マルチメディア通信と分散処理 30－8
（１９８６．７．２５）

ＩＣカードを用いた取引証明法

川村信一，神竹孝至，水谷博之
（株）東芝　総合研究所

将来、ホームバンキングやファームバンキングといった新しい形態の金融取引がさかんになると考えられる。このようなオンラインの取引システムを、従来の銀行窓口による取引と同様に安全確実なものにするためには、システムが悪意の顧客による虚偽申告を否定したり、取引に関するトラブルを解決するための取引証明機能を有することが重要である。本稿ではＩＣカードを利用することにより、この取引証明機能を実現する方法について検討する。具体的には取引の有無および内容を、後日証拠として示せるような取引記録を暗号機能の応用によって実現するものである。本文ではこのような取引記録方式をいくつか提案し、それぞれの方式の特徴と限界を明らかにする。

Prevention of Frauds and Perjuries for IC Card Transaction

Shin-ichi KAWAMURA, Takashi KAMITAKE, Hiroyuki MIZUTANI
TOSHIBA R & D Center Electronics Equipment Lab.
1,toshiba-cho,komukai,saiwai-ku,kawasaki-shi,210 japan

New electronic methods of transaction, such as a home banking and firm banking, will be introduced to improve the speed and convenience in the near future. These on-line transaction systems bring with it new security questions. An IC card is considered to be a key component solving these questions. In this paper, several methods are proposed to certificate a transaction between a customer and a bank or a service supplier and to prevent frauds and perjuries by use of IC card. The major technique to be used in these methods is cryptographic technique.

１．はじめに

ＩＣチップを磁気カード大のパッケージに封じ込めて様々な機能を実現させようというＩＣカードの実用化が間近に迫っている。ＩＣカードの利用分野としては、現在磁気カードやエンボスカードが用いられている銀行カードやクレジットカードのほかに、医療カード（カルテや健康手帳など）や従業員証、ＯＡ機器との組み合せなど多岐にわたる。当面、現在の磁気カードの次世代カードとして金融の分野での実用化が最も先行してゆくものと考えられる。一方、将来ホームバンキングやファームバンキングといった新しい形態の取引サービスの出現も予想されるが、これらが実用化されるためにはＩＣカードの使用が必須と思われる。

ＩＣカードが磁気カードと比べて優れている点は通常次のように考えられる。

（１）情報量が大きい、
（２）記憶データに対する保護、
（３）内蔵プロセッサによるセキュリティ機能。

ここで特に注目される点はセキュリティの格段の向上である。今後カード利用機会の増加に伴って多発化の可能性があるカード犯罪に対抗するためにはＩＣカードの実用化が急務であると考えられる。これは金融取引へのＩＣカードの利用検討が先行している要因の一つに挙げられよう。

本稿では上に挙げた３つの特長の内、特に（３）の内蔵プロセッサによるセキュリティ機能の向上に注目し、その応用としてＩＣカード取引における取引証明法について検討する。ここで取引証明と呼んでいるのは、悪意の顧客による取引記録の偽造を排除したり、取引に関するトラブルを解決するために、後日、取引の有無や内容を正しく示せるように取引に関する証拠を残すことを指している。取引証明を実現するための中心技術としては暗号化技術および装置のハードウェア的な安全性を利用する。取引証明を実現するに当っては（１），（２）の機能が前提となることは言うまでもないが、これについては本稿の目的からはなれるので詳しく述べない。　以下、まず２．では想定するＩＣカード・システムの概要を述べ、、３．では２．で述べたシステムでいかにして取引証明が実現可能であるか見てゆく。

２．ＩＣカードによる取引システム

ＩＣカードによる取引システムとはＩＣカードを用いた銀行システムや、クレジット・システムなどを指している。最も単純な場合として、取引を管理するセンタと、取引窓口である端末機が通信回線でスター状にむすばれたシステムが考えられる（図１）。利用者はＩＣカードを遠隔端末のリーダ・ライタに挿入してセンタに取引要求を出し、センタから所望のサービスを受ける。これが銀行システムであれば、センタ、端末機はそれぞれ銀行および現金自動支払機（ＣＤ機やＡＴＭ機）に対応することになる。本稿で取引システムという場合には、このようなオ

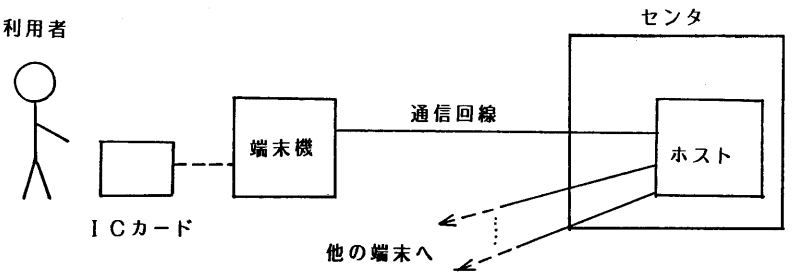

図１．ＩＣカードを用いた取引システム

ン・ライン取引システムを指す。ＩＣカードによる取引システムの形態としては、これ以外に端末機とＩＣカード間の通信のみで取引が完結し、センター－ＩＣカード間で実時間の情報交換の必要がないオフ・ライン取引も考えられるが、ここでは扱わない。

このような取引においては利用者とサービス提供者が互いに相手を見ることのできない状況の下で取引が実施される。したがって安全な取引手段および取引証明法の提供がきわめて重要となる。取引証明の説明の前にまず取引実行の一般的流れを説明する。

取引は大きく３つの段階に分けられる。まず第一の段階は、初期化の段階で、ここではカードが端末にセットされセンタのホストに対し通信要求が出されて、端末、カード、ホストが取引入力待状態までゆく。この段階では安全な取引入力が可能か否か確めるために次の様な正当性確認が行なわれる。

ａ．本人確認
ｂ．カード正当性確認
ｃ．端末正当性確認
ｄ．ホスト正当性確認

ａ．はカード使用者がカード所有者本人かどうかの確認であり、現在は暗証番号の照合によって行われている。今後個人認証技術が向上すれば、指紋や声紋などの身体的特徴による確認も利用される可能性がある。ｂ．は端末に挿入されたカードが有効なカードかどうかの確認である。ｃ．ｄ．の端末およびホストの正当性確認は、ＩＣカードがその通信相手が正当であることを確認する手続である。

以上の確認手続が全て正常に終了し、取引に関与するカード、カード所有者、端末、ホストがそれぞれ正当であることが確認されると次は第二の段階である取引実行に入る。

取引実行段階の詳しい内容は第３章で述べるが、一般にはホストへの取引要求の伝送、ホストの応答および取引実行などの手続が踏まれる。

最後の第三段階は終了手続であり取引が終了し、利用者がカードを受け取って端末機から去るまでがこの中に含まれる。

３．取引証明の実現

以上のようなＩＣカードを用いた取引システムにおいて、暗号機能を利用した取引証明を実現する具体的方式をいくつか挙げて、それぞれについて説明する。ここで述べる取引証明の基本的考え方は、その取引記録が誰のものであり、正当なものかどうかが後になって確かめられるような記録を証拠として残すことである。方式の大前提としてＩＣカードが内部に暗号器を備えている構成を考えている。尚、重要な暗号化鍵の配送については章を改めて説明するが、鍵は少なくともカード毎に異なるものと仮定する。

①電文に認証子を付加する方式

この方式は取引電文にその電文の認証子（ＭＡＣ＝Ｍessage Ａuthentication Ｃode）を付加してセンタに送信することによって電文の取引証明とするものである。ふつう、ＭＡＣは送受信者間で電文の完全性（偽造・改ざんが行なわれていないこと）を確認するために用いられるが、ここでは、電文とＭＡＣを対として記録して、取引の証拠とすることを考えている。

図２にこの方式の概要を示す。ＭＡＣとしては電文をＩＣカード内で暗号変換したものを用いている。暗号アルゴリズムは例えばＤＥＳのようなものでよい。鍵はセンタとＩＣカードだけが共有し第三者は知らないとする。しかもカード毎に、また取引のたび毎に異なるものとする。

一方、電文を受信したセンタでは独自に生成したＭＡＣとの比較により、受信したＭＡＣが正しいことを確認した後に取引を実行する。同一のＭＡＣが生成できるのは鍵を共有するセンタとＩＣカードだけだから電文の内容は信頼できるわけである。取引記録は電文Ｍ、ＭＡＣ、および鍵生成に用いた

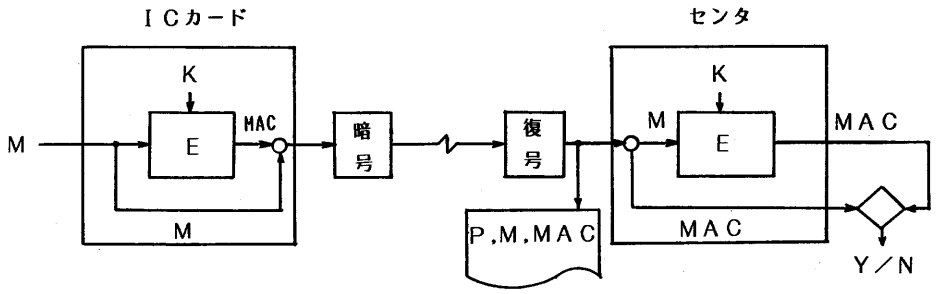

図２．認証子を用いた取引証明

パラメータなどから成っていて、後日いつでも、ＭＡＣを検査することによって電文の内容を確認することができる。

以上の手続で記録されたＭＡＣが証拠能力を持つためには以下のような前提が必要である。第一にＩＣカードがハードウェア的に安全であること。すなわち正規の方法以外では内部のデータにアクセスできないこと、改造や破壊によってシステムの安全性を脅かすことができないこと。特に鍵がカード外部に洩れないことが重要である。第二にセンタは暗号装置を悪用しないという意味で信用できるものとしている。さもなければＭＡＣ比較の時に暗号装置から得られるＭＡＣによってＭＡＣのでっちあげが可能となる。第三に取引記録装置は暗号装置と常に連動して、記録もれや、記録抹消が起きないように管理されていること。第四に暗号化の鍵は少なくとも各利用者毎に異なること。安全性を高めるには上の説明で述べたように、取引のたび毎に異なることが望ましい。

ところで、図２ではＩＣカード内の暗号器はＭＡＣ生成用だけに用いているので、回線上のデータを守るために、ＩＣカードの外部で別の暗号器を用いている。外部の暗号装置を用いずにＩＣカード内の暗号器を二重に用いてＭＡＣ生成と、データの秘匿の両機能に用いる構成も可能である。

②カード識別子込みで暗号化する方式

次にＩＣカードの暗号器によって取引電文全体をカード識別子込みで暗号化する方式を説明する。この方式の特長はＩＣカードに入力された電文にはカード固有の値Ｎ（カード識別子）が自動的に付加されて、しかる後に暗号変換される点である。このため同じ鍵を用いて同じ電文を暗号化しても、ＩＣカード毎に異なった暗号文が得られる。これを取引証明に用いるのである。付加の方法は様々に考えられるが、受信側でそれを分離できることが条件である。たとえば、上位ビットをＭとし下位ビットにＮを置くという方法が最も単純な例である。Ｎは暗号器固有の値であるので電文を復号すると、それがどのＩＣカードで暗号化されたか判る仕組みになっている。

この機能を用いた取引を図３に示す。センタは受信電文を復号したら、まずＮのチェックを行ない、相手カードの確認をした後に取引を実行する。①の方式と同様にセンタは鍵生成に用いたパラメータと復号前の電文Ｅ（Ｎ，Ｍ）を取引証明として保存しておく。センタ側の暗号器でも同様に電文には暗号器に入る前に自動的に識別子Ｎ'が付加されるので受信側では復号後Ｎ'によってその電文の作成者をチェックでき、さらに電文Ｅ（Ｎ'，Ｍ）を証拠電文として保存できる。

電文Ｅ（Ｎ，Ｍ）が証拠となるためには、他の暗号器ではそれが作成できない事が前提となる。そのためにこの方式では次の仮定をおく。ＩＣカード

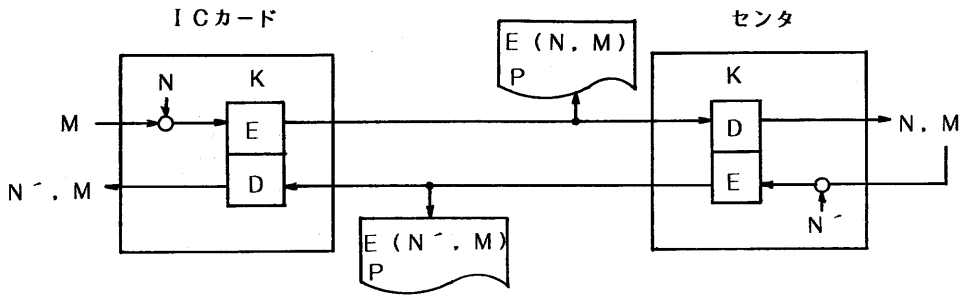

図３．カード識別子込みの暗号化による取引証明

がハードウェア的に安全であること。同時にセンタ側の暗号装置がハードウェア的に安全であること。取引記録装置は物理的に安全に管理されていること。また鍵Ｋは、ＩＣカードとセンタの装置で内部的に発生され、その形は利用者もセンタも知らない真の意味での秘密の鍵とする。しかも取引のたび毎に異なるものとする。

このように仮定すればアルゴリズムが公開で、暗号器への入力Ｎ，Ｍのデータ形式が知れても、Ｅ（Ｎ，Ｍ）を第三者がつくることはできない。また仮に、センタが証拠文Ｅ（Ｎ，Ｍ）の偽造を試みてＭの暗号化を行ったとしても、センタで生成できるのは暗号文Ｅ（Ｎ´，Ｍ）だけであり、センタによる証拠偽造も不可能になる。このように方式②では対向する暗号器間にハードウェア的に非対称性を作りだすことで電文の証拠性を高めているのである。この非対称性の考え方をさらに一般化した方式を次に述べる。

③非対称化による方式[1]

７６年にDeffie-Hellmanによって提案された公開鍵暗号系[2]は暗号鍵と復号鍵が異なりかつ暗号鍵から復号鍵を導出する事がきわめて困難という構造を持ち非対称暗号系とも呼ばれている。この暗号系の特色の一つは公開鍵暗号の非対称性を利用することによってディジタル署名、すなわち電文の発信元を証明する機能が実現されることである。これに対して、ここでは、ハードウェア的な安全性が期待できれば慣用暗号でも非対称な構造を実現できることを示し、これを利用した取引証明を与える。

図４に基本的な考え方を示す。図のようにＩＣカードには暗号器Ｅと鍵Ｋを持たせる（復号器は持たせない）。センタ側には、逆に復号器Ｄと鍵Ｋを持たせる（暗号器は持たせない）。暗号アルゴリズムは、暗号化変換Ｅ≠復号化変換Ｄという条件を満たす任意の慣用暗号系で良い。たとえばＤＥＳがそのひとつである。鍵Ｋは第三者はもちろん、利用者、センタも知らない完全な意味での秘密鍵とする。ここで、センタはＥ（Ｍ）とＭのペアを証拠データとして保存しておく。そうすれば利用者は送信の事実を否定できない。なぜなら、第一に、センタ装置は暗号器を持たないので、復号した時Ｍになるような取引証明文Ｅ（Ｍ）を作り出すことはできない。また利用者カード、センタ装置以外の装置は、鍵Ｋを持たないのでＥ（Ｍ）を作り出すことが当然できないからである。結局、意味のある平文Ｍに対応する証明文Ｅ（Ｍ）を作り出し得るのは利用者のＩＣカードのみである。本方式の基本的な考え方は、以上のように送信側、受信側の

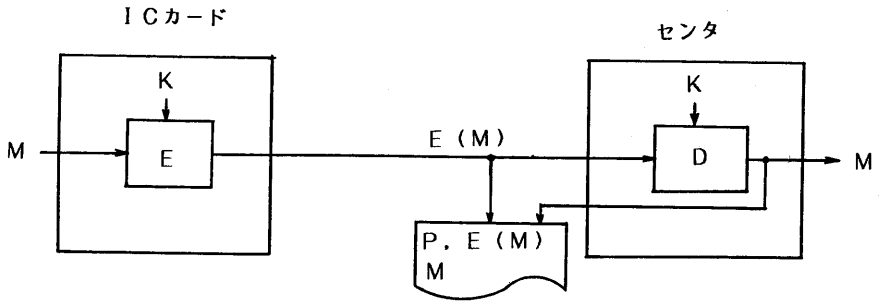

図４．非対称化による取引証明

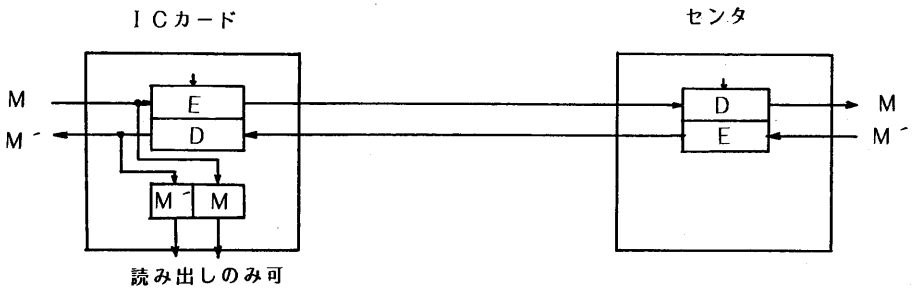

図５．カード内に取引記録を残す取引証明

暗号化変換を一方向的にすることによって、非対称性を実現し取引記録の証拠性を高めるものである。

この方式の前提は③の場合と同様で、ＩＣカードとセンタの暗号装置のハードウェア的安全性、取引記録生成装置の物理的安全性および鍵の秘密性である。鍵が上記のように真の意味での秘密鍵であればアルゴリズムが公開であっても暗号器間の非対称性を維持できる。真の意味での秘密鍵の生成は例えば、次のようにして実現できる。まず実際に取引に使われる鍵Ｋは親となるマスタ鍵から生成されるものとする。このときこのマスタ鍵をセンタの秘密の乱数と第三者、たとえば製造者の秘密の乱数との排他的論理和によって生成すればよい。鍵生成は４章で再び説明する。

④カード内に取引記録を残す方式[3]

これまでの３例では取引記録を何処で作成するかについて特に触れず、漠然と「センタ側」または「利用者側」というように述べてきた。しかし暗号化機能と組み合せて記録を残す場合でも、暗号装置と記録作成装置が独立して存在する場合には記録装置を暗号器と切離すことによって都合の悪い取引記録の抹消が行われるかもしれない。少なくともそのような事が生じないように記録生成装置を物理的に管理する必要があった。ここでは視点をやや変えて、取引記録生成装置をＩＣカードの中に暗号器と一体的に実装し、これらの問題を解決して取引記録の信頼性を向上させる方法について考える。

具体的方法としては、ＩＣカードに、暗・復号化と同時に自動的に電文の記録を内部のメモリに残す機能を持たせる。記録を残すメモリ領域は読み出しのみが許可されていて、書込み・消去ができないようにＣＰＵによるアクセス制御がかかっているものとする。

（図５）。取引に関わる電文は必ずＩＣカードのこの機能を用いて暗号化することにすれば、トラブルが発生した場合には、このメモリ内容を読み出すことにより、取引の内容をチェックできる。

しかしながら、ＩＣカード内の記録を単なる記録としてではなく、取引証拠として使えるようにするためには、単に個々の通信の記録を保存するだけでは不十分である。例えば、利用者が取引電文Ｍをメモリに記録した後に、通信を中止した場合や、或いは通信回線の事故等によって実際に通信が行なわれなかった場合を考えてみる。この場合、ＩＣカードのメモリ内には記録が残されるが、実際には電文はセンタに送られないので取引は実行されないままである。すなわち、記録内容と実際の取引との間に不一致が生じ、取引証明は実現されない。したがって、このような不一致が生じないような取引手順を定めておかねばならない。

上で述べた例を良く考えてみると、問題はセンタの知らない所で取引内容の記録が残されたために生じている。言い換えれば、取引記録生成に必ずセンタが関与するようにすれば不一致は生じないと考えられる。そのためには、取引要求の記録とそれに対するセンタの応答が常に対となって記録されるような通信手順を定めれば良い。その具体的手順を図６に示す。

図６で端末から入力された取引要求電文はＩＣカードにおいて、記録・暗号化された後、センタに送られる。センタはこれを復号し、取引内容をチェックし、取引可能であればYES 、不可能であればNOを暗号化して返送する。この段階ではまだ取引を実行しないでおく。返送電文はYES/NOの他に、返送文が確実にＩＣカードに届いた事をセンタが確認するための電文RNを含んでいる。RNはセンタが秘密に作る、取引毎に異なる乱数である。端末はセンタからの返送電文をＩＣカードに転送し、復号・記録し、平文となった電文を受け取る。電文のRN部は再びセンタにもどされオリジナルRNと比較され、これが一致してはじめて取引が実行される。RNの一致によってセンタの電文がＩＣカード内で正しく復号されたことがわかり、同時に応答電文がＩＣカード内に記録されたことが確認できる。

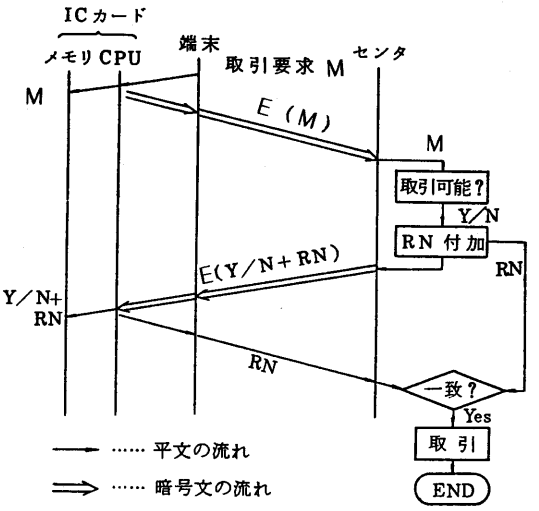

図６．方式④における取引実行手順

以上の手順によれば取引要求電文と、その可否を知らせるセンタからの応答電文が、メモリ内に必ず対となって記録されるので、これを取引証明として用いることができる。

この方式の場合はＩＣカードとセンタの暗号装置とがハードウェア的に安全であると同時に鍵が個々のカード毎異なっている事が条件である。

４．鍵の配送

ここでは第３章では説明しなかった鍵配送を考える。まず鍵に対して次の条件をおく。カード毎に異なり、また取引のたび毎に異なること。利用者は鍵Ｋを直接には知ることがなく、場合によってはセンタ自身も知らないものとする。

図７にこのような条件を満たす鍵生成の一例を示す。但し、装置のハード

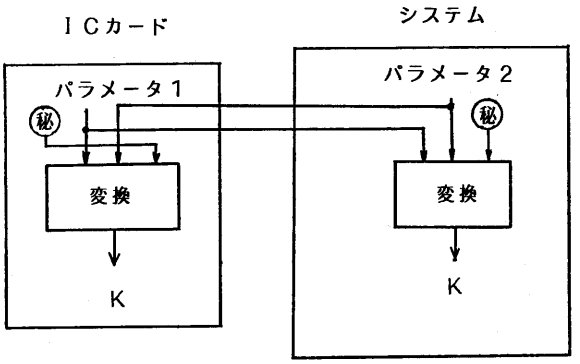

図７．鍵生成手続き

ウェア的安全は保証されているものとする。ＩＣカードとセンタは暗号通信に先立って、各々生成した乱数を交換してこれを変換手続によって変換し鍵Ｋを生成する。生成された鍵を秘密にするには変換手続を非公開にしてもよいし、図のように第３の秘密パラメータを変換の入力とすることも可能である。この時誰が秘密パラメータを生成管理するかは場合による。３章の方式③で述べたようにセンタさえも知らないようにすれば、完全な秘密鍵Ｋがえられる。

５．むすび

ＩＣカードの暗号機能の応用として、ＩＣカードを用いたオン・ライン取引システムにおける取引証明法について検討した。本稿で述べた各方式の目的は、電子的な取引記録に対して、従来の紙に書かれた証拠書類と同様の証拠能力を付加することであった。ここではその基本となる考え方を示したが、提案した方式を組合わせるだけでも、種々の変形方式を導くことが可能である。

はじめに述べたようにＩＣカードの用途は様々である。本文で提案した方式を実際に用いる場合には、カードの用途に合わせて、そのいずれかを選択することになるであろう。

今後の課題としては、さらに新しい方式の提案を行うこと、また本文では扱わなかったオフ・ライン取引の場合の検討、公開鍵暗号を用いた場合の検討などが挙げられる。

参考文献

(1) 神竹，水谷：”ＩＣカードを用いたディジタル署名の実現”，昭和６０年信学総全大，Ｎｏ．１８５８．

(2) W.Deffie, M.Hellman,"New direction in cryptography", IEEE Trans. on Inf.Theory Vol.IT -22,No.6,pp. 644-654(Nov.1976) .

(3) 神竹，川村：”ＩＣカード・システム－暗号機能の応用－”，昭和６１年信学総全大，Ｎｏ．１７９７．