} V_i\cdot q^i \pmod N$$

この計算結果は必ずしも $V<N$ を満足しないが，このまま図-4 を実行し

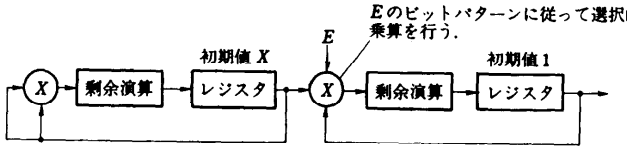


図-4 ベキ乗剰余演算構成図

てよい．最後に $X^E \pmod N$ を出力するときのみ，N 未満になるように引算を1，2回行えばよい．

以上のベキ乗剰余演算を表-1で示される32ビットDSP（μ PD 77230, NEC）を用いて行ったところ，512ビットの平文を暗号化するのに約0.63秒要した．ここに，N は512ビット長で剰余テーブル作成時間0.02秒を含む．0.63秒という時間はデータ暗号には長いが，暗号化鍵の配送やディジタル署名と呼ばれる認証機構には十分である．ちなみにマイクロコンピュータでは数秒かかるのが現状である．

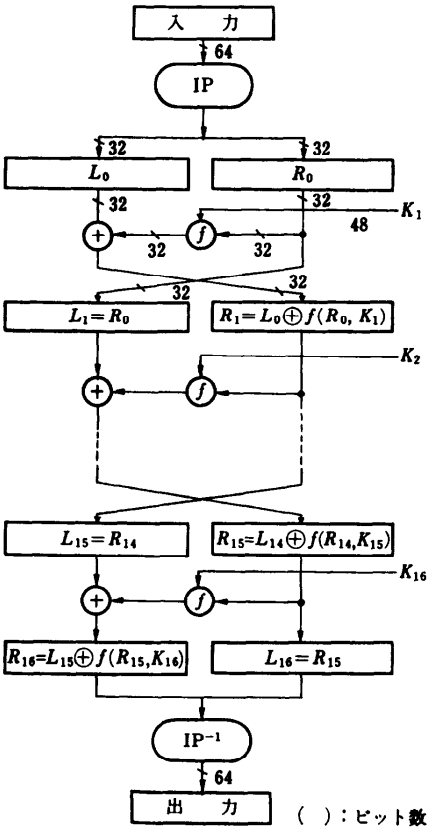
表-1　DSP（μPD 77230）の仕様パラメータ

クロック	13 MHz
乗　算	150ナノ秒 32ビット浮動小数または 24ビット固定小数
ALU	55ビット
インストラクション ROM	2K語×32ビット
データ　ROM	1K語×32ビット
RAM	2×512語×32ビット

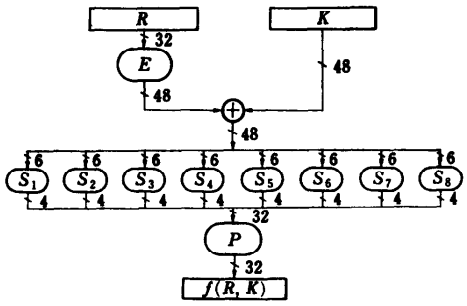
DSPは基本演算となる乗算が高速なのでベキ乗剰余以外の逆数 $1/X \pmod N$，乗除算 $X/Y \pmod N$ なども，ユークリッド互除法を用いれば，容易に計算できる．

3.2　慣用暗号—DES 暗号—の実現

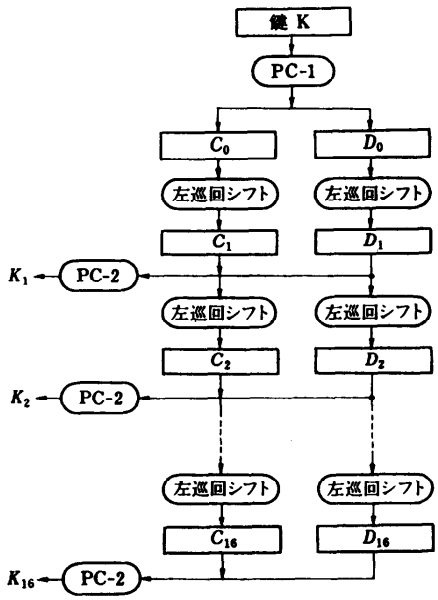
DSPを用いた慣用暗号の例は少ない．これは，DSPが乗算を高速化したLSIであるため，ビット処理が中心の慣用暗号に用いても，マイクロコンピュー



（a）　暗号化変換



（b）　$f(R,K)$ の計算



（c）　鍵系列生成

図-5　DES 暗号の構成

表-2 DSP (TMS 32010) による DES の実現[9]

機 能	メモリ (Kワード)	時間 (ミリ秒)
鍵生成／管理	0.6	0.6
暗号化処理	1.1	1.5 (42 Kb/s)

タを用いた場合に比較して大幅な高速化が得られないためである．ここでは DSP による DES の実現例のほかに，DSP の範囲をきわめて広く解釈して，マイクロコンピュータを用いた DES についても述べる．

DES は米国が 1977 年に制定したデータ暗号標準[1]で，米国だけでなく広く使われている．DES アルゴリズムは，図-5 に示すように，入力 64 ビットに対して簡単な初期転置変換 IP を施した後，転置と換字を組み合わせた変換を 16 回繰り返し，最後に初期転置の逆転置を施して出力 64 ビットを得る変換アルゴリズムである．鍵はパリティ 8 ビットを含めて 64 ビットである．図中，E, P, PC-1 および PC-2 は転置，$S_1, \cdots, S_8$ は換字を行う S ボックスである．DES の非線形性はこの S ボックスに依存している．

DES を DSP で実現した例として文献 5) がある．16 ビット DSP (TMS 32010, TI) を用いて，42.5 Kb/s を達成している．ちなみに後述のマイクロコンピュータでは 11.5 Kb/s であり，RSA 暗号などに比べると差はあまり大きくない．表-2 に，暗号化処理と鍵生成・管理に要するメモリと処理時間を示す．処理速度 42.5 Kb/s は DSP の能力を 100% 使ったときの値であり，たとえば 16 Kb/s なら 37% 程度である．このとき，残りを 16 Kb/s の SBC (Sub-Band Coding) 音声符号化処理などに割り当てることができる[5]．

DES をマイクロコンピュータで実行している例もいくつかあるが[6]，これらは汎用の 1 チップマイクロコンピュータあるいはその汎用周辺チップの ROM 部を DES アルゴリズムが実行できるように組み立てている．この方法は，DSP を用いる場合と同様，開発を終えた LSI の ROM 部にプログラムを書き込むだけでよいので，新たに専用の LSI を起こす場合に比較して，開発工数が少なくて済む．しかし暗号化の速度は小さい (4.8−11.5 Kb/s)．現在は専用 LSI が市販されているので，この形で使われることは少ない．

図-6 に ROM が CPU と別チップになっている例を示す (S 6894, AMI)[7]．ROM (S 6846) に DES プログラムが入っており，また I/O とタイマも含まれている．マイクロプロセッサ (S 6802) は，ROM のプログラムにしたがって，暗号化／復号化処理を行う．処理速度は 11.5 Kb/s である．

1 チップに納めた例を図-7 に示す (TMS 9940, TI)[8]．内蔵の 2K バイト ROM および 128 バイト RAM などを用いて 4.8 Kb/s の暗号化処理速度を得

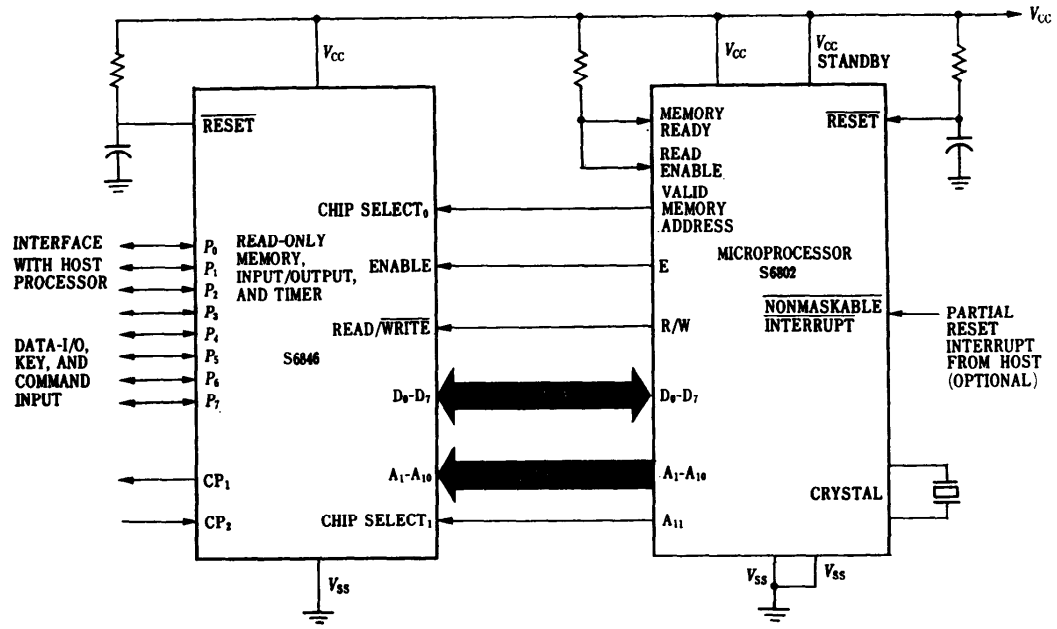


図-6 2 チップ構成 DES (マイクロプロセッサタイプ)
(Electronics/January 17, 1980 p. 136)

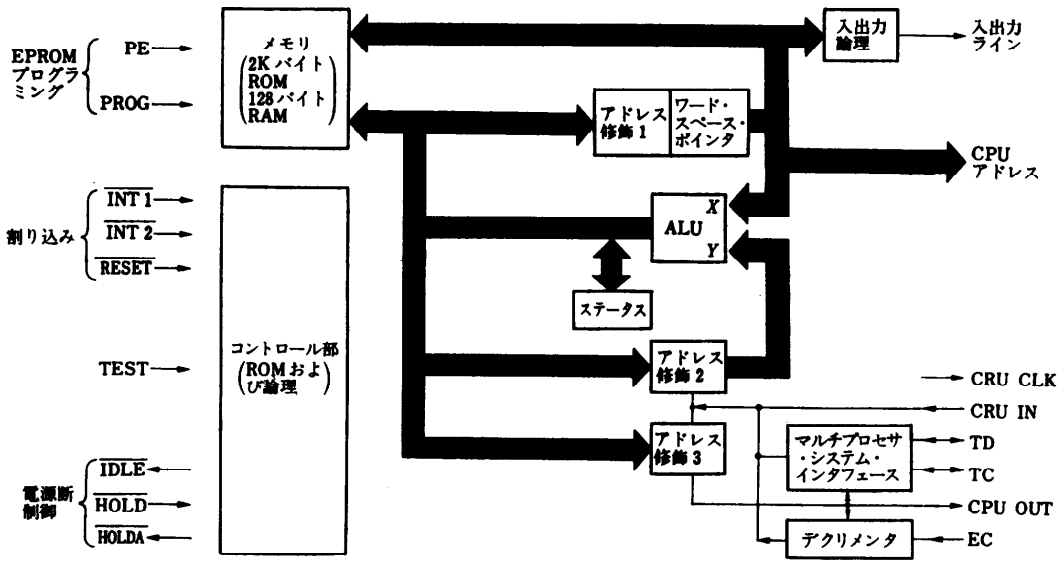


図-7 1チップ DES (マイクロコンピュータ)
(日経エレクトロニクス 1979.10.29 p. 174-175)

ている.

以上のほかに, パーソナルコンピュータのソフトウェアの例は多い.

4. DSP を用いたアナログ秘話

アナログ秘話に DSP を用いた例は多い. これらは秘話の処理自身のほか, 音声処理やコントロール情報の生成／処理にも DSP を使えるからである.

アナログ秘話には秘話化しても制限帯域を守らなくてはならないという条件がある. したがって, 使える秘話アルゴリズムが限られる.

アナログ秘話アルゴリズムには図-8 に示すように, 大きく分けて二種類ある. 一つは音声を符号化してビット系列として通常のディジタル暗号を用いる方式で, 他方はアナログ音声信号のまま暗号化する方式である.

符号化するタイプのアナログ秘話 (図-9) は, データ暗号を使えるので秘匿性が高いが, 帯域制限があるので最適な符号化方式を選ぶ必要がある. 前記文献 5) は 16 ビット DSP を音声符号化と DES 暗号化に用いている例であり, 表-3 におのおのの処理にかかるロード (%) を示す. DES と音声符号化のロード和が 100% 以下から 1 チップで実現可能であることがわかる. たとえば, 前述したように 16 Kb/s の DES と

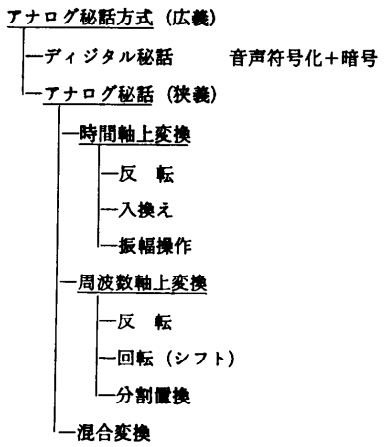


図-8 アナログ秘話方式

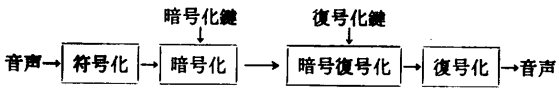


図-9 ディジタル秘話

SBC が可能である. 32 ビット DSP に DES をインプリメントした報告はないが, おそらく 16 Kb/s あるいは 9.6 Kb/s のマルチパルス音声符号化[9] と DES を構成できるものと思われる. 音声符号化については, 本特集号の「DSP のコーデックへの応用」「DSP の音声処理への応用」を参照していただきたい.

表-3 ディジタル秘話における DSP のローディング[9]

(a) 符号化

符号化法	ビットレート (Kb/s)	符号化ローディング (%)	復号化ローディング (%)
LPC	2.4	43	44
RELP	9.6	91	79
APC	16	87	35
SBC	16	38	38
ADPCM	32	52	48
ADPCM-CCITT	32	91	95

(b) DES

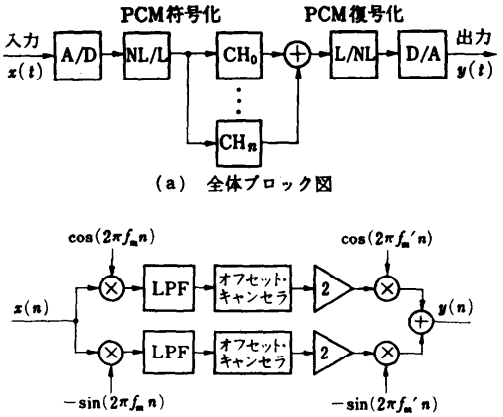
ビットレート (Kb/s)	ローディング (%)
42.8	100
32	75
16	37
9.6	22
2.4	6

注) LPC =Linear Predictive Coding, 10th-order model
RELP =Residual Excited Linear Predictive Vocoder
APC =Adaptive Predictive Coding
SBC =Sub-Band Coding
ADPCM=Adaptive Differential PCM (CCITT algorithm, not bit-by-bit compatible)
ADPCM-CCITT=CCITT ADPCM, bit-by-bit compatible

狭義のアナログ秘話には，図-8 に示すように，時間軸上変換方式と周波数軸上変換方式，およびその混合方式がある．いずれも線形変換暗号なので暗号強度の点からは低いといわざるを得ない．

時間軸変換方式は帯域が広がるので簡単な変換しか行えないので，あまり用いられない．現在，主流は周波数軸上変換方式である．その中で，比較的秘匿性が高いのは周波数帯域分割置換方式であり，フィルタバンク法，周波数シフト法[10]，FFT 変換法[11]，T-MUX 法[12]，非同期法[13]などがある．

DSP を利用した例として，図-10 に周波数シフト法を示す．サンプリングした信号をディジタル乗算器で周波数＝0を中心とする帯域に周波数シフトし，ディジタルローパスフィルタ (LPF) で分割帯域の1ブロックを抜き出す．この帯域を再び乗算器により中心周波数を移動する．この移動により分割された帯域が置換され，秘匿が達成される．この際の暗号化鍵は置換の方法，すなわち，入れ換え方である．この方法の特徴は，やや専門的になるが，乗算やフィルタが中心なので DSP で容易に実現できること，同一特性



(a) 全体ブロック図

(b) CHm 処理ブロック図

図-10 周波数シフト型アナログ秘話

の低次 LPF を使えること，急峻な特性が要求される LPF の出力に適応形のオフセット・キャンセラを備えることにより短い演算語長で十分な S/N 比が得られることなどである．したがって，小型化，低価格化が図れる．

一般にアナログ秘話は強度が低いので，暗号化鍵などの秘話パラメータを時間的に変える必要がある．

5. あとがき

DSP の秘匿技術への応用例を述べた．ここでは特に DES 暗号，RSA 暗号およびアナログ秘話を中心に述べたが，これ以外にも各機関，企業で独自の暗号に用いることも可能である．さらに，今後 DSP の発展にしたがって，暗号／秘匿だけでなく誤り訂正符号やデータ圧縮などへの応用も広がるものと考えられる．

末筆ながら，資料・情報を提供していただいた日本電気(株)伊藤泰雄氏，小沢一範氏，田中和恵氏に深謝する．

参考文献

1) Data Encryption Standard, FIPS Pub. 46, National Bureau of Standards (1977).
2) Rivest, R. L., Shamir, A. and Adleman, L.: A Method for Obtaining Digital Signatures and Public Key Cryptosystems, Commun,. ACM, 21, 2, pp. 121-126 (1978).
3) Diffie, W. and Hellman, M. E.: New Directions in Cryptography, IEEE Trans., IT-22, pp. 644-655 (1976).
4) 田中，岡本：シグナルプロセッサを用いた RSA

暗号系の実現，昭和63年電子情報通信学会春季全国大会，A-298.
5) Papamichalis, P. E. and Reimer, J. B.: Speech Encryption Using the DES on a TMS 32010, GLOBECOM '85, pp. 27. 2. 1-27. 2. 5.
6) 中村，岡本：通信のセキュリティ・信頼性とVLSI，通信と VLSI 小特集，電子通信学会誌，69, 2, pp. 136-140 (1986).
7) Humphrey, T. and Toth, F.L.: Two-chip Data-encryption Unit Supports Multi-key Systems, Electronics, January 17, pp. 136-139 (1980).
8) バジンスキ：暗号アルゴリズムの実行もできる1チップ・マイクロコンピュータ，日経エレクトロニクス，pp. 173-186 (1979. 10. 29).
9) Ozawa, K., Ono S. and Araseki, T.: A Study on Pulse Search Algorithms for Multipulse Excited Speech Coder Realization, IEEE J. SAC-4, 1 (1986).
10) 山根，尾知：秘話装置，公開特許公報昭 61-262330, pp. 191-197.
11) 松永，大川，桜井，古賀：FFT を用いた全二重アナログ秘話装置とその基本動作，電子情報通信学会論文誌，J 72-A, 4, pp. 692-702 (1989).
12) 東，鳥居，長谷部，秋山：トランスマルチプレクサを応用した秘話技術と性能評価，1988 年暗号と情報セキュリティシンポジウム.
13) Lee, L.: A Speech Security System Not Requiring Synchronization, IEEE Commun., Mag., 23, 7, pp. 42-55 (1985).

(平成元年9月5日受付)