解　説

ディジタル署名と暗号鍵管理†

小　山　謙　二††

1. はじめに

■現在のビジネス社会では，筆跡や印鑑によって本人であることと，契約内容の正当性を認証している．しかし，筆跡や印影などの原情報そのものをディジタル信号として通信，または，記録する場合，容易にコピーできるので，単に照合する認証方式は有効でない．そこで，ディジタル情報に適用できる認証方式の必要性が生じており，暗号を用いたディジタル署名の研究開発が進展している[1),4),5),10)]．

最近，発明された公開鍵暗号は，秘密通信のみでなく，送信者の身元と通信文の内容の改ざんの有無を確認する認証へも有効に適用できる．この認証機能はディジタル署名とも呼ばれ，公開鍵暗号を用いると送信者以外の誰も偽造出来ない署名ができる．つまり，公開鍵暗号は，鍵管理に質的なブレークスルーをもたらしただけでなく，暗号の適用領域を広げた．

ところで，暗号とは，保護したい多くの情報を小さなサイズの暗号鍵で管理しているといえる．現代暗号では，暗号アルゴリズムを公開しているが，慣用暗号の暗号化鍵・復号化鍵はもちろんのこと，公開鍵暗号においても復号化鍵は秘密にしておかねばならない．したがって，秘密のパラメータである暗号鍵をいかに管理するかは従来以上に重要な研究課題の一つである．

本稿では，最近のディジタル署名と暗号鍵管理の研究と実用化の動向を概説する．

2. 現在のディジタル署名法の特徴と問題点

ディジタル署名は，次の2段階の処理で行われる．

Step 1.　送信者は秘密に保持している鍵で通信文(平文)を暗号処理して“署名文”を生成し，受信者に送る．

Step 2.　受信者は署名文をもとにして，通信文の送信者（筆者）が本人であることと途中での改ざんの有無を確認する．

ディジタル署名においては，安全性の観点から，次の3条件を満たすことが必要である．

（A）　署名文が第三者によって偽造できない．

（B）　署名文が受信者によって偽造できない．

（C）　署名文を送った事実を送信者が後で否定できない．

現在のディジタル署名に用いる各手法を

① 暗号法（慣用暗号と公開鍵暗号）

② 検査法（通信文復元法と認証子照合法）

③ 構成法（直接署名と調停署名）

の観点から分類し，その特徴を以下に述べる．

2.1 暗号法

ディジタル署名を行うために用いられる暗号として慣用暗号と公開鍵暗号がある．

（1） 慣用暗号

慣用暗号とは，暗号化鍵と復号化鍵が同一でそれぞれ秘密にしておく暗号である．慣用暗号によるディジタル署名では，送信者と受信者のみで共有している秘密の鍵で署名文を生成するので，条件 A は満たされるが，条件 B は満たされていない．

現在の代表的な慣用暗号としてデータ暗号規格DES(Data Encryption Standard)[16)]がある．DESは，1977年に米国商務省標準局（NBS）より公布され，完成度の高い慣用暗号方式として，現在，米国の銀行システムなどで採用されている．DESは国際標準化機構（ISO）でも標準化が進行中であり，世界的に広まりつつある．

（2） 公開鍵暗号

公開鍵暗号とは，一対の暗号化鍵と復号化鍵が異なり，暗号化鍵は公開し，復号化鍵のみを秘密にしておく暗号である．公開鍵暗号によるディジタル署名では，送信者のみが秘密に保持している鍵を用いて暗号処理（復号化）を行い，署名文を生成するので，条件

† Digital Signature and Cryptographic Key Management by Kenji KOYAMA (Musashino Electrical Communication Laboratory, N. T. T.).

†† 日本電信電話公社武蔵野電気通信研究所

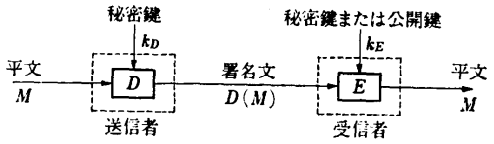

図-1 通信文復元法

A と B は満たされる.

現在の代表的な公開鍵暗号として，1978年に Rivest・Shamir・Adleman によって発表された RSA 法[18]と，1979年に発表された Rabin のR法[17]などがある.

RSA 法は，復号化関数が全単射なので，すべての通信文に対して署名が可能である長所を持つが，暗号化と復号化の計算量が多いことが欠点である．R法は，復号化関数が全単射でないので，すべての通信文に対して署名が可能とは限らない欠点をもつが，暗号化の計算量が少ない長所を持つ.

2.2 検査法

署名文の検査法として通信文復元法と認証子照合法がある.

（1） 通信文復元法

通信文復元法では，**図-1** に示すように，まず，送信者が通信文に秘密鍵 k_D で暗号処理 D を施して署名文に変換し，受信者に送る．次に，受信者は送られてきた署名文に鍵 k_E で（慣用暗号の場合 k_E と k_D は秘密，公開鍵暗号の場合 k_E は公開），暗号処理 D の逆変換 $E\ (=D^{-1})$ を施して元の通信文を復元する．復元された通信文が意味のあるものならば，（例えば，日本語として意味をなすものならば）受信者は通信文の送信者と内容が正しいと認証する．この方式は通信文の冗長性を利用した方式といえる．すなわち，もし，不正な秘密鍵で署名していれば，ランダムな意味のないパターンが現れ，正しい秘密鍵で署名していれば，意味のある通信文が現れることを利用している．この方式は暗号化と復号化による双方向の暗号操作で実現している．したがって，この方式に慣用暗号と公開鍵暗号のいずれを適用しても，第三者には秘密鍵は知られていないので，条件 A を満たす．しかし，慣用暗号による通信文復元法は，受信者が秘密鍵を持っているので，条件 B を満たさない．一方，公開鍵暗号による通信文復元法は，送信者のみが秘密鍵を持っているので条件 B を満たす.

ところが，この画期的な公開鍵暗号による通信文復元法も次のような問題点がある．第一に，通信文が日本語や英語などの自然言語の場合，復元された通信文が「意味のある」ものかどうかの判断を人間が介在しないで，計算機が自動的に処理することは，現在の意味処理技術のレベルでは非常に困難である．第二に，通信文が純然たるランダムな数字データで成り立っている場合は，冗長量が0なので，復元した通信文が「意味のある」ものかどうかを判定することは原理的に不可能である．これらの問題点の考察と解決策は第**3**章で後述する.

（2） 認証子照合法

認証子照合法は検証とも呼ばれている．認証子照合法では，**図-2** に示すように，まず，送信者が通信文に秘密鍵 k_h でスクランブル（データ圧縮型暗号処理）h を施して，認証子（署名文）に変換し，生のままの通信文とともに受信者に送る．次に，受信者は送られてきた生の通信文に送信者と同一の秘密鍵 k_h でスクランブル h を施して新たに認証子を生成し，送られてきた認証子と照合する．もし，一致したならば，受信者は通信文の送信者と内容が正しいと認証する．この方式は秘密鍵で一方向のスクランブルを行うことによって実現しており，逆変換が保証されている暗号を必ずしも用いなくともよい．また，照合を基本としているので，意味処理を行う必要はない．しかし，この方式は，送信者と受信者で共通の秘密鍵を保持することが必要なので，鍵配送が困難なことと安全性の条件 B を満たさないことが欠点である.

スクランブル関数 h の満たすべき条件は以下の通りである.

条件1：「h は通信文の分割単位であるブロックごとに独立に計算するのではなく，通信文のすべてのビットに依存した方法で計算する.」

この性質により，暗号解読者が一見，不自然でないブロックを通信文に挿入して，そのブロックに対する署名を得ることを困難にしている．この条件を満たすために，CBC (Cipher Block Chaining) モードの使用が提案されている.

条件2：「任意の与えられた通信文 M と $h\ (M)$ に

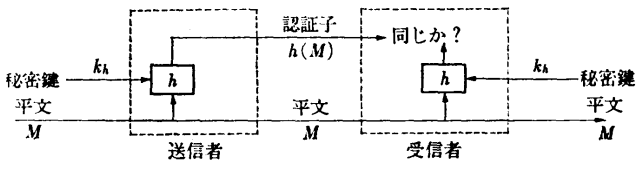

図-2 認証子照合法

対し，$h(M)=h(X)$ となるような他の通信文 X を見つけることが非常に困難である.」

この性質により，$h(M)$ を知っている第三者が認証子を変えないで，通信文 M を通信文 X に変えて，あたかも不正がないように改ざんすることを防ぐことができる．また，秘密通信とディジタル署名の両方を実現する場合に，通信文の秘密を守ることができる．この条件を満たすためには，$h(M)$ は一方向性関数でなければならない．さらに，異なる通信文が同じ $h(M)$ の値になる確率を小さくするために，$h(M)$ のサイズはある程度大きくなければならない．

条件3：「h に関して，次式が成立する必要がある．

$$h(X\cdot Y)\neq h(X)\cdot h(Y) \qquad (1)」$$

この性質により，Davida[3] と Denning[6] によって提案されている暗号解読が出来なくなる．式(1)を満たす条件は，演算・が＋のとき，

$h(X)\neq cX$，　c：定数

となり，演算・が×のとき

$h(X)\neq X^a$　a：定数

となる．

条件4：「$h(M)$ の計算が高速に実行できる.」

この性質により，関数 h を付加したオーバヘッドを極力おさえることができる．この条件を満たすためには，h を多項式とすると，出来るだけ次数の低い多項式が望ましい．

以上の性質を満たす関数 h として，DES と Rabin の公開鍵暗号法（R 法）の暗号化関数が提案されている．また，$h(M)$ のサイズとしては，32ビット[23]，512ビット[12]がそれぞれ提案されている．

2.3 構 成 法

ディジタル署名の構成法として，直接署名と調停署名がある．

（1） 直 接 署 名

直接署名では，受信者が直接，通信文の正当性を認証する．もめごとが起こった場合のみ判定者が呼ばれ，送信者と受信者のいずれが正しいかの判断を下す．慣用暗号による直接署名のプロトコルもいくつか提案されているが，メッセージを送るごとに，送信者と受信者が前もって秘密の鍵を共有する必要があるので，このプロトコルは非効率的と一般に考えられている．

直接署名は公開鍵暗号の性質を用いればうまく実現できる．特に，公開鍵暗号による通信文復元法を用いた直接署名は，鍵管理が容易で，条件 A，B を満たすので，「真の署名」とも呼ばれている．しかし，条件 C に関しては，いかなる暗号方式を用いても送信者と受信者の2人で直接署名をする限り，満たされない．

（2） 調 停 署 名

調停署名では，送信者と受信者以外の第三者である調停者が通信文の正当性を認証し，その結果を受信者に知らせる．すなわち，信頼のおける調停者を介して認証を行うのが調停署名である．この調停署名の概念は，本来，慣用暗号による署名において，条件 B を満たすために導入されたものであるが，公開鍵暗号による署名においても，条件 C を満たすために適用できる．しかし，調停署名は調停者の信頼性に大きく依存している．

2.4 ま と め

2.1 から **2.3** で述べたディジタル署名の各手法間の関連をまとめる．

通信文復元法では，慣用暗号と公開鍵暗号が適用できる．しかし，認証子照合法では，送受信者が共有している秘密鍵で認証子を生成せざるを得ないので，公開鍵暗号の特性は生かせず，慣用暗号しか提案されていない．

次に，各手法がディジタル署名の安全性の3条件を満たすかどうかの関連を**表-1** にまとめる．

3. 通信文復元法の意味処理

「真の署名」は秘密鍵の配送が不要な点と受信者が直接，認証できる点で大きなメリットをもつが，通信文復元法の意味処理に対する問題点があるので，本章

表-1 署名法とディジタル署名の3条件との関連

署名法			条件〔不正行為者〕		
暗号法	検査法	構成法	(A) 第三者	(B) 受信者	(C) 送信者
慣用暗号	通信文復元法	直接署名	○	×	×
		調停署名	○	×	○
	認証子照合法	直接署名	○	×	×
		調停署名	○	×	○
公開鍵暗号	通信文復元法	直接署名	○	○	×
		調停署名	○	○	○
	認証子照合法	直接署名	—	—	—
		調停署名	—	—	—

注）○：満たす，×：満たさない，
——：方式が提案されていない．

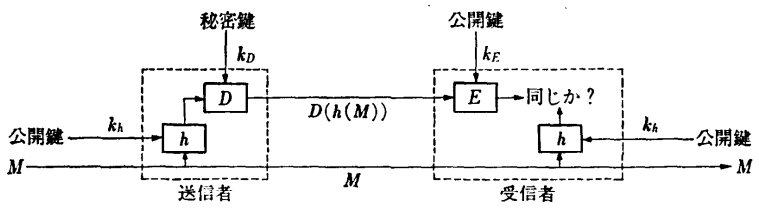

図-4 改良型ディジタル署名法

で詳しく考察する.

3.1 エントロピーとの関連

いま，ある言語の冗長量を R とし，暗号鍵のエントロピーを H_k とすると，H_k/R は判別距離 N_0 と呼ばれている．この言語のアルファベットからランダムに N 個選んで並べた通信文を生成した場合，N が N_0 以上ならば，通常（平均的に），この通信文は意味をなさないことが示されている.

ここで，通信文復元法で認証を行う場合の通信文長と判別距離との関係を考えよう．通信文の長さ N が N_0 以上の場合，正しい鍵が使われていれば，意味のある通信文はただ1通り復元される．不正な鍵が使われている場合，意味のある通信文は復元されない．通信文の長さ N が N_0 未満の場合，正しい鍵を使っても使わなくとも意味のある通信文が復元される．したがって，ディジタル署名による認証を確実に行うためには，

$$N > N_0$$

が望ましい.

ところで，自然言語には冗長性があり，例えば，英文の冗長量 R は 3.2 ビット/記号と言われている．一方，ランダムな数字列の冗長量 R は0である．ここで，鍵のサイズを有限なある値に設定すると，自然言語の判別距離は有限なある値になるが，ランダムな数字列の判別距離は無限長になる．したがって，もし，通信文がランダムな数字データ，または，判別距離以下の自然言語で成り立っている場合は，復元した通信文が「意味のある」ものかどうかを判定することは原理的に不可能であることがわかる.

一方，暗号化による秘密通信を行う場合，通信文の長さ N が N_0 以下ならば，無条件に安全であることを Shannon が明らかにした[22]．すなわち，$N < N_0$

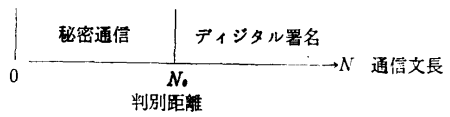

図-3 秘密通信とディジタル署名の適用領域

ならば，鍵を知らずに通信文の言語的特徴だけを用いて，暗号文から通信文に復元することは原理的に不可能である．したがって，秘密通信では，

$$N < N_0$$

が望ましい．通信文の長さに対する安全性に関してディジタル署名と秘密通信が“双対”の関係になっていることは興味深い．この関係を図-3 に示す.

3.2 付属情報による解決

復元した通信文の意味処理を容易にするために，送りたい狭義の通信文に付属情報（送信者の識別名，受信者の識別名，通信文の通し番号，日時）を付けた広義の通信文を生成することが考えられている[4]．この付属情報を付加した広義の通信文に対する署名文を送り，付属情報をもとに狭義の通信文が正しいものかどうかの判定に役立てている．特に，付属情報に通し番号と日時を含めることにより，第三者が署名文を盗聴して同じ署名文を何度も送ったり，時間をずらせて再送する不正行為を防ぐ役割も果たしている．この方式は付属情報という冗長性を付加して意味処理に役立てているといえる．また，付属情報のフォーマットや位置を前もって定めておくことにより，自動的に照合できるメリットもある.

3.3 検査法の併用による解決

最後に，高速で安全な改良型ディジタル署名法の方式を述べよう．この方式は公開鍵暗号による認証子照合法と通信文復元法を併用することによって，通信文復元法の意味処理と暗号化速度の問題点を解決し，かつ，条件 A と B を満たしている．この基本構成は以下の通りである．送信者は通信文 M に対し公開鍵 k_h でスクランブル h を施し，認証子 $T(=h(M))$ を生成する．さらに，この T に対し秘密鍵 k_D で暗号処理 D を施し，T の署名文 $V(=D(T))$ を生成する．そして，V と M を送る．受信者は V に対し公開鍵 k_E で D の逆関数 E を施し，認証子 T を復元する．一方，M に対し公開鍵 k_h でスクランブル h を施し，認証子 T を生成する．これらの2種類の T を照合して

認証する．この改良型ディジタル署名法のブロック図を図-4 に示す．

この改良型ディジタル署名法のスクランブル関数 h として，R 法の暗号化関数または，DES を CBC モードで用い，関数 D, E として RSA 法の復号化関数，暗号化関数を用いるプロトコルが提案されている[4),12)]．特に，R 法と RSA 法を併用する方式[12)]は，法の数 n を同一（512 ビット）にしているために認証子照合法と通信文復元法の整合性がよい．

4. 暗号鍵管理法

暗号鍵管理の主な課題として，鍵配送法，鍵保管法，鍵生成法，および，鍵変更法がある．

4.1 鍵 配 送 法

慣用暗号では，秘密通信を行う場合，前もって送信者と受信者の間で秘密鍵を共有しなければならない．そのために，秘密鍵を安全に配送する必要がある．外交や軍事などでは，信頼できる密使が直接，鍵を届けている．一方，ビジネス用の暗号通信では，書留や電話で鍵を連絡している例が多いが，安全とはいえない．まして，公衆網のように通信相手が多い場合には通信相手全員に鍵を秘密に配送することは非常に煩雑である．

公開鍵暗号では，秘密の復号化鍵は自分のみが保持すればよい．公開の暗号化鍵は秘密裏に配送する必要はないので，電話帳のように通信相手全員に公開でき，鍵管理が非常に便利である．ただし，公開鍵のファイルを管理する鍵配送センタは信頼できる機関によって運営されなければならない．公開鍵ファイルの読出しは自由であるが，変更と書き込みは資格のある人のみ許されるように，アクセス制御しなければならない．

ところで，暗号化速度の速い DES と，鍵配送が不要で認証機能がある公開鍵暗号を組み合わせた現実的なシステムも提案されている．このシステムでは，DES の鍵（64 ビット）を公開鍵暗号で送り，本来の大量のデータを高速な DES で暗号化する．米シーメンス社や我が国の郵政省の実験システムは公開鍵暗号として，RSA 法を採用している．米マイタ社や富士通は DES の鍵配送に Diffie・Hellman の公開鍵配送法[5)]を利用している．

4.2 鍵 保 管 法

従来の暗号鍵保管方式としては，暗号鍵を 1 人で保管する方式，あるいは，暗号鍵のコピーを複数人で保管する方式が中心であった．前者は鍵の紛失・破壊に対する信頼性が低く，後者は不正な使用に対する安全性が低い．このため，最近の暗号鍵保管方式として主に，個別鍵暗号化用マスタ鍵方式，個別鍵代替用マスタ鍵方式，暗号鍵分散共有方式の 3 方式が提案されている．

（1） 個別鍵暗号化用マスタ鍵方式

個別鍵暗号化用マスタ鍵とは複数の個別鍵を暗号化する「マスタ鍵」のことである．個別鍵と「マスタ鍵」を用意しておいて，両方の鍵が同時に揃った場合だけデータの暗号化/複号化ができる方式である．この方式は IBM 社やパラダイン社などで採用されている[14)]．暗号鍵管理の分野で「マスタ鍵」と言えば，通常，この方式を意味する．この方式は安全性の向上をねらった集中型の暗号鍵管理法であるが，鍵の紛失・破壊に対する信頼性は低い．

（2） 個別鍵代替用マスタ鍵方式

個別鍵代替用マスタ鍵とは，個別鍵の紛失・破壊の場合に個別鍵の代わりに使用できるマスタ鍵である．このマスタ鍵方式は物理的錠システムでは一般的な概念であるが，暗号システムでのマスタ鍵の存在条件と導出法は，1982 年の筆者の論文[8)]によって初めて明らかにされた．現在，RSA 法と R 法のマスタ鍵の存在が明らかになっている[11)]．この方式は，マスタ鍵を安全に保管する必要があるが，信頼性の向上をねらった分散型鍵管理法である．また，この方式は，送信者が公開のマスタ鍵で暗号化して放送し，受信者が秘密の個別鍵で復号化する秘密同報通信にも有効に適用できる[9)]．

以上の 2 種類のマスタ鍵，すなわち，個別鍵暗号化用マスタ鍵と個別鍵代替用マスタ鍵の違いを明確にす

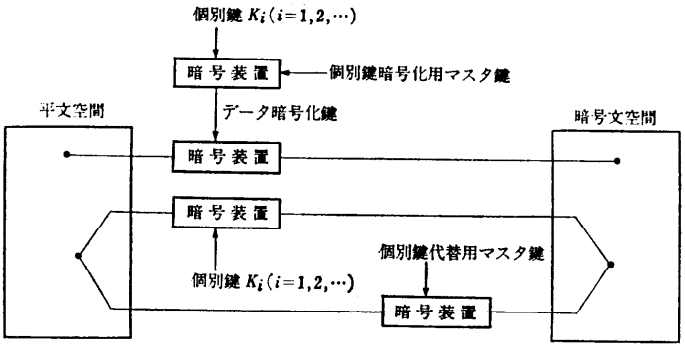

図-5 2 種類のマスタ鍵の概念図

るために，概念図を図-5 に示す．

（3） 暗号鍵分散共有方式

暗号鍵分散共有方式は，秘密情報である一つの暗号鍵から複数の分散鍵を生成して各構成員に分配する．そして，全構成員（m 人）の中の任意の構成員から一定人数（k 人）以上の合意が得られると，それらの構成員の分散鍵をもとに元の秘密暗号鍵を合成できる方式である．特に，k 人未満の分散鍵を持ち寄っても元の秘密鍵に関する情報は全く分からない点に特徴があり，いわば，k out of m しきい値アクセス構造を持った鍵管理法といえる．この方式の効率的な実現法として，Shamir は多項式の補間を用いる方法を提案している[2]．また，筆者はこのしきい値アクセス構造を拡張し，階層構造をもつ複数グループにも適用出来る方法を提案している[13]．

4.3 暗号鍵生成法

次に，暗号鍵生成法について述べる．暗号鍵の生成は通常，利用者自身が行う．鍵の値をランダムに選択することが重要である．また，「弱い鍵」を避けることも，やはり，重要である．

DES の弱い鍵としては次のようなものが IBM より提示されている（16 進表示）．

0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1
F E F E F E F E F E F E F E F E
1 F 1 F 1 F 1 F 0 E 0 E 0 E 0 E
E 0 E 0 E 0 E 0 F 1 F 1 F 1 F 1

一方，RSA 法とR法の公開鍵暗号では，大きな素数を生成することが必要となる．例えば，RSA 法の暗号化/複号化では，大きな2つの素数 p と q の積 n を法としてべき乗計算を行い，暗号の安全性の根拠を n の素因数分解の困難さにおいている．この素因数分解の手間が非常に大きくなるように，p と q の桁数を定めることが重要である．現在，知られている最高速の素因分解アルゴリズムを1マイクロ秒/1演算で行っても10億年かかるように，p と q の値は10進100桁程度に設定するように勧められている．さらに，p と q は次のような性質を持たせた方が安全上，望ましい[19]．

① p-1 が大きな素因数 p' を持つこと
② q-1 が大きい素因数 q' を持つこと
③ p'-1 が大きな素因数 p''を持つこと
④ q'-1 が大きな素因数 q''を持つこと

大きな整数が素数であるか否かを調べるには，フェルマー・テストが有用である．近年の高速判定法は，すべてフェルマー・テストを改良して，あるところまで調べれば，素数として正しく判定できるようにしたものである．近年，大きな貢献をしたのは，Adleman, Pomerance, Rumely らのグループである．最近，Lenstra と Cohen はさらに改良した手法を開発し，100桁の数に対して，40秒で素数判定できたそうである[2]．ところで，この手法は素因数分解の高速化には直接つながらないことに注意しよう．

4.4 暗号鍵変更法

次に暗号鍵変更法について述べる．暗号鍵をいかに厳重に保管していても，同じ鍵を長期間使用していると，鍵そのものが無断コピーや暗号解析により第三者に知られてしまう可能性がある．そこで，適当な周期で鍵を変更することが重要となる．実際には，1週間，1月，1年単位で鍵を変更していることが多い．この周期の決定にあたっては，暗号の強度，秘密にすべき情報の重要度，鍵変更の手間などのパラメータを考慮して最適化しなければならない．

ところで，暗号鍵の変更周期の最も短い暗号は，ヒットごとに鍵をランダムに変更するバーナム暗号である．このバーナム暗号の乱数鍵を自動的に生成するためには，小さなサイズ（例えば，64 ビット）の初期値のみを与えておいて暗号文をフィードバックさせる方法などが用いられている．このフィードバックの標準的な手法として，CBC (cipher block chaining) モード，CFB (cipher feedback) モード，OFB (output feedback) モードが推奨されている[16]．

5. あとがき

電子送金，電子郵便など高価値な情報を通信，記録するシステムが普及しつつある現在，システムの安全性を向上させる一つの対策として暗号が広く用いられようとしている．特に，暗号による認証技術は情報の付加価値を生む技術であり，その需要と市場は大きいと思われる．暗号の応用分野であるディジタル署名と暗号鍵管理技術は，今後もますます研究と実用化が進むであろう．

参考文献

1) Akl, S. G.: Digital Signatures: A Tutorial Survey, IEEE Computer (Feb. 1983).
2) Cohen, H. and Lenstra, H.W.: Primality Testing and Jacobi Sums, Math. Instituut Univ. van Amsterdam Netherland (Oct. 1982).
3) Davida, G. I.: Chosen Signature Cryptoanalysis of the RSA(MIT) Public Key Cryptosystem,

TR-CS-82-2, Univ. of Wisconsin (Oct. 1982).
4) Davis, D. W.: Applying the RSA Digital Signature to Electronic Mail, IEEE Computer (Feb. 1983).
5) Denning, D. E.: Protecting Public Keys and Signature Keys, IEEE Computer (Feb. 1983).
6) Denning, D. E.: Signature Protocols for RSA and Other Public-Key Cryptosystem, CSD-TR-419, Purdue University (1983).
7) Diffie, W. and Hellman, M.: New Directions in Cryptography, IEEE Trans. IT-22 (Nov. 1976).
8) 小山謙二：RSA 公開鍵暗号法のマスタ鍵，信学論(D)，No. 2(1982).
9) 小山謙二：マスター鍵による同報通信の暗号方式，信学論(D)，No. 9(1982).
10) 小山謙二：認証とディジタル署名，情報処理，Vol. 24, No. 7(1983).
11) 小山謙二：Rabin の公開鍵暗号法のマスタ鍵，信学論(D)，No. 12 (1983).
12) 小山謙二：公開鍵暗号による高速かつ安全なディジタル署名法，信学論(D)，No.3(1984).
13) 小山謙二：Cryptographic Key Sharing Methods for Multi-Groups and Security Analysis, 信学論(E)，E66, No. 1 (1983).
14) Matyas, S. M. and Meyer, C. H.: Generation, Distribution and Installation of Cryptographic Keys, IBM Sys. J., Vol. 17, No. 2 (1978).
15) Merkle, R. and Hellman, M.: Hiding Information and Receipts in Trapdoor Knapsacks, IEEE Trans. IT-24(1978).
16) National Bureau of Standard: Data Encryption Standard Federal Information Processing Standards, Pub. 46 (1977), Pub. 81 (1980).
17) Rabin, M. O.: Digitalized Signatures and Public-Key Functions as Intractable as Factorization, TECH. Rep. MIT/LCS/TR-212 MIT Lab. Comput. Sci. (1979).
18) Rivest, R., Shamir, and Adleman, L.: A Method of Obtaining Digital Siganatures and Public-Key Cryptosystems, CACM, Vol. 21, No. 2(1978).
19) Rivest, R.: Remarks on a Proposed Cryptoanalytic Attack on the MIT Public-Key Cryptosystem, Cryptologia (Jan. 1, 1978).
20) Shamir, A.: How to Share a Secret, CACM, Vol. 22, No. 11(1979).
21) Shamir, A.: A Polynomial Time Algorithm for Breaking the Basic Merkle-Hellman Cryptosystem, Proc. of 23 Ann. Sympo. on FOCS (1982).
22) Shannon, C. E.: Communication Theory of Secrecy System, Bell Syst. Tech. J. (1949).
23) Test Key, Document No. ISO/TC68/SC2/WG2, N 80 (Jan. 1982).

(昭和59年2月3日受付)