多重署名に適した公開鍵暗号系†

板倉和治†† 中村勝洋†††

Rivest らが発表した公開鍵暗号方式は，公開鍵機能と署名機能を備えたすぐれた方式である．しかし，査閲署名，承認署名のように一つの文書に多重に署名をする際に，異なる法 (modulo) による演算を多重に実行すると演算のたびにメッセージ長が増加し，演算単位であるブロックの数が増えていくという好ましくない点がある．本論文ではオフィス内の下の地位の人間から順に署名をする限り，多重に署名を行ってもメッセージ長やブロック数が増えることなく，かつ地位の変動があったとしても公開されている公開鍵には影響を与えないで，変動のあった個人のもっている非公開鍵のみの容易な変更で済むシステムを検討し，提案している．このシステムでは Rivest らの方法を直接的に拡張し，オフィスシステムに適合した多重署名機能を有する形で用いているが，パラメータの大きさ等を考慮に入れれば実際のシステムに適用しても十分実用可能であると考えられる．

1. まえがき

近年，オフィスオートメーションの重要な要素として文書情報の電子化がクローズアップされてきている．その際の問題点の一つにセキュリティ対策があり，その一環として電子化文書情報に対し暗号化やディジタル署名等を行う方法が検討され始めている．

一方，1976年米国の Stanford 大学の Diffie と Helman によって発表された公開鍵暗号系の概念は，従来の慣用暗号系においてあたりまえのことと考えられ，かつ最大の問題点であった鍵の配送を不要にするという点で，実に画期的なものであった[1]．この概念を具体的に実現する方法の一つを，米国 M.I.T. の Rivest, Shamir, Adleman の三氏が1977年に開発した[2),3)]．この RSA 法と呼ばれる方法は Helman らの考えた概念をほぼ完全に実現するきわめて理想に近いものであり，暗号機能に加えて署名機能をもつという点で，電子化文書情報のセキュリティ対策に適しているといえる．

しかし，オフィスの文書には文書作成者の署名だけでなく，査閲者，承認者等の署名が不可欠であることが多い．このような多重署名を考えたとき，従来の RSA 法では不可能ではないが，演算速度やシステムの単純さを考えたとき，必ずしも満足できない．

そこで本論文では RSA 法の考え方を拡張し，多重署名に適した暗号システムを構成する手法について述べる．

まず2章で RSA 法について簡単に触れたあと，RSA 法をオフィス内通信システムに用いる際の方式ならびに問題点，つまり多重署名への不適合性について述べ，3章において RSA 法の拡張ならびに，それを用いた多重署名／暗号システムおよび最適なシステムパラメータの選定法について述べる．

本稿で提案する手法は，電子化された文書情報システムのセキュリティを実現する上で，一つの実用的な解を与えるものと考えられる．

2. オフィス内通信システムへの公開鍵暗号化の利用

2.1 多重署名の必要性

オートメーション化されたオフィスでは文書情報の大部分は紙の上に存在するのではなく，電気信号によって表現されて通信回線上を移動したり，メモリやファイル上に貯えられるであろう．このような文書情報は冗長な情報が少なくコンパクトであるかわりに，誰が書いても等しい論理シンボル列となるし，また，空間的にはるかに隔たった場所から時間的に瞬時に手にいれることができる．このようなオフィスシステムでは次の危険性に対する対策が必要となる．

（1） 通信回線上またはファイル上にある情報源に対する不正なアクセス．

（2） 他人をかたってニセの文書情報を配布する．

（3） 自分が作成した文書情報であるにもかかわらず，あとになってから自分が作成したことを否定

† A Public-key Cryptosystem Suitable for Digital Multi-signatures by KAZUHARU ITAKURA (Printer Division, Nippon Electric Co., Ltd.) and KATSUHIRO NAKAMURA (C & C Systems Research Laboratories, Nippon Electric Co., Ltd.)

†† 日本電気(株) プリンタ事業部
††† 日本電気(株) C & C システム研究所

する.

以上の脅威への対策として

(a) 資格をもった人のみが復元できる暗号化を文書情報にほどこすこと.

(b) 本人のみが作成でき，かつ文書を正当に入手した人が署名者本人を確認できる署名を文書と一体化した形で文書に添付すること.

の2点が有効である.

ところでオフィスで実際に取り扱われる文書は，個人から個人への手紙のようなものは少なく，組織から複数の人間を対象として配布されるものが多い．この場合，対策(b)の署名機能は作成者本人の署名だけでなく，査閲者，承認者等の上位職者の署名が一つの文書の上に順序性をもって重ねて実行できるものである必要がある（これを多重署名と呼ぶ）．このような署名の必要性は実際のオフィスでは文書作成者の署名よりもむしろ承認者の署名のほうが重要な場合が多いことを考えれば自明であろう.

2.2 RSA 法の概要

RSA 法の原理は次の定理による[2),3)].

<定理>

二つの素数 p, q の積を n とし，$(p-1)\cdot(q-1)$ と互いに素で $(p-1)\cdot(q-1)$ より小さい整数を e とするとき，$n-1$ より小さい任意の整数 M において

$$M^{ed}=M_{\mathrm{mod}.n}$$

が成立するための十分条件は $ed=1_{\mathrm{mod}.(p-1)(q-1)}$ である：

RSA 法では (e,n) を公開鍵，d を非公開鍵とし d は復元を行う人が秘密に保存する．公開鍵から d を計算するには n を素因数分解しなければならないが，n が大きな数の場合は素因数分解はきわめて困難である.

(1) 暗号化操作

数値化された平文を $M(0\leqq M\leqq n_b-1)$ とすると暗号化操作は下式による.

$$C=M^{e_b}\bmod n_b \qquad (1)$$

ただし，e_b, n_b は受信者Bの公開鍵.

(2) 復元操作

暗号文 C から平文 M を得るには下記の操作を行う.

$$C^{d_b}\bmod n_b=M^{e_b d_b}\bmod n_b=M \qquad (2)$$

ただし d_b は受信者Bの非公開鍵.

上式が成り立つことは前述の定理より明らかである.

(3) ディジタル署名とメッセージ認証

数値化された平文を $M(0\leqq M\leqq n_a-1)$ とする．送信者Aは自分の非公開鍵 d_a を用いて平文 M に(2)式の操作を行い，Aしか作成することのできない署名文 S を得る.

$$S=M^{d_a}\bmod n_a$$

受信者Bは S をAの公開鍵 e_a を用いて(1)式の操作を行い平文 M を得る.

$$S^{e_a}\bmod n_a=M^{d_a e_a}\bmod n_a=M$$

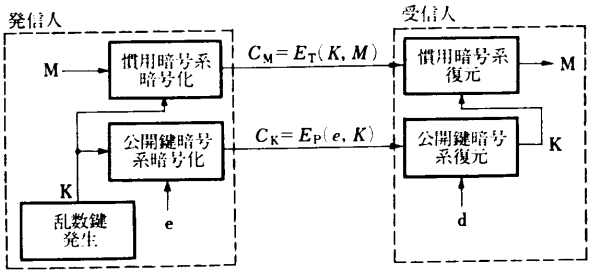
平文 M が意味の通る文になれば，S は確かにAの作成した文である．なお，S を受信者に送るとき，必要ならば(1),(2)で述べた暗号化／復元の手段をとることができる.

2.3 RSA 法による多重署名の問題点

RSA 法において解読に対する十分な安全性を保つには，n として十進で200桁程度の値をとることが必要であるとされており，暗号化，復元に要する計算時間は，専用のハードウェアを開発したとしてもなかなか実用的に十分な速度にはならないと見られている.

公開鍵暗号方式の利点を生かし，かつ実用的な速度の得られる方式として**図1**に示す複合方式[7)]がある．この方式では平文 M をたとえばDESアルゴリズム[5)]等の高速に演算が可能な慣用暗号系を用いて暗号化し，その鍵 K は公開鍵暗号系を用いて暗号化する（鍵 K は使い捨てとする）．慣用暗号系の鍵は一般にそう長くはないので，十分200桁以内の数値で表現できる．したがって処理速度の遅い公開鍵暗号化の1ブロックの演算だけで済むので，十分実用的な時間で暗号化が完了する．復元の場合も同様である.

上述の複合方式を使って鍵 K に RSA 法によって



E_T：慣用暗号方式による暗号化
E_P：公開鍵暗号方式による暗号化

図1 慣用暗号系と公開鍵暗号系の複合暗号化方式
Fig. 1 Mixed cryptographic system with conventional and public-key cryptography.

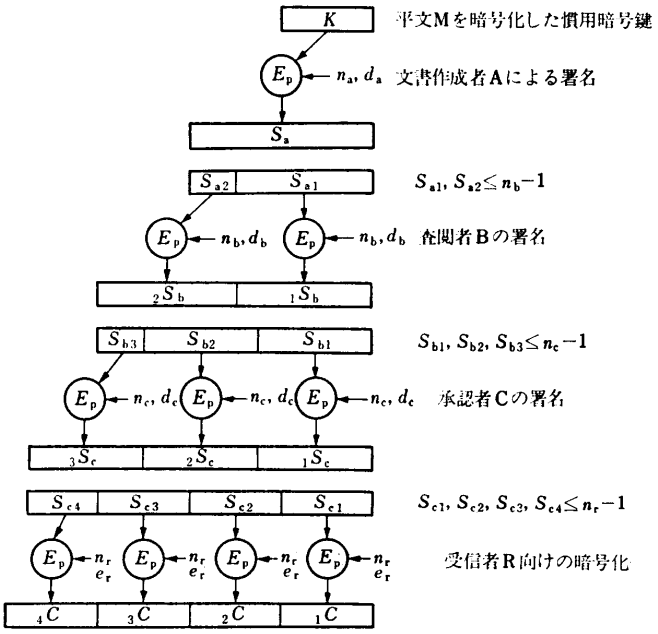


図 2 多重署名によってブロック数が増加する例
Fig. 2 Example in which the number of message blocks is increased through multi-signature.

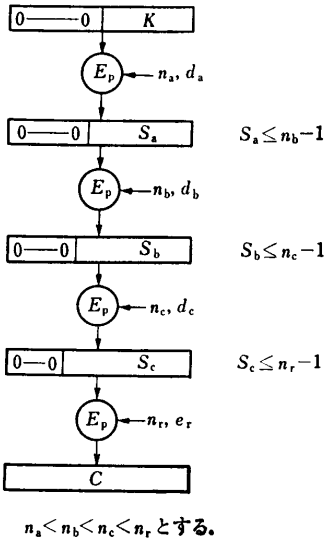


図 3 多重署名を行ってもブロック数が変わらない例
Fig. 3 Example in which the number of message blocks is constant through multi-signature.

多重署名をすることを考えてみよう（**図 2**）.

平文を暗号化した慣用暗号系の鍵 K に文書作成者 A が署名を行う.

$$S_a = K^{d_a} \bmod n_a$$

この演算の結果，署名文 S_a は最大 (n_a-1) までの値をとりうることになる．もし第2の署名者 B の n_b が n_a より小さければ，S_a を (n_b-1) より小さい値のブロックに分割しないと mod. n_b の演算ができない．したがって S_a を S_{a_1} と S_{a_2} の2ブロックにわけ，2回演算を行うことになる．このように，もし $n_a > n_b > n_c > n_r$ であるとすれば，**図 2** に示したようにどんどん演算回数は増えていき署名付の暗号文 C ができあがるまでに計 10 回の復元／暗号化演算を行わなければならない．上位署名者へ下位職者の署名文書をまわすとき，保全のため上位署名者の公開鍵で署名文書をさらに暗号化する場合には，演算回数はさらに増加する.

このようなシステムでは再び RSA 法の演算速度が遅いという点が問題となってくる可能性がある．また，演算をする度にブロック数とブロック長が変化するのでシステムはより複雑になる.

しかし，もし $n_a < n_b < n_c < n_r$ が成立していれば**図 3** に示すようにブロック数を何ら増やすことなく，多重に復元／暗号化の演算を重ねてゆくことができる．最後の署名付暗号文ができあがるまでの演算回数は 4 回で，図2の場合のおよそ半分以下の時間で済むことがわかる．加えて演算によってブロック数もブロック長も変化しないことから，アルゴリズムが単純となる.

しかし上位の署名を行う上位職者が下位職者より常に大きい n をもっていなければならないとする制限は，現実的にはこのようなシステムを実現不可能にすると思われる．たとえば入社時に鍵の組 (n, e, d) を与えるとして，年々 n の値を前年の最小の n の値より小さくしていったとしても，勤続年数の長い社員が必ずしも上位職にあるとは限らないので，結局，人事移動の度に多数の社員の鍵の変更が必要となってしまう．これは暗号システムに大混乱をきたすであろう.

3. 多重署名に適する公開鍵暗号方式

3.1 RSA 法の拡張

Rivest らの方法では二つの大きな素数の積である n を逆に素因数に分解することが困難であることを，

一方向性関数として利用している．これを拡張してnを三つの素数p,q,rの積とし，第3の素数rを公開しても何ら一方向性は失われない．そこでRSA法を3素数を用いる形に直接的に拡張する．

（1） 鍵の生成

三つの素数p,q,rを選びそれらの積をnとする．

$$n=p\cdot q\cdot r=n_0\cdot r \quad (p,q,r\neq 1) \tag{3}$$

$(p-1)\cdot(q-1)\cdot(r-1)$と互いに素で，かつ$(p-1)\cdot(q-1)\cdot(r-1)$より小なる数を選び$e$とする．

$$\text{gcd.}^{\star}\ (e,(p-1)\cdot(q-1)\cdot(r-1))=1 \tag{4}$$

mod.$(p-1)\cdot(q-1)\cdot(r-1)$において$e$の逆数を$d$とする．

$$e\cdot d=1_{\text{mod.}(p-1)\cdot(q-1)\cdot(r-1)} \tag{5}$$

このようにして作った(e,n_0,r)を公開鍵，(d,p,q)を非公開鍵とする．

（2） 暗号化操作

平文Mが$0\leqq M\leqq n-1$を満足していれば，Mは下式により暗号文Cとなる．

$$C=M^{e}_{\text{mod.}n} \tag{6}$$

（3） 復元操作と証明

暗号文Cから平文Mを得るには下記の操作を行う．

$$C^{d}_{\text{mod.}n}=M \tag{7}$$

以下に(7)式を証明する．

(5)式より適当な整数kに対して下式が成り立つ．

$$M^{e\cdot d}=M^{1+k(p-1)}=M\cdot(M^{p-1})^{k}$$

しかるに，Mがpの整数倍でないとき，フェルマの小定理により

$$M^{p-1}=1_{\text{mod.}p}$$

$$\therefore\quad M^{e\cdot d}=M_{\text{mod.}p}$$

また，Mがpの整数倍のとき

$$M^{e\cdot d}=M=0_{\text{mod.}p}$$

したがって$0\leqq M\leqq n-1$の範囲において

$$M^{e\cdot d}=M_{\text{mod.}p} \tag{8}$$

q,rについても同様にして(9)，(10)式が成り立つ．

$$M^{e\cdot d}=M_{\text{mod.}q} \tag{9}$$

$$M^{e\cdot d}=M_{\text{mod.}r} \tag{10}$$

p,q,rは素数であるから，(8)，(9)，(10)式より

$$M^{e\cdot d}=M_{\text{mod.}p\cdot q\cdot r}=M_{\text{mod.}n} \tag{11}$$

(証明完)

（4） 署名とメッセージ認証

平文Mが$0\leqq M\leqq n-1$を満足していれば，Mは下式の操作により鍵dをもっている者にしか作ることのできない署名文Sとなる．

$$S=M^{d}_{\text{mod.}n} \tag{12}$$

署名文Sから平文Mを得るには公開鍵eを用いて下式の操作を行う．

$$S^{e}_{\text{mod.}n}=M \tag{13}$$

(13)式が成立することは(11)式より自明である．

以上よりnを三つの素数の積とする方法においても，暗号化→復元，署名→復元がRSA法とまったく同様に成立することが証明された．この方式を拡張RSA法と呼ぶことにする．

3.2 拡張 RSA 法の問題点とその対策

nが3素数以上の積である場合，nが完全擬素数(絶対擬素数ともいう)となる可能性がある[8]．もしnが完全擬素数であると後述する方法によって秘密の鍵を知らなくても簡単に暗号文を解読することができる．したがって拡張RSA方式では鍵の組を決めるときにあらかじめnが完全擬素数とはならないように配慮する必要がある．

<定義> 完全擬素数[8]

gcd.$(M,n)=1$である$n-1$以下の任意の整数Mに対して

$$M^{n-1}=1 \ \text{mod.}n$$

を満足する素数でない整数nを完全擬素数という．

もし拡張RSA方式においてnが完全擬素数でありかつeがmod.$(n-1)$で逆元uをもつならば適当な整数kに対して下式が成り立つ．

$$eu=1+k(n-1)$$

暗号文$C=M^{e}$とすると下式により解読が可能となる．

$$C^{u}=M^{eu}=M^{1+k(n-1)}=M\cdot(M^{n-1})^{k}=M_{\text{mod.}n}$$

nが完全擬素数であるかどうかをチェックすることができれば，そのような鍵の組は初めから使用しないようにすることができる．完全擬素数に関する下記の定理を用いれば，nが完全擬素数であるかどうかを簡単にチェックできる．

<定理> (証明は付録1)

nが完全擬素数であるための必要十分条件は，nの各素因数p_iに対して(p_i-1)が$(n-1)$の約数であることである．

本定理によれば，拡張RSA方式においては$(n-1)$が$(p-1),(q-1),(r-1)$のすべてによって割り切れるとき，nは完全擬素数となるのでそのようなp,q,rの組は廃棄すればよい．

---

* gcd. は最大公約数の意．

3.3 拡張 RSA 法を用いた多重署名／暗号システム

3.1 節で証明した拡張 RSA 法を用いると上位職者が常に下位職者より大きな n をもち，かつ受信者が常に発信者より大きな n をもつというシステムを作ることができる．このようなシステムにおいては上位職者が下位職者の署名文にさらに署名をする場合とか，署名文を受信者あてに暗号化する場合に，演算の単位となるブロックの数や長さを変化させない図3に示した処理が可能となる．

（1） 鍵の生成

社員は入社時に公開鍵 (e, n_0, r_i) と非公開鍵，(d_i, p, q) を与えられる（r_i は入社時の職位を示す素数，n_0 は p と q の積である）．拡張 RSA 法では e を $(p-1)\cdot(q-1)\cdot(r_i-1)$ と互いに素で，かつ $(p-1)\cdot(q-1)\cdot(r_i-1)$ より小さい任意の数としたが，本システムでは e を $(p-1)\cdot(q-1)$ と互いに素で，かつ (r_i-1) の最大値より大きくかつ $(p-1)\cdot(q-1)$ より小さい任意の素数とする．この条件で選ばれた e は，任意の素数 r_i に対して拡張 RSA 法の条件である(4)式を満足することは自明である．

r_i は職位を表す数として使用される．したがって職位が変更になったとき，(3)，(4)，(5)式にしたがって，n_i, e, d_i を再計算しなければならないが，eに関しては(4)式は常に満足するので，n_i, d_i のみを再計算すればよい．

$$n_i = n_0 \cdot r_i$$

$$d_i \cdot e = 1 \bmod (p-1)\cdot(q-1)\cdot(r_i-1)$$

r_i は上位職者が下位職者より常に大きい $n = n_0 \cdot r_i$ をもつという条件を満足させるために使用される．このような条件をもつ r_i の選び方については3.3節でくわしく述べる．

また，すべての社員は r_i とは別に受信用の特別職位 r_t をもっている．r_t はすべての社員に共通の値で，最高の職位の上に位置する職位数である．r_t は地位の高い人の署名した文書を地位の低い人に暗号化して送る場合に必要となる．

すべての職位に対して $n_i = n_0 \cdot r_i$ が完全擬素数となる危険性をさけるため，鍵を生成したときにすべての職位数 r_i に対して $n_i - 1$ が $p-1$, $q-1$, r_i-1 の公倍数となっていないことをあらかじめ調べておく必要がある．n_i が完全擬素数となりうる鍵の組は廃棄され使用しない．r_i の総数は実際のシステムでは 10～20 程度であろうから，このチェックは比較的容易である．

（2） 職位数の決め方

暗号システム内の全メンバのもつ $n_0 = p \cdot q$ の集合を N_0 とし，N_0 内の任意の数と r_i との積を簡単のため $n_0^i \cdot r_i$ と表したとき，

$$n_0^0 < n_0^1 \cdot r_1 < n_0^2 \cdot r_2 < \cdots < n_0^t \cdot r_t < n_0^t \cdot r_t$$

となるように $r_1, r_2, \cdots, r_t, r_t$ を定める．ただし，r_tは最上位職の職位数，r_t は受信用の特別職位数である．

（3） 文書の署名／暗号化

本システムでは文書の暗号化は高速の演算が可能な慣用暗号方式によって行う．したがって以下に述べる署名／暗号化とは慣用暗号鍵に対する操作を意味している．

（4） 署名と復元

署名者の公開鍵を (e, n_0, r_i) 非公開鍵を (d_i, p, q) とするとき，署名は下記の操作を行う．

$$S = M^{d_i} \bmod n_0 \cdot r_i$$

また，この署名者の職位数より大きな職位数をもつ人は上記の S に対してさらに署名が可能である．署名文 S の復元は下記の操作を行う．

$$S^e \bmod n_0 \cdot r_i = M$$

（5） 暗号化と復元

受信者の公開鍵を (e, n_0, r_i) 非公開鍵を (d_i, p, q) とするとき，暗号化は下記の操作を行う．

$$C = M^e \bmod n_0 \cdot r_t$$

ただし r_t は(2)で説明した受信用の特別職位数である．r_t は他のいかなる職位数より上のレベルにあるので，暗号化の対象となる M がいかなる職位の人が署名した署名文であろうとも暗号化演算が可能である．暗号文 C の復元には下記の操作を行う．

$$C^{d_t} \bmod n_0 \cdot r_t = M$$

ただし，d_t は r_tに対応する受信専用の解読鍵で下式により求められる．

$$e \cdot d_t = 1 \bmod (p-1)\cdot(q-1)\cdot(r_t-1)$$

3.4 最適な p, q, r の決め方に関する考察

暗号化／復元演算の法となる数 n は p, q, r の積である．解読に対して十分な強度をもつには，nは 200 桁程度の数であることが必要であるとされているが，拡張 RSA 法では r は公開されているので，$n_0 = p \cdot q$ が 200 桁程度であることが必要である．r として大きな数が使用されると n の桁数は増加するが，それは暗号の強度には何ら寄与しないばかりか暗号化／復元の演算時間をいたずらに増加させるだけである．したがって職位数 r はなるべく小さな数を選ぶべきである．

（1） 最適な r の決め方

暗号システム内の全メンバのもつ $n_0=p\cdot q$ の集合を N_0 とし，N_0 内の任意の数と r_i との積を簡単のため $n_0^i\cdot r_i$ と表したとき，$r_1, r_2, \cdots, r_i, \cdots$ は下式を満足しなければならない．

$$n_0^{i-1}\cdot r_{i-1}<n_0^i\cdot r_i \quad i=1,2,\cdots, \quad r_0=1 \tag{14}$$

N_0 内の任意の数 n_0^i の値の範囲を下式で表す．

$$2^{l-\frac{\Delta l}{2}}<n_0^i<2^{l+\frac{\Delta l}{2}} \tag{15}$$

(14)式に(15)式の条件をいれると

$$2^{l+\frac{\Delta l}{2}}\cdot r_{i-1}<2^{l-\frac{\Delta l}{2}}\cdot r_i$$

$$\therefore \quad 2^{\Delta l}\cdot r_{i-1}<r_i \quad \text{ただし} \quad r_0=1 \tag{16}$$

したがって最適な r としては(16)式を満足する最も小さな素数列を選べばよい．また，(16)式から明らかなようになるべく小さな素数列を r として選ぶためには n_0 の分布範囲が狭いことが望ましい．

（2） コンパクトな分布の n_0 の決め方

二つの素数 p, q の積である n_0 の集合をなるべく狭い範囲に集中させるという要求に対して下記の2点を考慮する必要がある．

① 二つの素数組 p, q を妥当な計算時間で決定できること．

② n_0 がある狭い範囲に集中していることが，暗号破りの手がかりとならないこと．

上記条件を満足する一つとして次の方法をあげる．

n_0 の分布の中心値を 2^l 近辺とするとき，まず $2\sim 2^{l/2}$ の範囲でランダムに一つの整数を選びその整数の近辺にある素数をさがす（ある整数が素数であるかどうかを判定するには，たとえば G. L. Miller の算法[4]を用いる）．このようにして一つの素数 p が決まったら，$2^l/p$ 近辺の素数に対して同様の素数判定を行い，最も $2^l/p$ に近い整数 q を求める．

この方法で n_0 の集合を決めた場合，n_0 の分布範囲がどの程度になるかについて以下に評価する．

素数分布定理によれば整数 x を越えない素数の数は近似的に下式で表される．

$$x/\ln x$$

そこで，$x=2^y$ とおき y に関する素数密度分布を $f(y)$ とすると，

$$f(y)=\frac{d}{dy}(x/\ln x)=\frac{d}{dy}(2^y/y\ln 2)$$

$$=2^y(y\ln 2-1)/y^2\ln 2\fallingdotseq 2^y/y \tag{17}$$

となる．

$2\sim 2^{l/2}$ の範囲でランダムに決めた素数を $p=2^a$，$2^l/p=2^{l-a}$ に最も近い素数を $q=2^b$ とする．(17)式の逆数が2のべき乗軸上での素数間隔であるので

$$|(l-a)-b|\leqq\frac{1}{2}(l-a)/2^{l-a} \tag{18}$$

$p\cdot q=2^{l\pm\frac{\Delta l}{2}}$ としたとき(18)式より

$$\Delta l/2=|l-(a+b)|\leqq\frac{1}{2}(l-a)/2^{l-a} \tag{19}$$

$1\leqq a\leqq l/2$ であるから(19)式の右辺は $a=l/2$ のとき最大となる．

$$(\Delta l/2)_{\max}=\frac{1}{2}\left(l-\frac{l}{2}\right)\Big/2^{l-\frac{l}{2}}=\frac{1}{4}l/2^{l/2} \tag{20}$$

(20)式で求められた値は素数密度分布が(15)式の上に完全に乗っているという仮定の上で正しい．実際には(17)式はばらつきをもった素数密度の平均的なカーブと考えねばならない．したがって $(\Delta l/2)_{\max}$ は(20)式で定められる上限より大きくなるだろう．しかし，$2^l/p$ 近辺の素数 q をさがすとき，ある一定範囲をさがしても素数が見つからなければ，p を求めなおすことができる．このようにすれば，(20)式もしくは(20)式より多少広い範囲内で n_0 を分布させることは可能であろう．

3.5 職位数列の例

下記の現実的な条件で，職位数として用いることのできる素数値を求めてみる．

条件；

$n_0=p\cdot q$ の桁数：10進200桁

暗号システム内のメンバ数：100万人

職位のレベル数：20レベル

$10^{200}\fallingdotseq 2^{660}$ であるから(20)式より

$$\Delta l_{\max}=\frac{1}{2}\cdot 660/2^{330}\fallingdotseq 7.5\times 10^{-98}$$

(16)式において $i=1$ とすると $2^{\Delta l}<r_1$

上式を満たす最も小さい素数として $r_1=2$ が得られる．再び(16)式において $i=2$ とすると $2^{\Delta l}\cdot 2<r_2$ 上式を満たす最も小さい素数として $r_2=3$ が得られる．以下同様に計算を行い職位数列として次の数列が得られる．2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71.

この例においては r の最大値は71となり，

$$n_{20}=n_0\cdot r_{20}\fallingdotseq 2^{660}\times 71\fallingdotseq 2^{667}$$

すなわち，職位数を導入したことによって暗号化／復元の演算の法はたかだか7ビット増加したにすぎない．なお，上記の Δl の値は素数密度分布が(18)式の上に完全にのっているとしたときの値であるが，もし

安全サイドに Δl を大きく見積もり，たとえば $10^5 \cdot \Delta l$ を新しい Δl としても，職位数列としては上記と同じものが選ばれる．また，p の値としては，2^{330} 以下の素数が選べるので，システム内のメンバ数100万人の n_0 の値は十分用意しうる．

4. むすび

本論文の方式によれば，本文を暗号化した慣用暗号系の鍵に多重に署名を重ねていっても，署名文のブロック長，ブロック数は不変となるので，演算時間の点で有利であるばかりでなく演算機構のアルゴリズムが単純化できる．これは演算機構のハードウェア化の点でも有利であろう．しかし，1文書情報について1ブロックだけの演算で済むのであるから，マイクロプロセサによる演算方式も十分実現性があると思われる．

本文を暗号化する慣用暗号系としては，高速のLSIがすでに入手できる点を考えると DES 方式[5] が有望であろう．DES を用いるならば，鍵は64ビットであるが，それに対して拡張 RSA 法で推奨される n は600ビット以上であり鍵だけを暗号化の対象とするのではもったいない．鍵以外に何を組みあわせて1ブロックとするかは今後の検討としたい．

なお，本論文は日本電気技術研修所における基幹技術研修でまとめた研修論文をさらにまとめなおしたものである．

謝辞 ご指導をいただいた加藤 C & C システム研究所長はじめ各指導講師の方々に深く感謝します．

また，査読者の方には完全擬素数に関する有益なご指摘を受けた．あわせて感謝いたします．

参考文献

1) Diffie, W. and Helman, M.: New Directions in Cryptography, *IEEE Trans. Inf. Theory*, IT-22, 6 pp. 644-654 (Nov. 1976).
2) Rivest, R.L., Shamir, A. and Adleman, L.: A Method for Obtaining Digital Signatures and Public-key Cryptosystems, *Comm. ACM*, Vol. 21, No. 2, pp. 120-126 (Feb. 1978).
3) Rivest, R.L., Shamir, A. and Adleman, L.: On Digital Signatures and Public-key Cryptosystems, IEEE International Symposium on Inform. Theory, p. 41 (Nov. 1977).
4) Miller, G.L.: Theory of Computing, Proc. Seventh Annual ACM Symposium, pp. 234-239 (1975).
5) National Bureau of Standards, U.S. Department of Commerce: Data Encryption Standard, Federal Information Processing Standard (FIPS) Publication 46 (Jan. 1977).
6) Kowalchuk, J. et al.: Communications Privacy: Integration of Public and Secret Key Cryptography, Proc. of NTC '80. pp. 49.1.1-1.5 (1980).
7) 郵政省電気通信政策局：ネットワーク化に伴なう諸問題の調査研究—データ保護手法の利用手引書— (1982.6).
8) 伊理正夫編：数と式と文の処理，岩波講座情報科学，Vol. 23，岩波書店，東京，pp. 4-5. (1981).

付録

<定理> （参考文献8) の5頁の問を参照)

gcd.$(M, n)=1$ である $n-1$ 以下の任意の整数 M に対して

$$M^{n-1}=1_{\mathrm{mod}.n} \rightleftarrows n-1=k_i(p_i-1)$$

ただし，p_i は n のすべての素因数，k_i は適当な整数．

<略証明>

(→)

$n=\prod p_i$ だから $M^{n-1}=1_{\mathrm{mod}.p_i}$

一方，フェルマの小定理により $M^{p_i-1}=1_{\mathrm{mod}.p_i}$

gcd.$(M, n)=1$ である任意の整数 M に対して上式が成立するので適当な整数 k_i を用いて

$$n-1=k_i(p_i-1)$$

となる．

(←)

フェルマの小定理により $M^{p_i-1}=1_{\mathrm{mod}.p_i}$ であるので $M^{n-1}=M^{k_i(p_i-1)}=(M^{p_i-1})^{k_i}=1_{\mathrm{mod}.p_i}$

p_i は素数だから $M^{n-1}=1_{\mathrm{mod}.\prod p_i}=1_{\mathrm{mod}.n}$

（証明完）

（昭和57年 9 月24日受付）
（昭和58年 1 月17日採録）