離散的対数問題に基づく公開鍵暗号系†

八木沢 正博††

xを未知数とした離散的対数問題 $y\equiv a^x \bmod P$ の難しさに基づいた公開鍵暗号系を提案する．離散的対数問題の難しさに基づいている点において，ElGamal 暗号系に似ているが，ElGamal 暗号系は，乱数を用いて暗号化しており，暗号文のサイズが平文のサイズの2倍となり，さらに，この乱数を通信文ごとに変える必要がある．本論文で提案している暗号系は，ElGamal 暗号系の乱数部を平文情報 qx_1+x_2 で置き換えることにより，ElGamal 暗号系の欠点を軽減した．つまり，平文 (x_1, x_2) から，次式のように暗号文 (y_1, y_2) を生成する．

$$\begin{cases} y_1\equiv a^{qx_1+x_2} \bmod P & (1)\\ y_2\equiv x_2 b^{qx_1+x_2} \bmod P & (2)\end{cases}$$

ここで，$P-1$ は，次のように素因数に分解される．

$$P-1=q_1^{n_1}\cdots q_m^{n_m}\cdot q,\ q_i<q_{i+1} \qquad (3)$$

q は十分大きな素因数，他の q_i は十分小さな素因数である．a は，素数 P の原始根であり，$P-1$ と互いに素である整数 r を用いて，b は

$$b\equiv a^r \bmod P \qquad (4)$$

と表される．r は秘密鍵である．暗号文のサイズは，平文の 4/3 倍程度となる．復号化は，

$$\begin{cases} x_2\equiv y_2\cdot y_1^{-r} \bmod P & (5)\\ a^{qx_1}\equiv y_1\cdot a^{-x_2} \bmod P & (6)\end{cases}$$

となるが，式(6)に，ポーリック-ヘルマンの方法またはその改良型である，筆者の提案した方法を用いることにより，x_1 を復号化する．

1. まえがき

1976年に公開鍵暗号系が提案されて以来，RSA 法を代表例として，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，xを未知数とした離散的対数問題 $y\equiv a^x \bmod P$ の難しさに基づいた公開鍵暗号系を提案する．素数 P が十分大きく，かつ $P-1$ が十分大きな素因数を含むとき，離散的対数を求めることは，計算量の上から非常に困難となる．

この公開鍵暗号系では，多数のユーザが共通の法 P をもつことができるという特徴をもつ．

暗号化式の形が似ており，離散的対数問題の難しさに基づく暗号系に ElGamal 暗号系があるが，暗号化に乱数 k を用いており，暗号文のサイズが，平文の2倍となる．さらに，乱数 k を通信文ごとに変える必要があると言われている．

本論文で提案している暗号系では，乱数を平文情報で置き換えることにより，暗号文のサイズは素数 P の選び方によるが，平文のサイズの 4/3 倍程度となる．復号化には，一つの平文を求めるのに離散的対数の計算をする必要があり，ポーリック-ヘルマンの方法[1]，または，筆者が提案した方法[2]を用いることができる．

† A Public-key Cryptosystem Based on Discrete Logarithm Problem by MASAHIRO YAGISAWA (Showa Engineering Corporation).

†† 昭和エンジニアリング(株)

2. 暗号化アルゴリズム

素数 P として，次のような性質をもつものを選ぶ．

$P-1$ の素因数分解を

$$P-1=q_1^{n_1}\cdot q_2^{n_2}\cdot\cdots\cdot q_m^{n_m}\cdot q \qquad q_i<q_{i+1} \qquad (2.1)$$

としたとき，q は十分大きな素因数であり，他の素因数 q_i は，十分小さい．つまり，

$$q\gg q_i \quad (i=1, 2, \cdots, m) \qquad (2.2)$$

さらに，A, A_i, B_i を次のように定義する．

$$A=q_1^{n_1}\cdot q_2^{n_2}\cdot\cdots\cdot q_m^{n_m} \qquad (2.3)$$

$$A_i=q_i^{n_i} \quad (i=1, 2, \cdots, m) \qquad (2.4)$$

$$B_i=A/A_i \quad (i=1, 2, \cdots, m) \qquad (2.5)$$

$q, q_1, q_2, \cdots, q_m$ は相異なる素数であり，n_i は自然数である．

さらに，$q-1$ は十分大きな素因数 q' をもつ，つまり，

$$q=2\eta q'+1 \quad (\eta \text{ は自然数}) \qquad (2.6)$$

平文 x_1, x_2

$$0\leqq x_1\leqq A-1 \qquad (2.7)$$

$$0\leqq x_2\leqq P-1 \qquad (2.8)$$

暗号文 y_1, y_2

$$0<y_1\leqq P-1 \qquad (2.9)$$

$$0 \leqq y_2 \leqq P-1 \tag{2.10}$$

に対して

$$\begin{cases} y_1 \equiv a^{qx_1+x_2} & \mod P \quad (2.11) \\ y_2 \equiv x_2 b^{qx_1+x_2} & \mod P \quad (2.12) \end{cases}$$

を暗号化式とする．ここで，整数 a, b の範囲を

$$1<a<P-1 \tag{2.13}$$

$$1<b<P-1 \tag{2.14}$$

とする．a と b は整数 r を用いて，

$$b \equiv a^r \mod P \tag{2.15}$$

と関係づけられる．a は素数 P の原始根とする．

r は，$P-1$ と互いに素とする．つまり，

$$gcd(P-1, r)=1 \tag{2.16}$$

暗号化鍵 K_E は，

$$K_E=(P, q, a, b) \tag{2.17}$$

で与えられる．式(2.11)，(2.12)の暗号化式は公開されるが，式(2.15)の r は秘密にされる．つまり，r が秘密の復号化鍵の主体をなす．

3. 復号化アルゴリズム

暗号文 y_1, y_2 から平文 x_1, x_2 を復号化する復号化式を

$$\begin{cases} x_2 \equiv y_2 \cdot y_1^{-r} & \mod P \quad (3.1) \\ a^{qx_1} \equiv y_1 \cdot a^{-x_2} & \mod P \quad (3.2) \end{cases}$$

とする．r の値を知るのは，正当な受信者のみである．式(3.1)から，x_2 は容易に求まるが，x_1 は次に述べる展開表現を利用して求める．

復号化鍵 K_D は

$$K_D=(P, q, a, r) \tag{3.3}$$

で与えられる．

3.1 x_1 の展開表現

中国剰余定理より，x_1 は次のように表現できる．

$$x_1 \equiv \sum_{i=1}^{m} c_i z_i \mod A \tag{3.4}$$

ここで，

$$z_i \equiv x_1 \mod A_i \ (i=1, 2, \cdots, m) \tag{3.5}$$

B_i と A_i は互いに素であるから，適当な整数 s_i と t_i を用いて

$$s_i B_i - t_i A_i = 1 \tag{3.6}$$

とすることができる．この s_i を用いて，c_i は

$$c_i \equiv s_i B_i \mod A \ (i=1, 2, \cdots, m) \tag{3.7}$$

と表される．

さらに，z_i は次のように展開できる．

$$z_i \equiv \sum_{j=0}^{n_i-1} d_{ij} q_i^j \mod A_i \ (i=1, 2, \cdots, m) \tag{3.8}$$

$$0 \leqq d_{ij} \leqq q_i - 1 \tag{3.9}$$

式(3.7)を式(3.4)に代入すると

$$x_1 \equiv \sum_{i=1}^{m} s_i B_i z_i \mod A \tag{3.10}$$

が得られ，さらに，式(3.8)を代入すると

$$x_1 \equiv \sum_{i=1}^{m} \sum_{j=0}^{n_i-1} s_i B_i d_{ij} q_i^j \mod A \tag{3.11}$$

が得られる．

ところで，

$$\gamma_i \overset{\text{def}}{\equiv} a^{(P-1)/q_i} \mod P \tag{3.12}$$

で与えられる γ_i は，1の q_i 乗根であるから，式(3.2)の左辺と右辺を入れ替えて A/q_i 乗し，γ_i を用いて変形すると

$$\begin{aligned} (y_1 a^{-x_2})^{A/q_i} &\equiv (a^{qx_1})^{A/q_i} \equiv (a^{(P-1)/q_i})^{x_1} \\ &\equiv \gamma_i^{x_1} \equiv \gamma_i^{d_{i0}} \mod P \end{aligned} \tag{3.13}$$

が得られる．

3.2 x_1 の復号化アルゴリズム

式(3.2)で与えられる平文 x_1 を復号化することは，式(3.14)

$$a^{q\left(\sum_{i=1}^{m}\sum_{j=0}^{n_i-1} s_i B_i d_{ij} q_i^j\right)} \equiv y_1 \cdot a^{-x_2} \mod P \tag{3.14}$$

から，d_{ij} $(1 \leqq i \leqq m,\ 0 \leqq j \leqq n_i-1)$ を求めることに等しい．

式(3.14)で a, m, n_i, s_i, B_i, q_i, q は定数であり，右辺の y_1, x_2 が与えられたとき，d_{ij} を求め，式(3.11)から x_1 を復号化することを考える．

まず，d_{10} を求めよう．式(3.14)の左辺と右辺を入れ替えて，A/q_1 乗すると，式(3.13)より

$$(y_1 \cdot a^{-x_2})^{A/q_1} \equiv \gamma_1^{d_{10}} \mod P \tag{3.15}$$

が得られる．ここで，

$$\gamma_1 \equiv a^{(P-1)/q_1} \mod P \tag{3.16}$$

である．式(3.15)の d_{10} に，0から q_1-1 までの値を代入して，式(3.15)の右辺の値を求め，その値が左辺の値と一致するか調べる．

ところで，$g_1(w)$ を

$$\gamma_1^{g_1(w)} \equiv w \mod P \tag{3.17}$$

と定義して，事前に各 $g_1(w)$ の値に対する w の値を求めて，$g_1(w)$ のテーブルを作成しておくことができる．

とくに，$q_1=2$ のときは，$g_1(w)=0$ または1となる．

次に，d_{11} を求める．式(3.2)の左辺と右辺を入れ替

え，

$$a^{-qd_{10}} \tag{3.18}$$

をかけたのち，A/q_1^2 乗すると，

$$\begin{aligned}(y_1 \cdot a^{-x_1} \cdot a^{-qd_{10}})^{A/q_1^2} &\equiv (a^{qx_1} \cdot a^{-qd_{10}})^{A/q_1^2} \\ &\equiv (a^{(P-1)/q_1})^{(x_1-d_{10})/q_1} \\ &\equiv \gamma_1^{d_{11}} \end{aligned} \tag{3.19}$$

が得られる．したがって，d_{10} と同様にして，$g_1(w)$ のテーブルを用いて，d_{11} を求めることができる．

以下，同様にして，

$$d_{12}, d_{13}, \cdots, d_{1\,n_1-1} \tag{3.20}$$

が得られる．

さらに，同じ方法で

$$\gamma_i^{g_i(w)} \equiv w \quad \mod P \ (i=2, 3, \cdots, m) \tag{3.21}$$

を満足する $g_i(w)$ のテーブルを利用して，d_{ij} $(i=2, 3, \cdots, m;\ j=0, 1, \cdots, n_i-1)$ を求めることができる．その手順を図1に示す．

式(3.11)に d_{ij} を代入することにより，x_1 が復号化される．

図1のアルゴリズムを用いると，$O(\log_2 A)^2$ の計算量と，$O(\log_2 P)$ bit の記憶容量を必要とする．

筆者が提案したアルゴリズム[2]を用いれば，$O(c(\log_2 \log_2 A)(\log_2 A))$ の計算量と $O(d(\log_2 \log_2 P)(\log_2 P))$ bit の記憶容量で十分である (c, d は小さい定数)．

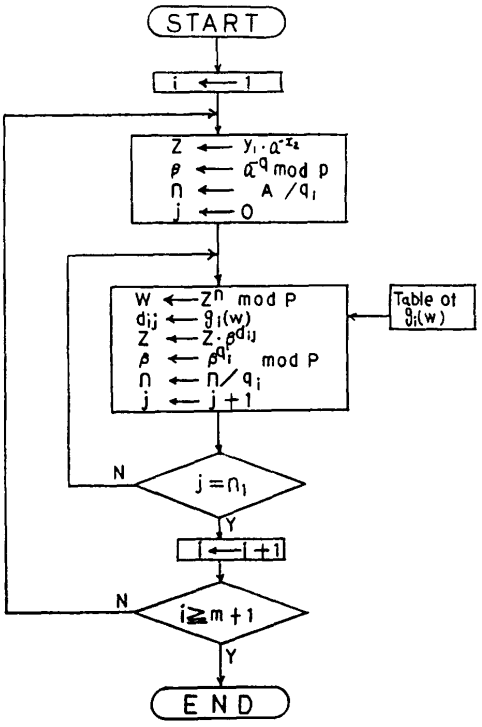

図1 d_{ij} を求めるアルゴリズム
Fig. 1 Flowchart for algorithm to calculate d_{ij}.

4. ElGamal 暗号系との比較

ElGamal 暗号系[3]は，離散的対数問題の難しさをもとにした公開鍵暗号系であり，暗号化，復号化は次式で与えられる．

x_1 を乱数，x_2 を平文，y_1, y_2 を暗号文，α を素数 P の原始根とすると，ユーザ u_A から，ユーザ u_B への秘密通信を考えると，暗号化式は，

$$y_1 \equiv \alpha^{x_1} \quad \mod P \tag{4.1}$$

$$y_2 \equiv x_2 (K_B)^{x_1} \quad \mod P \tag{4.2}$$

ここで，K_B は，ユーザ u_B の公開鍵であり，秘密鍵 γ_B を用いて，

$$K_B \equiv \alpha^{\gamma_B} \quad \mod P \tag{4.3}$$

$$0 < \gamma_B < P \tag{4.4}$$

と表される．

復号化式は，

$$x_2 \equiv y_2 \cdot y_1^{-\gamma_B} \quad \mod P \tag{4.5}$$

となる．

ElGamal 暗号系の短所としては，暗号文のサイズが平文のサイズの2倍となること，および，同一の x_1 を用いて，他の平文 x_2' を暗号化した場合，暗号文を y_1', y_2' とすると

$$x_2'/x_2 = y_2'/y_2 \tag{4.6}$$

が成立し，1組の x_2 と y_2 がわかると，他のすべての x_2 は，y_2 からわかり，既知平文攻撃が容易に可能であることである．

本暗号系では，8章で述べるように，暗号文の冗長度は，約 0.25 であるから，暗号文のサイズは平文の約 4/3 倍程度になり，ElGamal 暗号系に比べて，冗長度は小さくなるが，復号化に要する計算量は大きくなる．また，乱数 k を用いるかわりに，平文情報 qx_1+x_2 を用いている．この平文情報 qx_1+x_2 の値が同一となる．つまり，平文 (x_1, x_2), (x_1', x_2') が

$$qx_1 + x_2 \equiv qx_1' + x_2' \quad \mod P-1 \tag{4.7}$$

となる平文集合に対しては，ElGamal 暗号系と同じように，既知平文攻撃が容易に可能となる．

5. 法 P の選び方

本論文で提案している暗号系は，素数 P を法とする演算を必要とし，また，離散的対数問題

$$y \equiv a^x \quad \mod P \tag{5.1}$$

の難しさに基づいているため，$P-1$ が十分大きな素

因数 q をもつ必要がある．$P-1$ は次のように合成数 A と q の積で表される．

$$P-1=Aq \tag{5.2}$$

さらに，$q-1$ も十分大きな素数 q' をもつ．

$$q-1=2q'\eta \quad (\eta \text{ は自然数}) \tag{5.3}$$

A の形として，離散的対数演算量を少なくする目的から

$$A=2^n \quad (n \text{ は自然数}) \tag{5.4}$$

が考えられる．したがって，素数 P の形として，

$$P=2^n(2\eta q'+1)+1 \tag{5.5}$$

が代表的なものとなる．

P の数値例として，小さなものからいくつか挙げる．

$P=2^5(2\cdot1\cdot41+1)+1=2,657,\ q=83$

$P=2^7(2\cdot1\cdot53+1)+1=13,697,\ q=107$

$P=2^7(2\cdot1\cdot83+1)+1=21,377,\ q=167$

$P=2^{11}(2\cdot1\cdot89+1)+1=366,593,\ q=179$

$P=2^{15}(2\cdot1\cdot89+1)+1=5,865,473,\ q=179$

6. 安 全 性

本暗号系の安全性は，式(2.15)で与えられる離散的対数を求めることの困難さに基づいている．

アドルマンの方法では，$P-1$ が大きな素因数をもっている場合，離散的対数を求めるのに必要な演算数は，概略次式のとおりである[4]．

$$N=\exp\sqrt{\log_e P\log_e(\log_e P)} \tag{6.1}$$

本暗号系では，素数 P に

$$P-1=Aq$$

となる制約があるが，一般の素数に比較して，アドルマンの方法の v-smooth になる確率 ρ に差はないと思われるので，離散的対数を求めるのに必要な演算数は，式(6.1)で与えられる．

式(6.1)は，$P\fallingdotseq10^{150}$ のとき，$N\fallingdotseq3.2\times10^{19}$ となる．

式(2.15)の r を求めるのに，1秒間に 10^6 回演算可能な計算機を用いて

$$N/(10^6\cdot3600\cdot24\cdot365)\fallingdotseq1.0\times10^5 \text{ 年} \tag{6.2}$$

かかることになる．

表1に P の桁数に対する演算数，実行年数を示す．

次に，x_1, x_2, r を未知数とした連立方程式

$$\begin{cases} y_1\equiv a^{qx_1+x_2} & \bmod P \quad (2.11)\\ y_2\equiv x_2b^{qx_1+x_2} & \bmod P \quad (2.12)\\ b\equiv a^r & \bmod P \quad (2.15)\end{cases}$$

を解くことの難しさを考えよう．まず，

表1 離散的対数の計算量
Table 1 Complexity for calculating discrete logarithms.

Pの桁数	演算数	実行年数
50	1.4×10^{10}	23分
100	2.3×10^{15}	7.4年
150	3.2×10^{19}	1.0×10^5年
200	1.2×10^{23}	3.8×10^8年
250	1.8×10^{26}	5.8×10^{11}年
300	1.5×10^{29}	4.8×10^{14}年

$$X=qx_1+x_2 \tag{6.3}$$

とおく．

いま，任意の暗号文 (y_1, y_2) が与えられたとき，平文 (x_1, x_2) を求めるアルゴリズムが存在すると仮定すると，式(6.3)より，X の値も計算できる，つまり，式(2.11)で与えられる y_1 の離散的対数 X の値を求めることが可能となる．

逆に，式(2.15)の r，つまり，b の離散的対数 r の値を求めるアルゴリズムが存在すると仮定すると，連立方程式(2.11)，(2.12)，(2.15)で暗号文 (y_1, y_2) が与えられると，平文 (x_1, x_2) を求めることが可能となる．

したがって，本暗号系の安全性は，離散的対数問題の難しさに基づいていると言える．

7. 計 算 量

暗号化式および復号化式における計算量を概算する．P, q, n, A の値を次のように選んだ場合を例にとって説明する．

$P\fallingdotseq10^{150}$ $\quad q\fallingdotseq10^{74}$

$g=8$ $\quad n=2^g-1=255$

$A=2^n\fallingdotseq5.8\times10^{76}$

7.1 暗号化式における計算量

$$\begin{cases} y_1\equiv a^{qx_1+x_2} & \bmod P \quad (7.1)\\ y_2\equiv x_2b^{qx_1+x_2} & \bmod P \quad (7.2)\end{cases}$$

式(7.1)における乗算数$\fallingdotseq2[\log_2P]+1$

式(7.2)における乗算数$\fallingdotseq2[\log_2P]+1$

したがって，

乗算数 $N_m\fallingdotseq4[\log_2P]+2=1994$ (7.3)

([・]は・を越えない最大の整数を表す．)

必要メモリー容量 $M_m\fallingdotseq10([\log_2P]+1)\fallingdotseq5$ kbit (7.4)

ところで，$a^2, a^{2^2}, \cdots, a^{2^k}$; $b^2, b^{2^2}, \cdots, b^{2^k}$ ($k=[\log_2(P-1)]$) を前もって，mod P 上で計算し，その結果をテーブルとして，用いる場合は，

$$N_m \fallingdotseq 2[\log_2 P]+2=998 \quad (7.5)$$

$$M_m \fallingdotseq (2k+10)([\log_2 P]+1) \fallingdotseq 502\,\text{kbit} \quad (7.6)$$

となる．

7.2 復号化式における計算量

$$\begin{cases} x_2 \equiv y_2 \cdot y_1^{-r} & \mod P \quad (7.7) \\ a^{q x_1} \equiv y_1 \cdot a^{-x_2} & \mod P \quad (7.8) \end{cases}$$

式(7.7)における乗算数$\fallingdotseq 2[\log_2 P]+1$

式(7.8)の右辺における乗算数$\fallingdotseq 2[\log_2 P]+1$

式(7.8)の x_1 を求めるのに，筆者の提案した改良型アルゴリズム[2]を用いると，必要な乗算数 n_{x_1}，メモリー量 m_{x_1} は，$q_1=2$ を考慮して

$$n_{x_1} \fallingdotseq q \cdot n \cdot (1/2+2\log_2 q_1)=5100 \quad (7.9)$$

$$m_{x_1} \fallingdotseq (2g-3+q_1-1)([\log_2 P]+1) + g([\log_2 P]+1) \fallingdotseq 11\,\text{kbit} \quad (7.10)$$

となる．さらに，改良型アルゴリズム(2)[2]を用いて，式(3.8)の展開係数 d_{ij} を，8個ごとに求める場合 ($l=8$) は，x_1 を求めるのに必要な乗算数は減少し，メモリー量は増加する．つまり，

$$n_{x_1}' \fallingdotseq 5100/8=640 \quad (7.11)$$

$$m_{x_1}' \fallingdotseq m_{x_1}+2^g([\log_2 P]+1) \quad (7.12)$$

となる．また，法 P のかわりに，法 $R \fallingdotseq 10^7$ を用いて，データ圧縮を行うと，メモリー量を減少させることができる．つまり，

$$m_{x_1}'' \fallingdotseq m_{x_1}+2^g([\log_2 R]+1) \fallingdotseq 24\,\text{kbit} \quad (7.13)$$

となる．(改良型アルゴリズム(2)では，d_{ij} を求める際に参照するデータテーブルを格納するとき，法Rを用いて，データ圧縮を行っている．)

したがって，復号化式に必要な乗算数 N_m，メモリー容量 M_m は

$$N_m \fallingdotseq 2634 \quad (7.14)$$

$$M_m \fallingdotseq 29\,\text{kbit} \quad (7.15)$$

となる．

さらに，a^{2^j}, b^{2^j} のテーブルを用いる場合は，

$$N_m \fallingdotseq 1638 \quad (7.16)$$

$$M_m \fallingdotseq 526\,\text{kbit} \quad (7.17)$$

となる．

8. 暗号文の冗長度

平文 (x_1, x_2) のもつ情報量は，

$$H_x=\log_2 A+\log_2 P \quad (8.1)$$

であり，暗号文 (y_1, y_2) のもつ情報量 H_y も H_x と同じであるはずだから

$$H_y=\log_2 A+\log_2 P \quad (8.2)$$

である．式(2.9)，(2.10)から，y_1, y_2 が独立に選べるならば，その情報量 H は

$$H=\log_2(P-1)+\log_2 P \quad (8.3)$$

となるはずであるが，y_1, y_2 には冗長さがあり，その冗長度 R_e は，

$$R_e=(H-H_y)/H = \log_2\{(P-1)/A\}/\log_2\{P(P-1)\} \quad (8.4)$$

であり，$A \fallingdotseq \sqrt{P}$ となるように選ぶと

$$R_e \fallingdotseq \frac{1}{2}\log_2 P/(2\log_2 P) \fallingdotseq 0.25 \quad (8.5)$$

となる．

ElGamal 暗号系における冗長度は

$$R_e=0.5$$

である．

9. あ と が き

離散的対数問題 $y \equiv a^x \mod P$ の難しさに基づいた公開鍵暗号系を提案した．ElGamal 暗号系との相違を明らかにして，本暗号系の有効性を示した．

今後は，本暗号系を用いて，認証通信が可能となることを示すこと，暗号化，復号化演算の計算量を減小させるアルゴリズムの開発が課題となる．

参 考 文 献

1) Pohlig, S. C and Hellman, M. E.: An Improved Algorithm for Computing Logarithms over GF(P) and Its Cryptographic Significance, *IEEE Trans. Inf. Theory*, Vol. IT-24, No. 1, pp. 106-110 (1978).
2) 八木沢正博：GF(Q) 上の対数計算アルゴリズム，情報処理学会論文誌，Vol. 28, No. 2, pp. 124-130 (1987).
3) 池野信一，小山謙二：現代暗号理論，pp. 92-93，電子通信学会，東京 (1986).
4) Davies, D. W. and Price, W. L.: 上園忠弘監訳：ネットワーク・セキュリティ，p. 202，日経マグロウヒル社，東京 (1985).

(昭和62年2月25日受付)
(平成元年6月13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．公開鍵暗号法に興味を持つ．