マルチメディア通信と分散処理　50－2
（１９９１．５．１６）

パソコン間暗号通信方式の一検討

小柳津育郎　松本 博幸　石井 晋司
ＮＴＴ情報通信処理研究所

先に開発したマルチメディア通信用暗号ＬＳＩを搭載し，音声の実時間暗号処理と並行してメモリ上のデータをＩｎ／Ｏｕｔ命令で暗号処理できる簡単なハードウェア構成のパソコン用暗号処理ボードを試作した．この報告は，試作した暗号処理ボードの構成と各種通信メディアへの適用性，処理性能について述べる．また，本暗号処理ボードをオーディオグラフィック通信会議システムの手書き入力信号のＩＳＤＮ通信に適用し，暗号処理時間がシステムに及ぼす影響を評価した結果，リアルタイム通信の暗号処理に適用できることを確認した．

A STUDY OF ENCRYPTION METHOD ON PERSONAL COMPUTER COMMUNICATION

Ikuro Oyaizu Hiroyuki Matsumoto Shinji Ishii
NTT Communications and Information Processing Laboratories
1-2356, Take, Yokosuka-shi, Kanagawa-ken, 238-03 Japan

An Encryption PC plug-in expansion board has been developed that can encrypt stored file data and handle the real-time encryption of voice data in parallel. The encryption board have been simply implemented with only 7 chips by using the formerly developed single chip FEAL encryption processor. In this paper the design of the encryption board and evaluation of its performance are discussed. And its application to ISDN audio-graphics teleconferencing system is also reported.

1．はじめに

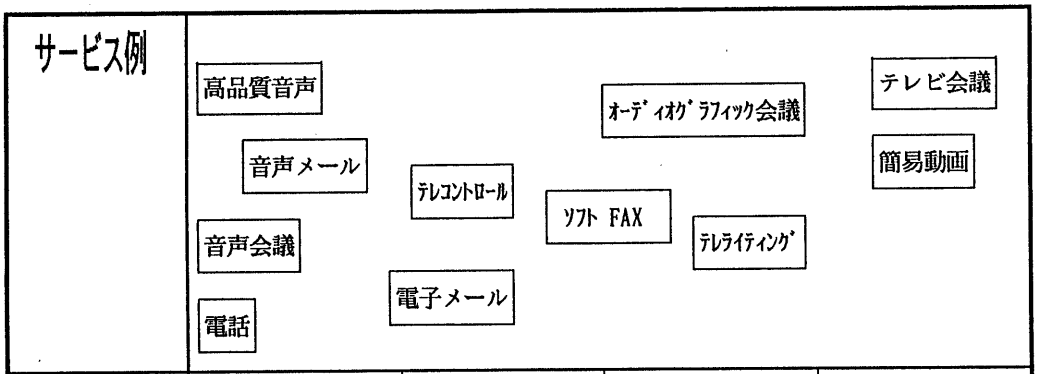
ＩＳＤＮの普及とパソコンの高性能化にともない，オフィス間のコミュニケーション支援の手段としてパソコンをベースとした各種マルチメディアデータを扱う通信システムが開発されている[1][2]．パソコン間通信がオフィス間のコミュニケーション支援ツールとして多用されるにともない，企業の秘密や個人のプライバシー保護に対する要請が高まってきている．

このような要請に応えるため，われわれはＦＥＡＬ－８暗号アルゴリズムを用いて，メモリ上に格納されたデータの暗号化，復号だけでなく，音声ＣＯＤＥＣ等のビットシリアルデータをリアルタイムで暗号化，復号ができる低価格なマルチメディア通信用暗号ＬＳＩ（以下暗号ＬＳＩと記す）を開発した[3]．上記暗号ＬＳＩを搭載し，音声の実時間暗号処理と並行してメモリ上のデータをＩｎ／Ｏｕｔ命令で暗号処理する簡単なハードウェア構成のパソコン用暗号処理ボード（以下暗号処理ボード）を試作した．本報告では，試作した暗号処理ボードの構成と暗号処理ボードをパソコンに収容し各種通信メディアへの適用性ならびに処理性能を実測した結果を述べる．また，暗号処理ボードをオーディオグラフィック通信会議システム[4]に適用し，暗号処理時間が手書き入力信号処理時間に及ぼす影響を評価した結果，リアルタイム通信の暗号処理に適用できることを確認した．

2．パソコンの暗号通信方式

２．１ パソコン間通信のメディア

ＩＳＤＮにより可能となる高度通信サービス例[5]からパソコンを利用するサービスに暗号処理を適用するという立場から見た通信メディアの分類結果を図－１に示す．暗号化したデータを人が知覚によって観察することがあるかどうか，およびリアルタイム性に対する要求度の観点から通信メディアを分類した．



通信メディア	音声	テキスト	静止画	動画
知　覚	聴覚	－	視覚	視覚
リアルタイム性	必要	－	－	必要

図－１　パソコン間通信サービスとメディアの特徴（例）

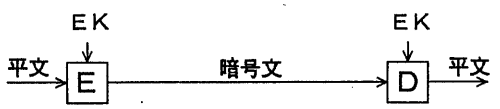
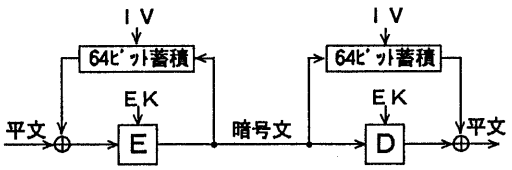
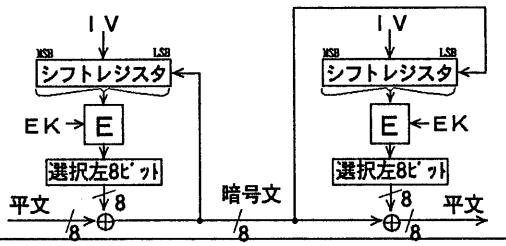
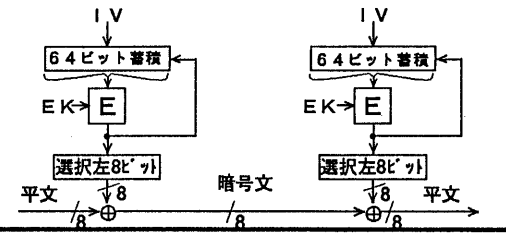
２．２ マルチメディア通信用暗号ＬＳＩの概要

暗号ＬＳＩはＩＳＯ，ＪＩＳで標準化されている暗号利用モードに準拠している．表－１に暗号ＬＳＩがサポートしている暗号利用モードの特徴とブロック図を示す．

また暗号ＬＳＩは，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，CODECインタフェース，DMA転送機能等の周辺回路を内蔵しており，ＦＡＸ，ディジタル電話機等の各種ＩＳＤＮ通信機器に容易に組み込めるように設計した．

表－2に暗号ＬＳＩの端子とその機能を示す．

表－1　各暗号利用モードの特徴とブロック図

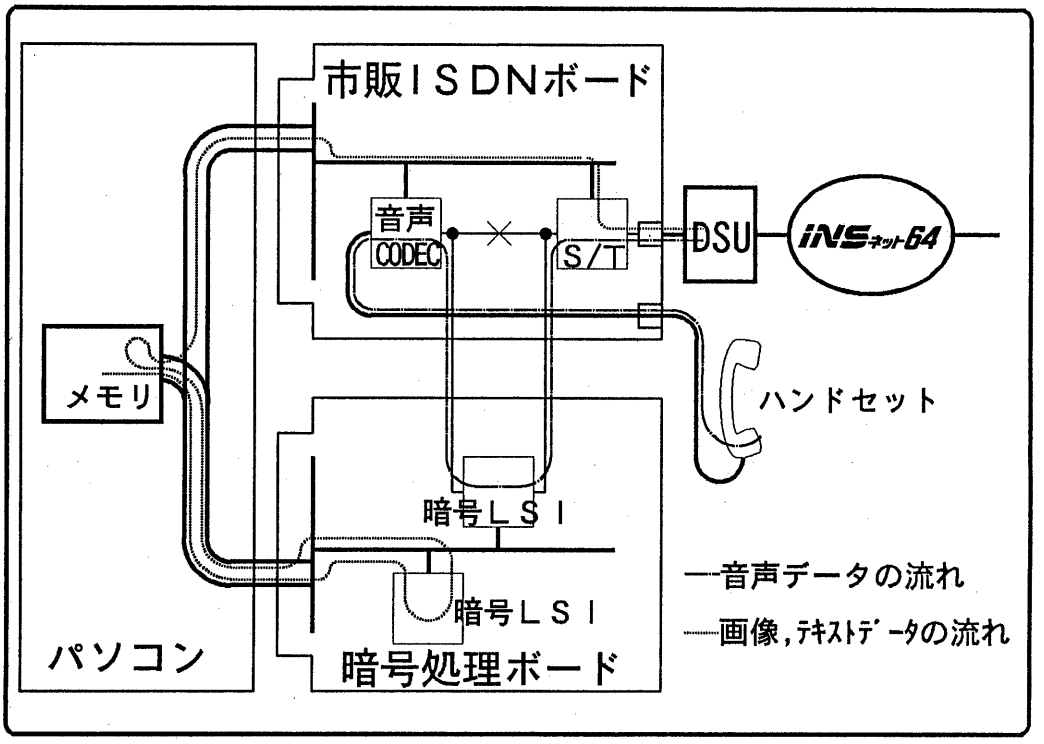
ﾓｰﾄﾞ	特　　徴	ブロック図
ECB	・1ﾌﾞﾛｯｸ(64ﾋﾞｯﾄ)単位の暗号． ・同一内容のﾌﾞﾛｯｸは同一の暗号鍵に対して同一の暗号文となるため暗号強度は弱い． ・他のモードで使用する暗号鍵やIVを送信するのに適する．	ＥＣＢ（Electronic Codebook）モード 
CBC	・1ﾌﾞﾛｯｸ(64ﾋﾞｯﾄ)単位の暗号． ・暗号処理結果と次の入力ﾃﾞｰﾀと演算し，さらに，暗号処理するので暗号強度は強く，演算効率がよい． ・一つの暗号文ﾌﾞﾛｯｸ内のﾋﾞｯﾄ誤りはそのﾌﾞﾛｯｸおよび次のﾌﾞﾛｯｸの復号結果に影響を及ぼす． ・ﾌｧｲﾙの伝送，蓄積時に適する．	ＣＢＣ（Cipher Block Chaining）モード 
CFB -8	・8ﾋﾞｯﾄ単位の暗号． ・1文字(8ﾋﾞｯﾄ)単位の暗号で，伝送路の暗号文1字のﾋﾞｯﾄ誤りはその文字および以降の8文字の復号結果に影響を及ぼす． ・データ通信に適する． ・暗号強度はOFBﾓｰﾄﾞより強い．	ＣＦＢ（Cipher Feedback）－8モード 
OFB -8	・8ﾋﾞｯﾄ単位の暗号． ・暗号化と復号は同一ロジックである． ・1文字(8ﾋﾞｯﾄ)単位の暗号で，伝送路上の暗号文1字のﾋﾞｯﾄ誤りはその文字の復号結果にのみ影響を及ぼす． ・音声，映像等の伝送に適する．	ＯＦＢ（Output Feedback）－8モード 

（EK:暗号鍵を拡張した拡張鍵　IV:初期値）

２．３ 暗号処理ボードの構成

暗号処理ボードの仕様は，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時間より短いことを生かし，汎用ポートへ暗号化，復号データをＩｎ／Ｏｕｔ命令を繰り返し実行することにより，暗号処理ができるようにした．このような仕様を採用した理由は，暗号化，復号処理を行う暗号処理ボードを制御するプログラムをＣ言語等の高級言語で容易に作成でき，かつ既存プログラ

ムへの移植性を容易にするためである．暗号処理ボードは音声用と画像およびテキスト用の計２個の暗号ＬＳＩとアドレスデコード，水晶発振子およびＰＣ９８バス等のドライブ回路の計７チップから成る簡単な構成にすることができた．各通信メディアの暗号処理データの流れおよびＩＳＤＮへの接続方式を図－２に示す．



図－２　暗号処理データの流れおよびＩＳＤＮ接続方式

音声データの流れは，ハンドセット，音声ＣＯＤＥＣを通り，暗号ＬＳＩで暗号化され，Ｓ／Ｔ点，ＤＳＵを通り，ＩＮＳネット６４に送出される（復号は逆の流れ）．画像，テキストデータはパソコン内のメモリから暗号ＬＳＩに出力され，暗号化データとなり，ふたたびメモリに格納され，つぎに市販ＩＳＤＮボードを通り，ＩＮＳネット６４に送出される（復号は逆の流れ）．

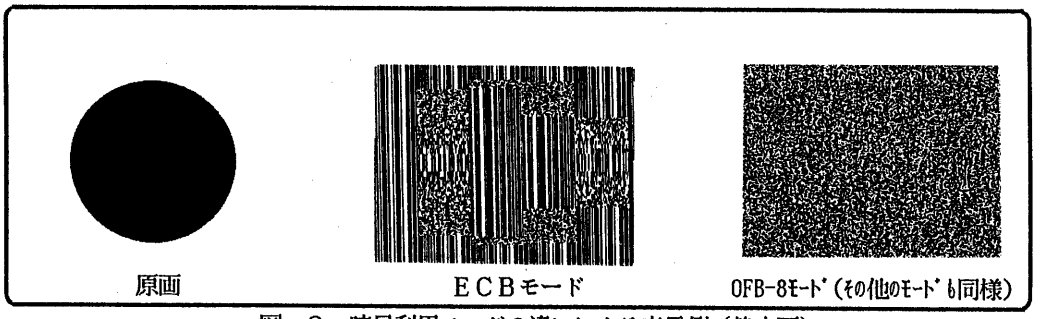
３．実験内容

３．１ 通信メディアと暗号利用モード

画像データを圧縮せずに暗号化した場合，暗号利用モードによっては，暗号化データに周期的なパターンが現れる可能性がある．そこで，静止画，疑似動画について，暗号利用モードと暗号化データの周期的なパターンとの関連性を調べた．

3.1.1 静止画（図－３参照）

暗号ＬＳＩがサポートしている４つの暗号利用モードとのすべての組み合わせ実験を行った．その結果，ＥＣＢモード（図－３中央）では，原画（図－３左）の図形の大きさと上下の対象性が容易に推測できた．



図－３　暗号利用モードの違いによる表示例（静止画）

3.1.2 疑似動画

ＥＣＢモードは静止画と同様な結果であった．

ＥＣＢモードを除き，疑似動画の暗号化結果は，送信画面単位ごとにＩＶを初期化しない場合と初期化した場合とで以下に示す違いが見られた．

送出画面単位ごとにＩＶを初期化しない場合（ＥＣＢモードは除く）の暗号化結果は，暗号化されたデータに周期性や移動物体の外形の推測は不可能であった．

送出画面単位ごとにＩＶを初期化した場合（ＥＣＢモードは除く）には，すべてのモードで物体が移動していることが容易に目視できた．ＯＦＢ－８，ＣＦＢ－８，ＣＢＣモードの順に図形の外形を推測することが容易であった．なお，ＥＣＢモードと送出画面単位ごとにＩＶを初期化した場合のＣＢＣモードの移動物体の推測の容易さは同程度であった．

３．２ 暗号処理ボードの処理性能

3.2.1 音声暗号通話

通常の通話から暗号通話へ，暗号通話から通常の通話へ移行するときにクリック音が聞こえる．暗号ＬＳＩが備えている機能であるレイヤ２以上のプロトコルを持たない音声等通信メディアのための暗号化開始および終了に同期して復号開始および終了を制御するコード（以下同期制御コード）を挿入する．上記クリック音は，上記同期制御コードの送出バイト数を３０byteに設定し，音声データに割り込ませたことによる．

アナログ電話網で使用される秘話電話装置[6]と違い，同期制御コード送信時のクリック音以外は，暗号処理を施すことによる音質の劣化は理論上はない．

暗号利用モードと暗号処理のための遅延時間（暗号化処理時間と復号処理時間との和）を表－３に示す．ただし表示した値にはＩＮＳネット６４での遅延時間は含まない．

表－３ 暗号利用モードと暗号処理の遅延時間

暗号利用ﾓｰﾄﾞ	遅延時間
ＣＦＢ－８	4ﾌﾚｰﾑ+500μs
ＯＦＢ－８	4ﾌﾚｰﾑ+500μs

ＩＮＳネット６４におけるＢチャネルの伝搬遅延時間は平均１６ｍｓと報告[7]されているので，表－３とこの値と比較して，遅延時間は，数十分の１であるから暗号機能を持っていないディジタル電話機と比較したとき，暗号処理による伝搬遅延時間に問題はないと結論づけられる．

3.2.2 テキスト転送実験

暗号処理ボードの2byteのデータ暗号化時間（復号時間も同じ）とパソコンに暗号処理ボードを収容したときの2byteのデータの転送時間を表－4に示す．暗号処理ボードのデータの暗号化時間は，暗号処理ボード（水晶発振子の周波数16MHz）に与えたデータが暗号ＬＳＩにより暗号化されるまでの時間をロジックアナライザで測定した．パソコンにおける暗号処理時間については，パソコンの汎用ポートへの入出力を，PC-9801RX(80286,12MHz)ＭＳ－Ｃ Ver.5.1を使用し2byte単位のＯｕｔ命令で暗号処理ボードにデータを送出し，その直後にＩｎ命令で暗号処理ボードからデータを読み込む動作を連続して行ったときの時間をタイマ監視を利用して測定した．

表－4　処理時間の比較

ＣＦＢ-8,ＯＦＢ-8ﾓｰﾄﾞによる測定	測定結果
暗号処理ﾎﾞｰﾄﾞ暗号化時間（2byte単位）	2.0μs(8.0Mbps)
ﾊﾟｿｺﾝによるﾃﾞｰﾀ転送時間（2byte単位）	7.3μs(2.2Mbps)

表－4の結果は，パソコンがＯｕｔ命令直後にＩｎ命令を行ったときには，暗号処理ボードの暗号化処理は終了しており，パソコンが暗号処理ボードからのデータ引き取り要求を監視する必要がないことを示している．なお，ＥＣＢ，ＣＢＣモードは8byte単位に暗号処理を行うため，暗号化時間は表－4に示した暗号化時間より短い．

３．３ システムへの適用例

ケーススタディとして，本暗号処理ボードをオーディオグラフィック通信会議システムの手書き入力信号のＩＳＤＮ通信に適用し，暗号処理時間がシステムに及ぼす影響を評価した．

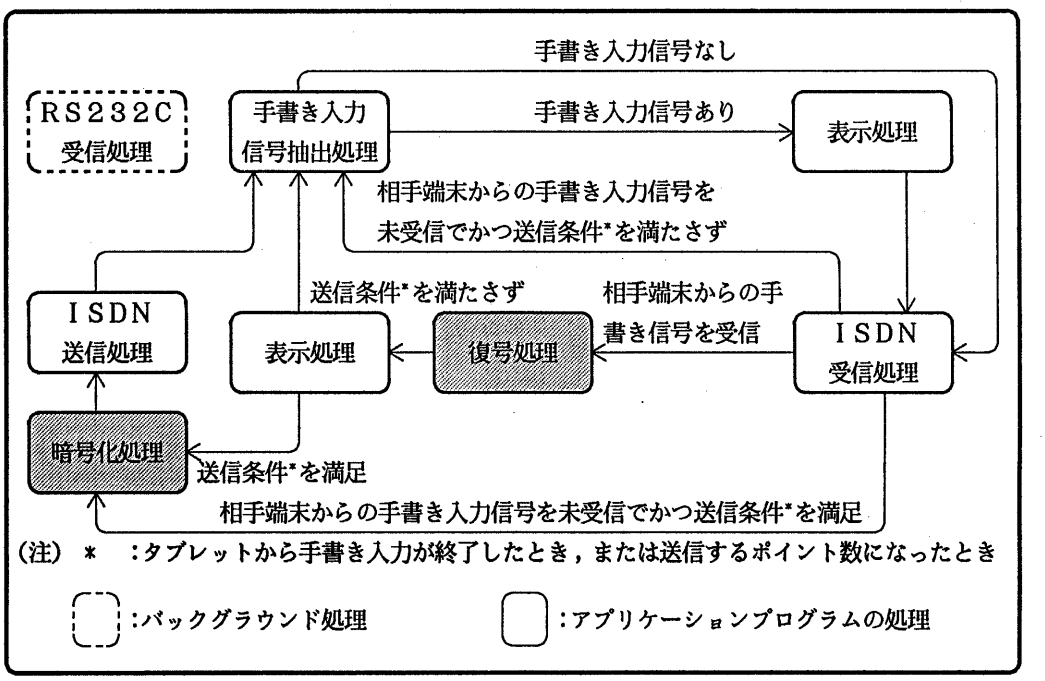
オーディオグラフィック通信会議システムの手書き入力信号処理に暗号化，復号処理を付加した場合の処理モデルを図－4に示す．

図－4の暗号処理付き手書き入力信号の処理モデルは，文献(4)の図1の処理モデルに暗号化処理およびに復号処理が付加されたものである．したがって，図－4の処理モデルの条件式は，文献(4)の条件式の右辺に，パソコンの暗号化，復号処理時間（7.3×α μs：αは暗号処理データのバイト長）を加えたものである．

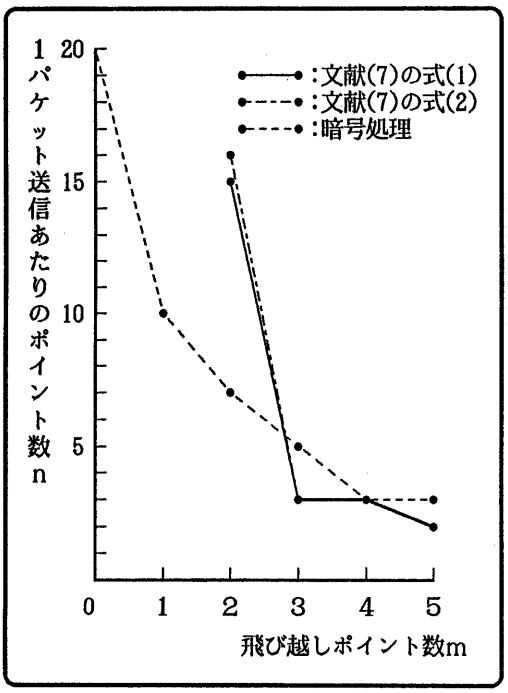
本暗号処理ボードおよび市販ＩＳＤＮ通信ボードをパーソナルコンピュータに収容し，手書き入力信号処理の飛び越しポイント数mと1パケットあたりの最大送信ポイント数ｎの関係を求めた．文献(4)のＩＳＤＮ通信ボードＡとＢについてｍとｎとの関係を求めた結果をそれぞれ図－5，図－6に示す．

図－5では，通信ボードＡでは飛び越しポイント数ｍ＝2において，1パケットあたりの送信ポイント数ｎは暗号処理を行う場合，暗号処理を行わない場合に比べて1ポイント送信ポイント数が多くなる．これは，相手端末の装置における表示レスポンスが暗号処理を行わない場合に比べてタブレットからの手書き入力の1標本化周期（7.14ｍｓ）分遅くなることを示しており，実用上問題とならない．ｍ＝3以上では，暗号処理を行う場合と行わない場合で同じであり，暗号処理の影響がないことを示している．一方通信ボードＢでは，飛び越しポイント数がどのような場合にも1パケットあたりの送信ポイント数ｎが文献(4)の式（2）の条件で決まることを示している．これは，暗号処理の影響がないことを示している．

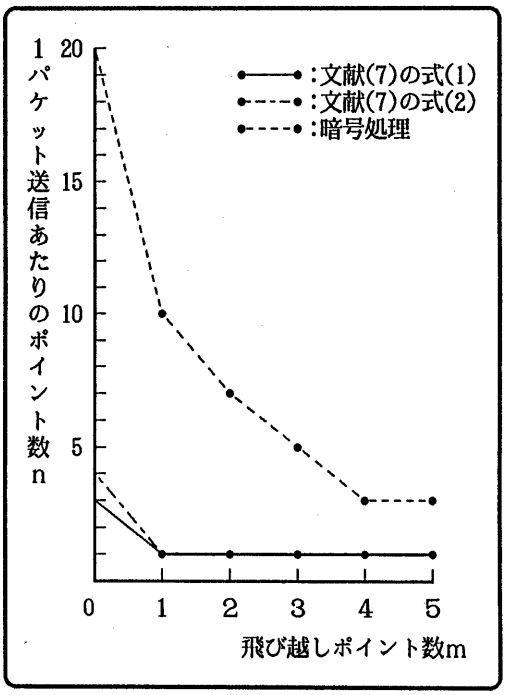
オーディオグラフィック通信会議システムに暗号処理機能を付加し，図－5，図－6のｍ，ｎの組合わせで両端末からの手書き入力を行い，実時間表示ができることを確認した．



図－4　暗号処理付き手書き入力信号の処理モデル



図－5　ISDN通信ﾎﾞｰﾄﾞAのmとnの関係



図－6　ISDN通信ﾎﾞｰﾄﾞBのmとnの関係

4. まとめ

先に開発したマルチメディア通信用暗号ＬＳＩを搭載し，音声の実時間暗号処理と並行してメモリ上のデータをＩｎ／Ｏｕｔ命令で暗号処理できる簡単なハードウェア構成のパソコン用暗号処理ボードを試作した．

試作した暗号処理ボードをパソコンに収容し，音声については市販ＩＳＤＮボードの音声ＣＯＤＥＣに接続し暗号通話ができることを確認した．

暗号処理ボードを利用したことにより，パソコン内のメモリの暗号化，復号処理については，Ｃ言語で記述した場合でも，６４kbpsを上回る２．２Mbps出力がえられたことを確認した．なお，この暗号処理ボードをオーディオグラフィク通信会議システムに収容し，リアルタイム通信への適用を確認した．

今後は，今回試作した暗号処理ボードを使用し，ＤＭＡ転送方式を採用し，さらに高速暗号処理の要求される通信メディアに対する適用領域を調べるとともに，暗号ＬＳＩを利用し，ＩＮＳネット１５００，ＩＳＤＮ－ＬＡＮ間接続への適用性の確認も行う予定である．

謝辞

日頃，ご指導・ご鞭撻頂く当研究所研究企画部松永俊雄部長，情報通信処理研究部拝原正人部長に感謝いたします．

参考文献

(1)有川,谷川,林:“パソコンを用いたマルチメディア通信会議サービス”,NTT R&D,Vol.39,No.9,PP.1265-1274,1990
(2)山口,田中,宮保,高橋:“ＩＳＤＮを利用したオーディオ・グラフィック通信会議端末の設計”,情報処理学会　マルチメディア通信と分散処理研究会,48-9,1991
(3)小柳津,松本,石井:“マルチメディア通信用暗号ＬＳＩ”,情報処理学会,マルチメディア通信と分散処理研究会,48-10,1991
(4)小柳津,山口,田中,宮保,高橋:“手書き入力信号のＩＳＤＮ通信方式について”,情報処理学会,マルチメディア通信と分散処理研究会,50-11,1991
(5)郵政省監修:“ＩＳＤＮ製品導入ガイド”,p4,1991/4
(6)中尾,田中,飯塚,渡辺,佐藤:“ディジタル秘話電話機「コンブレイクＤ」の開発”,信学会全国大会春A-295,1991
(7)飯塚,林,長谷川:“ＩＮＳネットサービスの普及拡大をねらい,品質を開示”,ＮＴＴ技術ジャーナルp.50,1990/4