

ディオファントスの一次不定方程式に基づく公開鍵暗号系†

八木 沢 正 博††

公開鍵暗号系の実現化手法は、RSA 法を初めとして、これまでに多数提案されているが、実用化されているものは極めて少ない。ビット長の大きい演算回数が多いため、計算量が膨大になり、暗号化・復号化に時間がかかり過ぎることが主要因である。本論文でディオファントスの一次不定方程式に基づく公開鍵暗号系を提案する。本暗号系の暗号化・復号化では扱うビット長、演算量が小さくなる。その結果 RSA 法と比べて演算量がかなり小さくなる利点がある。また、デジタル署名の実現も可能である。系の構成は、次のようになる。素数 P_i ($i=0, \dots, n$)、正整数係数 k_i を用いて $b_i = k_i P_0 P_1 \dots P_{i-1}$ ($i=1, \dots, n$) を生成し、 $b_1 P_1 + \dots + b_n P_n < R$ なる素数 R および R と互いに素な整数 β を選び、 $a_i \equiv b_i \beta \pmod{R}$ ($i=1, \dots, n$) を生成する。この際、 $a_1 P_1 + \dots + a_n P_n < R$ となるように、 k_i, β, R を選定する。正整数 a_i を係数、 C を与えられた整数、 x_i を未知数とするディオファントスの一次不定方程式 $C = a_1 x_1 + \dots + a_n x_n$ を利用して、 $0 \leq x_i < P_i$ ($i=1, \dots, n$) なる x_i を平文、 C を暗号文とする暗号系を構築する。復号化では、 $0 \leq C < R$ の範囲の任意の C に対しては、 $0 \leq x_i < P_i$ ($i=1, \dots, n-1$)、 $-(n-1) * o(P_n) < o(x_n) < n * o(P_n)$ の範囲に平文を拡張することにより、デジタル署名が可能になる。

1. はじめに

1976 年に公開鍵暗号系が提案されて以来、RSA 法¹⁾を代表例として、いくつかの実現手法が発表されている。RSA 法では、素因数分解の難しさに基づいているが、本論文では正整数係数 a_i ($i=1, \dots, n$) および正整数 C と n 個の未知数 x_i ($i=1, \dots, n$) から成るディオファントスの一次不定方程式

$$C = a_1 x_1 + \dots + a_n x_n \quad (1-1)$$

に基づいた公開鍵暗号系を提案する。 n 個の未知数 x_i ($i=1, \dots, n$) は、すべて自然数として、平文 $X = (x_1, \dots, x_n)$ に対応し、公開されている n 個の正整数係数 a_i ($i=1, \dots, n$) から、暗号文 C を

$$C = a_1 x_1 + \dots + a_n x_n$$

により生成し、送信する。 C を受信したものは、 C, a_i ($i=1, \dots, n$) の値から、平文 x_i ($i=1, \dots, n$) を求めることになるが、これはディオファントスの一次不定方程式であり、多項式時間で自然数解を求めることは、計算量の上から非常に困難である。しかし、正整数係数 a_i ($i=1, \dots, n$) を生成する上で、あるしかけを導入することにより容易に、上記不定方程式を解くことが可能となる。このしかけを知らなければ、計算量の上から、平文 x_i ($i=1, \dots, n$) を復号することは非常に困難となる。本暗号系と形が似ている暗号系に 0-1 ナップザック型暗号系²⁾があるが、平文に相当する 2 進

ベクトルを求める問題である。この暗号系はシャミール³⁾によって解読されている。しかし、本暗号系では、2 進ベクトルの代わりに、ある範囲の正整数を要素としたベクトルを考えているために、あるしかけを知らなければ計算量の上からは、0-1 ナップザック問題より、かなり困難な問題となる。

2. 暗号系の生成

2.1 暗号化手順

$$P_0 = 1 \quad (2-1)$$

$$P_i \text{ は素数 } (i=1, \dots, n) \quad (2-2)$$

$$o(P_1) = o(P_2) = \dots = o(P_n) = A \quad (2-3)$$

A は正定数、 b_i ($i=1, \dots, n$) を、次のように生成する。

$$b_1 = k_1 P_0 \quad (2-4 a)$$

$$b_2 = k_2 P_0 P_1 \quad (2-4 b)$$

⋮

$$b_n = k_n P_0 P_1 \dots P_{n-1} \quad (2-4 c)$$

ここで、 k_i ($i=1, \dots, n$) は

$$o(k_1) = A^{n-1} \quad (2-5 a)$$

$$o(k_2) = A^{n-2} \quad (2-5 b)$$

⋮

$$o(k_{n-1}) = A \quad (2-5 c)$$

$$k_n = 1 \quad (2-5 d)$$

のように選ぶ。

したがって、 b_i の大きさは

$$o(b_1) = o(b_2) = \dots = o(b_n) = A^{n-1} \quad (2-6)$$

となる。

† A Public-key Cryptosystem Based on Diophantine Equation
by MASAHIRO YAGISAWA (Showa Engineering Corporation).

†† 昭和エンジニアリング(株)

平文 x_i ($i=1, \dots, n$) の定義域を次のように定める.

α は正整数

$$0 \leq x_i < P_{\min} \quad (2-7)$$

$$P_{\min} \leq \min_{0 < i < n} P_i - \alpha \quad (2-8)$$

$$d \nmid b_1 P_1 + \dots + b_n P_n < R \quad (2-9)$$

なる素数 R を選び, R と互いに素な正整数 β を次のように選ぶ.

(2-4 a) ~ (2-4 c) 式の b_i を β, R でモード変換したものを a_i とする.

$$a_i \equiv \beta b_i \pmod{R} \quad (2-10)$$

この時,

$$0 < a_i < b_i < n A^* = o(R) \quad (2-11)$$

$$o(a_i) \leq A^{*-1} \quad (2-12)$$

$$(i=1, \dots, n)$$

となるように, LLL のアルゴリズム⁵⁾を用いて, β, R を選ぶ.

つまり, 次の基底ベクトルをもつ $n+1$ 次元の整数ラティスを構成する.

$$v_1 = (R, 0, \dots, 0, 0) \quad (2-13 a)$$

$$v_2 = (0, R, \dots, 0, 0) \quad (2-13 b)$$

$\vdots$

$$v_n = (0, 0, \dots, R, 0) \quad (2-13 c)$$

$$v_{n+1} = (b_1, b_2, \dots, b_n, 1) \quad (2-13 d)$$

次に, このラティスで最も短い, 要素が正のベクトル v を見つける.

$$v = (\beta b_1 - l_1 R, \beta b_2 - l_2 R, \dots, \beta b_n - l_n R, \beta) \quad (2-14)$$

l_i ($i=1, \dots, n$) は整数である.

v を見つけるのに必要な演算時間は,

$$o(n^6 (\log R)^3) \quad (2-15)$$

である. 実際には, 最短なベクトルを求める必要はなく, (2-11), (2-12) 式を満たす a_i が求まれば十分である. また, R の値は (2-9) 式を満たす素数であれば任意に選べるので, β, R の候補は多数存在すると思われる.

P_i は秘密にするため, x_i の定義域を明確に公開することはできないが, $P_{\min}$ を公開する.

パラメータのサイズとして, 次のサイズを推奨する.

$$n=5 \quad (2-16)$$

$$o(A)=10^{30} \quad (2-17)$$

$$o(R)=5 \cdot 10^{150} \quad (2-18)$$

$$o(a_i)=o(b_i)=10^{120} \quad (i=1, \dots, n) \quad (2-19)$$

$$o(P_{\min})=10^{30} \quad (2-20)$$

公開する暗号鍵 K_E は,

$$K_E = [a_i \ (i=1, \dots, n); P_{\min}] \quad (2-21)$$

である.

暗号化に要する計算量は, 5 個の乗算と 4 個の加算のみである. K_E が必要とする容量は 2260 bit となる.

平文 x_i ($i=1, \dots, n$) を送信しようとするものは, 公開されている a_i から,

$$C = a_1 x_1 + \dots + a_n x_n \quad (2-22)$$

を計算し, C のみを送信する.

2.2 復号化手順

正規の受信者が C を受信すると, β^{-1} を用いて C' を求める.

$$C' \equiv C \beta^{-1} \pmod{R} \quad (2-23)$$

$$\equiv (a_1 x_1 + \dots + a_n x_n) \beta^{-1} \pmod{R}$$

$$\equiv b_1 x_1 + \dots + b_n x_n \pmod{R}$$

$$= b_1 x_1 + \dots + b_n x_n \quad (2-24)$$

$$\equiv C'' \quad (2-25)$$

したがって,

$$C'' \pmod{P_1} \equiv b_1 x_1 \equiv k_1 x_1 \pmod{P_1} \quad (2-26)$$

$$C'' k_1^{-1} \pmod{P_1} \equiv x_1 \quad (2-27)$$

$$C'' - b_1 x_1 \pmod{P_2} \equiv k_2 P_1 x_2 \pmod{P_2} \quad (2-28)$$

$$(C'' - b_1 x_1) k_2^{-1} P_1^{-1} \pmod{P_2} \equiv x_2 \quad (2-29)$$

以下同様にして, x_i ($i=1, \dots, n-1$) を求めることができる.

$$x_i b_i \equiv C'' - b_1 x_1 - \dots - b_{i-1} x_{i-1} \pmod{P_i} \quad (2-30)$$

だから,

$$x_i \equiv (C'' - b_1 x_1 - \dots - b_{i-1} x_{i-1}) k_i^{-1} P_1^{-1} \dots P_{i-1}^{-1} \pmod{P_i} \quad (2-31)$$

最後に,

$$x_n = (C'' - b_1 x_1 - \dots - b_{n-1} x_{n-1}) / b_n \quad (2-32)$$

より, x_n を求める.

復号化鍵 K_D は,

$$K_D = [\beta; R; b_i \ (i=1, \dots, n); P_i \ (i=1, \dots, n)] \quad (2-33)$$

であるが, 各 b_i を公開されている a_i の値から求めることも可能である.

(2-16) ~ (2-20) 式のパラメータを採用すると, 復号化に必要な計算量は, R を法とするモジュラ乗算 1 個, P_i を法とするモジュラ乗算 6 個, 4 個の減算, 1 個の除算のみである.

K_D が必要とする容量は 3595 bit である.

(2-32) 式の右辺が整数であることの証明

$$b_n = k_n P_0 P_1 \dots P_{n-1} = P_1 \dots P_{n-1} \quad (2-34)$$

であるから、(2-32)式の分子が $P_1 \cdots P_{n-1}$ の倍数であることを示せば十分である。

$$\text{分子} = L = C'' - b_1 x_1 - \cdots - b_{n-1} x_{n-1} \quad (2-35)$$

両辺に $\text{mod } P_j$ 演算を施すと、

$$L \text{ mod } P_j \equiv C'' - b_1 x_1 - \cdots - b_j x_j \text{ mod } P_j \quad (2-36)$$

(2-30)式より、

$$\equiv 0 \text{ mod } P_j \quad (j=1, \dots, n-1) \quad (2-37)$$

(2-32)式が整数であることが示された。

(証明おわり)

(2-27)～(2-32)式で与えられる x_i を(2-24)式に代入することにより C'' が得られることは、次のように容易に分かる。

$$\begin{aligned} & b_1 x_1 + \cdots + b_{n-1} x_{n-1} + b_n x_n \\ &= b_1 x_1 + \cdots + b_{n-1} x_{n-1} + b_n (C'' - b_1 x_1 - \cdots \\ & \quad - b_{n-1} x_{n-1}) / b_n \\ &= C'' \end{aligned} \quad (2-38)$$

3. 復号化の一意性

与えられた暗号文 C から平文を復号するに当たって平文が一意に決定されることを証明する。

平文の存在は保証されているものとする。

命題

与えられた暗号文 C から、2つの平文

$$X = (x_1, x_2, \dots, x_n) \quad (3-1)$$

$$X' = (x_1', x_2', \dots, x_n') \quad (3-2)$$

が復号されたとする。つまり、

$$C = a_1 x_1 + \cdots + a_n x_n \quad (3-3)$$

$$= a_1 x_1' + \cdots + a_n x_n' \quad (3-4)$$

が成立するときは、

$$X = X' \quad (3-5)$$

つまり、

$$x_i = x_i' \quad (i=1, \dots, n) \quad (3-6)$$

である。

証明

$$C = a_1 x_1 + \cdots + a_n x_n$$

$$= a_1 x_1' + \cdots + a_n x_n'$$

より、

$$\sum_{i=1}^n a_i (x_i - x_i') = 0 \quad (3-7)$$

β^{-1} を両辺に掛け、 $\text{mod } R$ を施すと、

$$\beta^{-1} \sum_{i=1}^n a_i (x_i - x_i') \text{ mod } R \equiv 0 \quad (3-8)$$

$$\sum_{i=1}^n a_i \beta^{-1} (x_i - x_i') \text{ mod } R \equiv 0 \quad (3-9)$$

(2-10)式より、

$$\sum_{i=1}^n b_i (x_i - x_i') \text{ mod } R \equiv 0 \quad (3-10)$$

ところで、

$$0 \leq x_i, x_i' < P_i \quad (i=1, \dots, n) \quad (3-11)$$

だから、

$$|x_i - x_i'| < P_i \quad (i=1, \dots, n) \quad (3-12)$$

となる。したがって、

$$\begin{aligned} & \left| \sum_{i=1}^n b_i (x_i - x_i') \right| \\ & \leq \sum_{i=1}^n b_i |x_i - x_i'| < \sum_{i=1}^n b_i P_i \end{aligned} \quad (3-13)$$

(2-9)式より、

$$\left| \sum_{i=1}^n b_i (x_i - x_i') \right| < R \quad (3-14)$$

が得られるから、

$$\sum_{i=1}^n b_i (x_i - x_i') = 0 \quad (3-15)$$

となる。上式に $\text{mod } P_1$ を施すと、

$$\sum_{i=1}^n b_i (x_i - x_i') \text{ mod } P_1 \equiv 0 \quad (3-16)$$

(2-4 a)～(2-4 c)式より、

$$\begin{aligned} & b_1 (x_1 - x_1') \text{ mod } P_1 \equiv 0 \\ & x_1 \equiv x_1' \text{ mod } P_1 \end{aligned} \quad (3-17)$$

(2-8)式より、

$$0 \leq x_1, x_1' < P_1 \quad (3-18)$$

だから、

$$x_1 = x_1' \quad (3-19)$$

この結果を(3-10)式に代入し、 $\text{mod } P_2$ を施すと、

$$\sum_{i=1}^n b_i (x_i - x_i') \text{ mod } P_2 \equiv \sum_{i=2}^n b_i (x_i - x_i') \text{ mod } P_2 \quad (3-20)$$

(2-4 a)～(2-4 c)式より、

$$\begin{aligned} & b_2 (x_2 - x_2') \text{ mod } P_2 \equiv 0 \\ & x_2 \equiv x_2' \text{ mod } P_2 \end{aligned} \quad (3-21)$$

(2-7)式より、

$$0 \leq x_2, x_2' < P_2 \quad (3-22)$$

だから、

$$x_2 = x_2' \quad (3-23)$$

以下、同様にして、

$$x_i = x_i' \quad (i=3, \dots, n-1) \quad (3-24)$$

が得られる。

この結果を、(3-10)式に代入すると、

$$b_n(x_n - x_n') \bmod R \equiv 0 \quad (3-25)$$

$$0 \leq x_n, x_n' < R \quad (3-26)$$

だから,

$$x_n = x_n' \quad (3-27)$$

となる。したがって,

$$X = X' \quad (3-28)$$

つまり,

$$x_i = x_i' \quad (i=1, \dots, n) \quad (3-29)$$

が得られた。

(証明おわり)

4. 数 値 例

理解を助けるため簡単な数値例を示す。

ユーザ U_A とユーザ U_B との通信を考える。ユーザ U_A は次の手順で正整数係数 a_i を生成する。

$$P_0 = 1$$

(2-3)式の A の大きさとして, $A=10$ とする。

$n=3, P_1=5, P_2=7$ を選ぶと,

$$b_1 = k_1 P_0 = k_1$$

$$b_2 = k_2 P_0 P_1 = 5k_2$$

$$b_3 = k_3 P_0 P_1 P_2 = 35k_3$$

となる。(2-5 a) ~ (2-5 d)式から,

$$o(k_1) = 100, o(k_2) = 10, k_3 = 1.$$

したがって, (2-9)式の R の値を次のように決める。

$$\begin{aligned} o(b_1 P_1 + b_2 P_2 + b_3 P_3) \\ = o(100 \cdot 10 + 100 \cdot 10 + 100 \cdot 10) \\ = o(1000 \cdot 3) < R = 11003 \end{aligned}$$

次に, R と互いに素な整数として (2-10)式の a_3 の大きさが $o(100)$ となるように β を定める。

$$\begin{aligned} a_3 &\equiv \beta b_3 \pmod{R} \\ &\equiv 35\beta \pmod{11003} \\ \beta &= 5033 \end{aligned}$$

に選ぶと, $a_3 = 107$ が得られる。

a_1, k_1 を求める。

$$\begin{aligned} o(a_1) &= 100, o(k_1) = 100 \\ a_1 &\equiv \beta b_1 \pmod{R} \\ &\equiv 5033 \cdot k_1 \pmod{11003} \\ k_1 &= 129 \end{aligned}$$

に選ぶと,

$$a_1 = 80 \text{ となる。}$$

a_2, k_2 を求める。

$$\begin{aligned} o(a_2) &= 100, o(k_2) = 10 \\ a_2 &\equiv \beta b_2 \pmod{R} \\ &\equiv 5033 \cdot 5 \cdot k_2 \pmod{11003} \\ k_2 &= 115 \end{aligned}$$

に選ぶと,

$$a_2 = 186 \text{ となる。}$$

以上, 纏めると

$$a_1 = 80 \quad b_1 = 129 \quad k_1 = 129$$

$$a_2 = 186 \quad b_2 = 575 \quad k_2 = 115$$

$$a_3 = 107 \quad b_3 = 35 \quad k_3 = 1$$

$$R = 11003 \quad \beta = 5033$$

$$P_{\min} = 4$$

公開される暗号鍵は,

$$[a_1, a_2, a_3; P_{\min}] = [80, 186, 107; 4]$$

である。

暗号化

ユーザ U_B は, 平文 X として

$$X = (1, 2, 3)$$

を選ぶ。公開された a_i および x_i から

$$C = \sum_{i=1}^3 a_i x_i = 80 \cdot 1 + 186 \cdot 2 + 107 \cdot 3 = 773$$

を計算し, ユーザ U_A に, C を送信する。

復号化

$$\beta^{-1} \bmod R \equiv 10592$$

である。

ユーザ U_A は C を受信すると, 次の手順により平文 X を復号する。

$$\begin{aligned} C' &\equiv C \cdot \beta^{-1} \bmod R \equiv 773 \cdot 10592 \bmod R \\ &\equiv 1384 \end{aligned}$$

$$b_1 x_1 \equiv C' \bmod P_1 \equiv 4$$

よって,

$$x_1 \equiv 4 \cdot b_1^{-1} \bmod P_1 \equiv 1$$

が得られた。次に, x_2 は

$$b_2 x_2 \equiv (C' - b_1 x_1) \bmod P_2 \equiv 1255 \equiv 2$$

よって,

$$x_2 \equiv 2 \cdot b_2^{-1} \bmod P_2 \equiv 2$$

x_3 は,

$$b_3 x_3 \equiv (C' - b_1 x_1 - b_2 x_2) / P_1 / P_2 = 105 / 35 = 3$$

つまり, 平文 X として,

$$X = (1, 2, 3)$$

が, 復号された。

5. 解 読 法

5.1 LLL アルゴリズムを用いた解読法

LLL アルゴリズム⁵⁾を用いて, 本暗号系を攻撃することを考える。平文 x_i ($i=1, \dots, n$) は正整数として秘密にされ, 公開されている n 個の正整数係数 a_i ($i=1, \dots, n$) と, 暗号文 C

$$C = a_1x_1 + \dots + a_nx_n \quad (5-1)$$

から平文 x_i ($i=1, \dots, n$) を求める。まず,

$$v_1 = (1, 0, \dots, 0, -a_1) \quad (5-2a)$$

$$v_2 = (0, 1, \dots, 0, -a_2) \quad (5-2b)$$

$\vdots$

$$v_n = (0, 0, \dots, 1, -a_n) \quad (5-2c)$$

$$v_{n+1} = (0, 0, \dots, 0, C) \quad (5-2d)$$

を基底ベクトルとする $n+1$ 次元の整数ラティスを考える。LLL アルゴリズムを用いて、このラティスで最も短い非零ベクトル

$$w = (w_1, w_2, \dots, w_n, w_{n+1}) \quad (5-3)$$

を見出すことができる。

$$x_i \in \{0, 1\} \quad (5-4)$$

ならば、確かに w を見出すことにより、

$$\text{平文 } X = (x_1, \dots, x_n) = (w_1, \dots, w_n) \quad (5-5)$$

となり、解読可能であるが、 q を正整数として

$$0 \leq x_i \leq q \quad (5-6)$$

の範囲を x_i がとる場合、

$$X^* = (x_1, x_2, \dots, x_n, 0) \quad (5-7)$$

が最も短いベクトルとなりうるか疑問である。

$$o(x_i) = A \quad (i=1, \dots, n) \quad (5-8)$$

であるため、

$$C' = a_1x_1' + \dots + a_nx_n' \quad (5-9)$$

$$|C' - C| < A \quad (5-10)$$

となる C' が存在したとすれば、

$$X^{*'} = (x_1', \dots, x_n', C - C') \quad (5-11)$$

も十分短いベクトルとなり得る。

簡単な例を挙げる。

$$a = (110, 121, 185, 133) \quad (5-12)$$

$$X = (3, 12, 7, 4) \quad (5-13)$$

$$C = a_1x_1 + \dots + a_4x_4 = 3609 \quad (5-14)$$

このとき、

$$w = (3, 12, 7, 4, 0) \quad (5-15)$$

より、

$$|w| = 218 \quad (5-16)$$

が得られる。

$$X' = (5, 8, 7, 6) \quad (5-17)$$

とすると、

$$C' = a_1x_1' + \dots + a_4x_4' = 3611 \quad (5-18)$$

このとき、

$$w' = (5, 8, 7, 6, 2) \quad (5-19)$$

より、

$$|w'| = 178 < |w| \quad (5-20)$$

が得られる。

この例のように、必ずしも最短ベクトルが平文を与えるとは限らないと言える。

$$|C' - C| < A \quad (5-21)$$

となる $X = (x_1, \dots, x_n)$ の場合の数はどの程度か。

$$0 \leq x_i < P_i \quad (5-22)$$

の範囲で動くとして、

$$0 \leq C = a_1x_1 + \dots + a_nx_n < nA^* \quad (5-23)$$

この範囲内に C の値が平均して分布すると仮定すると X のすべての場合の数は、 A^* だから

$$(2A/nA^*) * A^* \quad (5-24)$$

$$= 2A/n$$

$$|C' - C| < A$$

の範囲に入る X の場合の数は、十分大きくなり、求めるべき平文の近傍にも多数の平文が存在することになり、LLL アルゴリズムを利用して解読することは困難と思われる。

5.2 シャミールのアルゴリズム^{3),4)}による攻撃

シャミールのアルゴリズムは、 n 個の正整数の組 $(a_1, \dots, a_n)$ が与えられたとき、 $a_i \beta \bmod R$ が超増加数列となっている場合、その総和が R 未満となる正整数 (β, R) の組を見出すアルゴリズムである。 $b_i \equiv a_i \beta \bmod R$ が超増加数列をなすことが必要であるが、本暗号系の b_i は k_i の値を変化させ、各 b_i の大きさがほぼ同じ大きさとしているため、シャミールのアルゴリズムを適用することは非常に困難と思われる。また、超増加数列が見出されても、本暗号系は 0-1 ナップザックではないので解読困難であろう。

5.3 直接法

平文 $(x_1, x_2, \dots, x_n)$ に順次値を代入して C を与える $(x_1, x_2, \dots, x_n)$ を求めることは場合の数が 10^{150} となり、正解を見出すことは非常に困難と思われる。

6. デジタル署名

本暗号系を利用して、デジタル署名が可能になる。まず、

$$0 \leq C < R \quad (6-1)$$

の範囲の任意の暗号文 C に平文 X を対応させることを考える。2章で述べた暗号系では、

$$0 \leq C < R = o(nA^*) \quad (6-2)$$

$$0 \leq x_i < P_{\min} \quad (i=1, \dots, n) \quad (6-3)$$

$$o(P_1 \dots P_n) = A^* < nA^* = o(R) \quad (6-4)$$

であり、暗号文の定義域の方が大きいため一対一対応は不可であるが、 x_n の定義域を

$$-(n-1)A < o(x_n) < nA \quad (6-5)$$

と拡張することによって, 上記の任意の暗号文 C に対応する明文 X が存在し得ることが可能となり, デジタル署名が可能となる. そのための必要十分条件は,

$$(2-19) \text{式を, 暗号化写像 } E \quad (6-6)$$

$$(2-20) \sim (2-29) \text{式を, 復号化写像 } D \quad (6-7)$$

とすると,

$$D(E(X))=X, X \in S_x \quad (6-8)$$

$$S_x = \{X = (x_1, \dots, x_n) | 0 \leq x_i < P_i \ (i=1, \dots, n)\} \quad (6-9)$$

$$E(D(C))=C, C \in S_c \quad (6-10)$$

$$S_c = \{C | 0 \leq C < R\} \quad (6-11)$$

が成立することである (図1参照).

ただし,

$$D(C) \in S_0 \quad (6-12)$$

$$S_0 = \{X = (x_1, \dots, x_n) | 0 \leq x_i < P_i \ (i=1, \dots, n-1), \\ -(n-1)A < o(x_n) < nA\} \quad (6-13)$$

(6-8)式は2章で述べたことより明らかである.

(6-10)式が成立することを示す.

証明

まず, (6-12)式を示そう. 2.2 節の復号化手順により順次 x_i を求めることになるが,

$$0 \leq x_i < P_i \ (i=1, \dots, n-1) \quad (6-14)$$

は明らかであり, (2-29)式より, x_n が与えられるから x_n は,

$$-\sum_{i=1}^{n-1} b_i P_i / b_n < X_n < C'' / b_n$$

の範囲に入るから

$$-(n-1)A^* / b_n < o(X_n) < nA^* / b_n \\ -(n-1)A < o(X_n) < nA \quad (6-15)$$

したがって,

$$D(C) \in S_0 \quad (6-16)$$

が示せた. 次に,

$$a_1 x_1 + \dots + a_n x_n \bmod R \\ \equiv (b_1 x_1 + \dots + b_n x_n) \beta \bmod R \quad (6-17)$$

(2-35)式より,

$$\equiv C'' \beta \bmod R \quad (6-18)$$

(2-20), (2-22)式より,

$$\equiv C \beta^{-1} \beta \bmod R \equiv C \quad (6-19)$$

が得られる. また, (2-9), (2-11)式より,

$$0 \leq a_1 x_1 + \dots + a_n x_n < R \quad (6-20)$$

だから,

$$a_1 x_1 + \dots + a_n x_n = C \quad (6-21)$$

したがって,

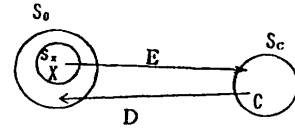


図1 暗号化写像と復号化写像

Fig. 1 Enciphering map and deciphering map.

$$E(D(C))=C, C \in S_c \quad (6-22)$$

が得られる. (証明おわり)

簡単な数値例を示す.

$$n=3 \quad (6-23)$$

$$P_1=13, P_2=11 \quad (6-24)$$

$$k_1=1738, k_2=5, k_3=1 \quad (6-25)$$

$$b_1=k_1=1738, b_2=k_2 P_1=65, b_3=k_3 P_2 P_1=143 \quad (6-26)$$

$$R=11087, \beta=2559 \quad (6-27)$$

を採用する.

$$\beta^{-1}=1850 \quad (6-28)$$

となる.

b_1, b_2, b_3 を R, β で変換すると,

$$a_1 \equiv b_1 \beta \equiv 1655 \bmod R < b_1 \quad (6-29)$$

$$a_2 \equiv b_2 \beta \equiv 30 \bmod R < b_2 \quad (6-30)$$

$$a_3 \equiv b_3 \beta \equiv 66 \bmod R < b_3 \quad (6-31)$$

となっている.

暗号化式は

$$C = 1655x_1 + 30x_2 + 66x_3 \quad (6-32)$$

である.

暗号文として,

$$C = 9876 \quad (6-33)$$

を選ぶと, 復号化手順により,

$$X = (6, 7, -4) \quad (6-34)$$

が得られる.

この X を求めることができるのは, 復号化鍵を持つユーザのみである.

この X より, 他のユーザは,

$$C = 1655*6 + 30*7 + 66*(-4) \\ = 9876 \quad (6-35)$$

を得ることができる.

7. おわりに

ディオファントスの一次不定方程式に基づく公開鍵暗号系を提案した. 本暗号系では, 暗号化・復号化に必要な計算量が, RSA 法と比較してかなり少なく済むことを示した. また, 明文の定義域をわずかに拡張することによりデジタル署名が可能になることも

示した。

しかし、暗号系を構築するうえで前提となる b_i, a_i の存在を厳密に示すことはしなかった。モジュラ R に比べ数値的に小さい b_i, a_i を用いることにより、平文 x_i との内積がモジュラ R を越えないことがポイントの1つとなっている。

また、数値例を示したが、いずれも数値が小さい例であり、実用に耐えうる例を示すことができなかった。上記の問題点は、今後の課題としたい。

参 考 文 献

- 1) Rivest, R. L., Shamir, A. and Adleman, L.: A Method of Obtaining Digital Signatures and Public Key Cryptosystems, *Comm. ACM*, Vol. 21, No. 2, pp. 120-126 (1978).
- 2) Merkle, R. C. and Hellman, M. E.: Hiding Information and Signature in Trapdoor Knapsacks, *IEEE Trans. Inf. Theory*, Vol. IT-24, No. 5, pp. 525-530 (1978).
- 3) Shamir, A.: A Polynomial-Time Algorithm for Breaking the Basic Merkle-Hellman Crypto-

system, *IEEE Trans. Inf. Theory*, Vol. IT-30, No. 5, pp. 699-704 (1984).

- 4) Lenstra, H. W., Jr.: Integer Programming with a Fixed Number of Variables, Univ. of Amsterdam Tech. Report, 81-03 (Apr. 1981).
- 5) Lenstra, A. K., Lenstra, H. W., Jr. and Lovasz, L.: Factoring Polynomials with Rational Coefficients, *Mathematische Annalen*, Vol. 261, No. 4, pp. 515-534 (1982)

(平成2年4月23日受付)

(平成2年9月11日採録)



八木沢正博 (正会員)

昭和25年生。昭和49年東京大学工学部計数工学科卒業。昭和51年同大学院修士課程修了。同年昭和電工(株)入社。川崎工場勤務。昭和61年昭和エンジニアリング(株)に出向。現在に至る。化学プラントの計装エンジニアとして、プラントの設計、保全に従事。現在、不定方程式の解法に興味を持つ。