ランダム多項式を秘密鍵に有する多次多変数公開鍵暗号の拡張

境　　隆一†　　笠原　正雄††

† 大阪電気通信大学工学部
†† 大阪学院大学情報学部
E-mail: †sakai@isc.osakac.ac.jp

あらまし　筆者等はランダム多項式を秘密鍵として用い，逐次復号可能な多次多変数公開鍵暗号を提案してきた．この方式は，従来の代数的な復号を要する方式に比べて復号時の処理速度を大幅に向上することができる．本稿では，この復号処理の高速性を暗号の安全性向上のために利用した多次多変数公開鍵暗号を提案する．
キーワード　多次多変数，公開鍵暗号，ランダム連立方程式

Some Extentions of Multi-Variate Public Key Crytptosystems

Ryuichi SAKAI† and Masao KASAHARA††

† Osaka Electro-Communication University
†† Osaka Gakuin University
E-mail: †sakai@isc.osakac.ac.jp

Abstract　We have been proposed multi-variate public key cryptosystems based on random simultaneos equations(RSE(2)PKC). In thess system, the decryption algorithm can be done very fast as the encryption algorithm compared with the conventional algebraic decryption algorithm. Using the property of the fast decryption, we propose some new extension sof RSE(2)PKC and decryption algorithms. For the secure multi-valiate public key system, the new RSE(2)PKC seems apparantly secure compared with the original RSE(2)PKC [?].
Key words　multi-variate, public-key, cryptosystem, random simultaneos equation

1. まえがき

筆者等はランダム多項式を秘密鍵として用い，逐次復号可能な多次多変数公開鍵暗号 [1] [2] [3] を提案してきた．この方式は，従来の代数的な復号を要する方式 [4] に比べて復号時の処理速度を大幅に向上することができる．本稿では，この復号処理の高速性を暗号の安全性向上のために利用した多次多変数公開鍵暗号を提案する．

2. ランダムな連立方程式を用いた多次多変数公開鍵暗号 (RSE(2)PKC)

本章では，$\mathbb{F}_q$ 上の RSE(2)PKC の構成法について説明する．

2.1 変換と変数の記述

公開鍵作成時に使用する変換および変数を以下に示す．

平文ベクトルの次元	:	n
ブロック数	:	N
各ブロックの次元	:	$t = n/N$
正則線形変換行列	:	$A = (a_{i,j}), B = (b_{i,j}),\ a_{i,j}, b_{i,j} \in \mathbb{F}_q$
t 変数正則二次変換	:	$(\Phi^{(1)}(), \cdots, \Phi^{(N)}())$
連立二次方程式	:	$\Phi^{(j)}() = \left(f_1^{(j)}(), f_2^{(j)}(), \cdots, f_t^{(j)}\right)$
平文変数	:	$\boldsymbol{X} = (x_1, x_2, \cdots, x_n)$
線形変換後の変数	:	$\boldsymbol{Y} = (\boldsymbol{Y}_1, \cdots, \boldsymbol{Y}_N) = (y_1, \cdots, y_n)$
二次変換後の変数	:	$\boldsymbol{Q} = (\boldsymbol{Q}_1, \cdots, \boldsymbol{Q}_N) = (q_1, \cdots, q_n)$
乱数多項式	:	$\boldsymbol{R} = (\boldsymbol{R}_1, \cdots, \boldsymbol{R}_N) = (r_1, \cdots, r_n)$
多項式付加後の変数	:	$\boldsymbol{Z} = (\boldsymbol{Z}_1, \cdots, \boldsymbol{Z}_N) = (z_1, \cdots, z_n)$
公開鍵多項式	:	$\boldsymbol{K} = (\boldsymbol{K}_1, \cdots, \boldsymbol{K}_N) = (k_1, \cdots, k_n)$

ただし，正則二次変換の逆変換は，q^t の大きさの表を参照することによって行うものとする．

2.2 公開鍵生成

$\mathbb{F}_q$ 上の n 次元の平文ベクトル $\boldsymbol{M}=(m_1,m_2,\cdots,m_n)$ を代入する変数ベクトルとして $\boldsymbol{X}=(x_1,x_2,\cdots,x_n)$ を準備する．ただし，$m_i\in\mathbb{F}_q$ である．図1に示すように，これを以下の順に変換し公開鍵多項式ベクトル $\boldsymbol{K}=(k_1,k_2,\cdots,k_n)$ を生成する．

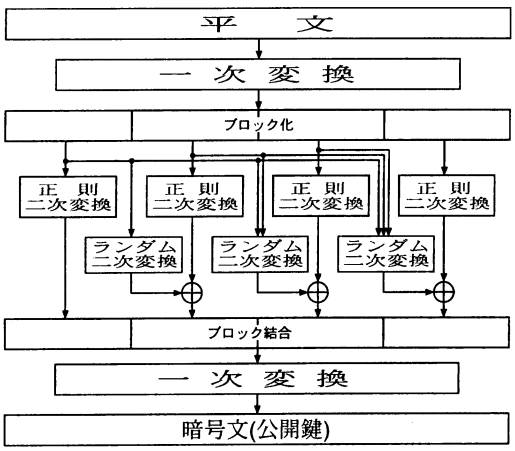

図1　公開鍵の構成法 (RSE(2)PKC)

Step1: $\boldsymbol{X}$ を線形変換 A により変換し，$\boldsymbol{Y}$ を得る．

$$\boldsymbol{Y}=\boldsymbol{X}A. \tag{1}$$

Step2: $\boldsymbol{Y}$ を t 変数毎にブロック化して $\boldsymbol{Y}_j$ を得，これを二次変換 $\Phi^{(j)}$ により変換し

$$\boldsymbol{Q}=(\boldsymbol{Q}_1,\cdots,\boldsymbol{Q}_N)=(\Phi^{(1)}(\boldsymbol{Y}_1),\cdots,\Phi^{(N)}(\boldsymbol{Y}_N)) \tag{2}$$

を得る．

Step3: 乱数多項式ベクトル $\boldsymbol{R}_j$ を $\boldsymbol{Q}_j$ に加え，$\boldsymbol{D}$ を得る．

$$\boldsymbol{Z}=\boldsymbol{Q}+\boldsymbol{R}=(\boldsymbol{Q}_1,\cdots,\boldsymbol{Q}_N)+(\boldsymbol{R}_1,\cdots,\boldsymbol{R}_N). \tag{3}$$

Step4: $\boldsymbol{Z}$ を線形変換 $\boldsymbol{B}$ により変換し，公開鍵多項式ベクトル $\boldsymbol{K}$ を得る．

$$\boldsymbol{K}=\boldsymbol{D}B. \tag{4}$$

ここで，線形変換 A,B および，二次変換 $\boldsymbol{Q}_j$ を構成する二次連立方程式はランダムに生成された正則な変換であり，乱数多項式ベクトル $\boldsymbol{R}_{j+1}$ は次のような変数より構成されている．

$$\begin{aligned}\boldsymbol{R}_{j+1}&=\boldsymbol{R}_{j+1}(Y_1,Y_2,\cdots,Y_j)=\boldsymbol{R}_{j+1}(y_1,y_2,\cdots,y_{tj})\\&=\begin{pmatrix}r_{tj+1}\\r_{tj+2}\\\vdots\\r_{t(j+1)}\end{pmatrix}^t=\begin{pmatrix}r_{tj+1}(y_1,\cdots,y_{tj})\\r_{tj+2}(y_1,\cdots,y_{tj})\\\vdots\\r_{t(j+1)}(y_1,\cdots,y_{tj})\end{pmatrix}^t\end{aligned} \tag{5}$$

また，各乱数多項式 $\boldsymbol{r}_i$ の係数 $r_{i,k,l}\in\mathbb{F}_q$ は次のように構成されている．

$$r_i=r_i(y_1,y_2,\cdots,y_{tj})=\sum_{k,l=0}^{tj}r_{i,k,l}y_ky_l \tag{6}$$

ただし，$tj+1\leqq i\leqq t(j+1)$ であり，簡単のため $y_0=1$ としている．

3. RSE(2)PKC の拡張

本章では，RSE(2)PKC の新しい拡張法とその復号法を提案する．

3.1 公開鍵の構成

前章で示したように，乱数多項式を逐次付加して公開鍵を作成し，復号次にこの乱数多項式を逐次取り除く RES(g)-PKC においては，公開鍵作成時に $x\longrightarrow$ [一次変換，ブロック化] $\longrightarrow y\longrightarrow$ [二次変換+逐次乱数多項式付加] $\longrightarrow z\longrightarrow$ [一次変換] $\longrightarrow z$ という変換をしているため，変数 y を用いて公開鍵を並べて見た場合の係数を行列表現すると，この行列を行操作によって三角化することができる(注1)．例えば 8 次元の平文に対して，2 変数づつブロック化している場合 ($t=2$)，z_i を

$$z_i=\sum_{k,l=1}^{n}z_{k,l}y_ky_l, \tag{7}$$

として，この係数 $a_{i,j}$ を z_i ごとに横に列べて表示すると表 1 のようになる．

表1　z_i の係数 $z_{k,l}$(従来方式)

(空白は 0 の係数，記号 * は非零となり得る係数)

k	1 1 2 1 2 3 1 2 3 4 1 2 3 4 5 1 2 3 4 5 6 1 2 3 4 5 6 7 1 2 3 4 5 6 7 8
l	1 2 2 3 3 3 4 4 4 4 5 5 5 5 5 6 6 6 6 6 6 7 7 7 7 7 7 7 8 8 8 8 8 8 8 8
z_1	* * *
z_2	* * *
z_3	* * * * * * * * * *
z_4	* * * * * * * * * *
z_5	* *
z_6	* *
z_7	* *
z_8	* *

表1に示すように，変数 y で公開鍵を表した場合，適当な線

(注1)：(注意) 攻撃者は直接 y の表現を得ているわけではないので，攻撃者はこの三角化を直ちに実行できるわけではない

形変換により多項式の係数の多くが 0 となる．このような三角化が公開鍵の変形によって実現される場合，逐次復号と同様の方法で平文を解読されてしまう．

本章で提案する拡張方式は，この 変数 y により三角化された場合において，多項式の係数が 0 となる箇所を減らす方式である．

3.2 拡張方式 I

3.2.1 公開鍵の構成

公開鍵の構成において，ベクトル $\boldsymbol{Y}$ の成分のうち，10 数ビット程度に対応する変数を ベクトル $\boldsymbol{Y}$ の後列から s 個選び，これを $\boldsymbol{Y}_j$ の成分と重ならない乱数多項式ベクトル $\boldsymbol{R}_j$ の変数に追加する．すなわち $q^s = 2^{10} \sim 2^{15}$ 例えば，図 2 のように $s = t$ 個の変数 $\boldsymbol{Y}_N = (y_{n-t+1}, \cdots, y_n)$ を乱数多項式 $r_i (i = 1, 2, \cdots, n-t)$ の変数として加える．

$$r_i = r_i(y_1, \cdots, y_{tj}, y_{n-t+1}, \cdots, y_n) \tag{8}$$

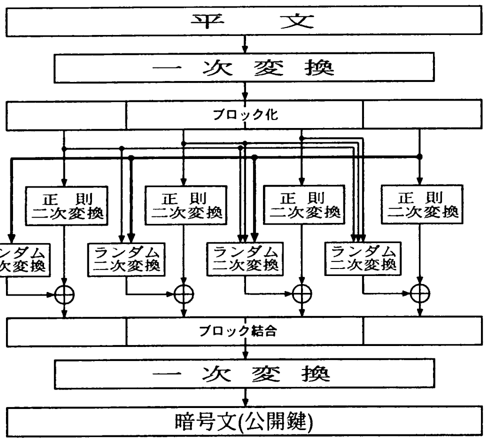

図 2 公開鍵の構成法 (RSE(2)-PKC の拡張)

図 2 の公開鍵構成において，平文の次元を 8，各ブロックの変数の個数を 2 とすると，係数行列は表 2 のようになる．これを表 1 の係数行列と比べると，係数が 0 とならない可能性のある箇所が増加している．これにより，安全性が向上していると考えられるが，q^s 回分の 復号を並列に行う必要があり、計算時間が増加する．

3.2.2 復 号 法

復号の手順は，乱数多項式の変数として追加した s 個の変数が取り得る全ての値を各々の場合にわけて代入して，これらの全ての場合の復号を並列に実行する．図 2 の構成の場合，Y_4 が乱数多項式に追加される変数であるが，Y_4 の取り得る値全てについて復号を実行し，Y_4 が正則二次逆変換により復号された時点で 一致する Y_4 を見いだして Y_4 の値を確定するという手順で平文の復号を行う．すなわち，Y_4 の取り得る値の個数は q^s であるので，従来の RSE(2)PKC の q^s 倍の復号時間を必要とする．また，ランダム二次多項式に新に付け加えた t 変数によって，平文と暗号文の一対一の対応関係が失われる可能性があり，この場合，復号文が一意に定まらない場合が発生する．

表 2 z_i の係数 $z_{k,l}$(拡張方式 I)

(空白は 0 の係数，記号 *, ! は非零となり得る係数)

k	1	1	2	1	2	3	1	2	3	4	1	2	3	4	5	1	2	3	4	5	6	1	2	3	4	5	6	7	1	2	3	4	5	6	7	8
l	1	2	2	3	3	3	4	4	4	4	5	5	5	5	5	6	6	6	6	6	6	7	7	7	7	7	7	7	8	8	8	8	8	8	8	8
z_1	*	*	*																									!							!	!
z_2	*	*	*																									!							!	!
z_3	*	*	*	*	*	*	*	*	*	*												!	!					!	!	!					!	!
z_4	*	*	*	*	*	*	*	*	*	*												!	!					!	!	!					!	!
z_5	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	!	!	!	!			!	!	!	!	!			!	!
z_6	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	!	!	!	!			!	!	!	!	!			!	!
z_7	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
z_8	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*

3.3 拡張方式 II

拡張方式 I では，変数ベクトル Y の後列から順に変数 y_i を選んだが，各ブロックから変数 y_i を選ぶことも可能である．このようにした場合の公開鍵の構成法を図 3 に示す．

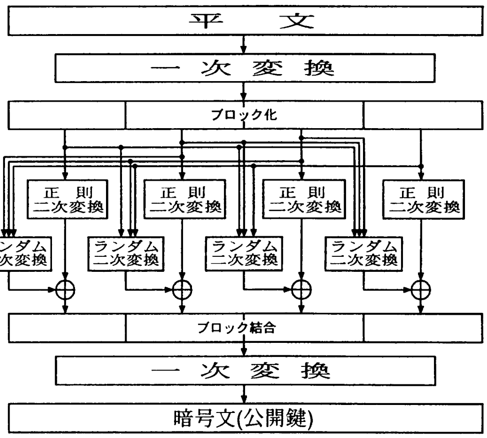

図 3 公開鍵の構成法 (RSE(2)-PKC の拡張 II)

拡張方式 II においては，各ブロックにおいて 復号時に想定している y_i を正則二次逆変換により復号した際に，y_i が一致しなかった場合，そこで幾つかの並列実行している復号処理を除去することができる．

3.4 拡張方式 III

平文に冗長変換を行うことにより，平文と暗号文の対応関係が一対一で無くなった場合においても，十分高い確率で復号を行うことができる．

さらに，拡張方式 I および II の方式において，公開鍵の一部

を非公開とする方式が考えられる．このようにした場合の公開鍵の構成法を図 4 に示す．ただし，この場合，一定の確率で復号エラーとなるが，複数の暗号文ブロックに渡ってハッシュ値を取る等の工夫により，復号エラーを小さくすることができる．

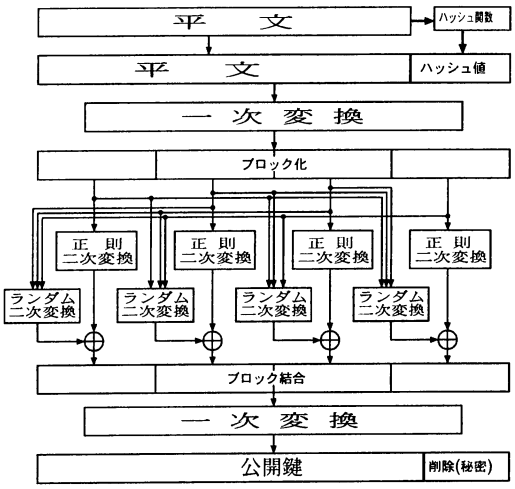

図 4　公開鍵の構成法 (RSE(2)-PKC の拡張 III)

3.5　拡張方式 IV

表?? のような構造を攻撃者が知ったとき，攻撃者は z_1, z_2 の多項式から逐次解読を行う．したがって，図 5 のように，平文にハッシュ関数で冗長を付加し，z_1, z_2 の項を公開鍵から削除することにより，このような攻撃が困難となる公開鍵を構成する方式が考えられる．この図 5 のような公開鍵構成法を用いた拡張 RSE(2)PKC においては，復号時に $\boldsymbol{Y}_1$ の取り得る全ての値を想定した復号を並列に行い，得られた複数の平文の中から正しい平文をハッシュ値の一致により見出すという手順で復号を行う．

3.6　ハイブリッド拡張方式

公開鍵作成時に変数ベクトル $\boldsymbol{Y}$ を用いるが，これをブロック化する際，$\boldsymbol{Y}_1, \boldsymbol{Y}_2, \cdots, \boldsymbol{Y}_{N-1}$ の変数ベクトルについては，正則二次逆変換が表の参照により可能な大きさの t 変数とし，Y_N の変数の個数をビット換算で 80 ビット程度する．さらに，Y_N の変数のうち，ビット換算で 10 数ビット程度に対応する s 個の変数を乱数多項式ベクトル R_j の変数に加える方式を考える．この場合，$\boldsymbol{Q}_N$ から $\boldsymbol{Y}_N$ の正則二次逆変換は，文献 [5] で提案されている代数的復号が可能なように，正則二次変換 Φ_N を構成しておく．

3.7　拡張方式の復号文の多値性

復号に際して，想定する s 個の変数が正しいものと異る場合，代数的復号 Φ_N^{-1} に入力される Q_N の実現値は，ランダムな値をとると仮定すると，これを Φ_N^{-1} によって逆変換した $\boldsymbol{Y}_N$ の

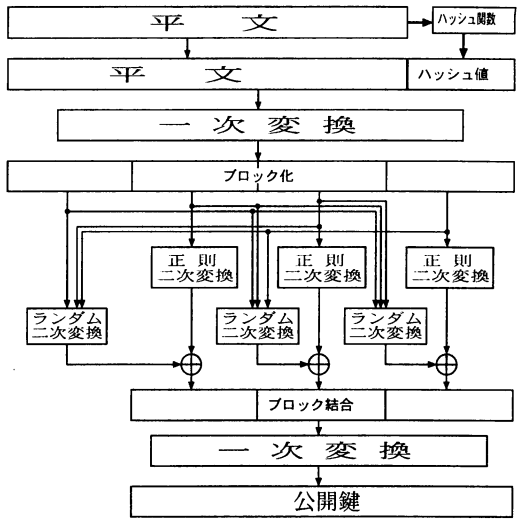

図 5　公開鍵の構成法 (RSE(2)-PKC の拡張 IV)

実現値もランダムな値と考えられるので，これが想定した正しい s と一致する確率は q^{-s} である．並列実行で得られる実現値は q^s 個程度であるので，想定した s 個の変数の実現値と復号された $\boldsymbol{Y}_N$ の実現値が一致する期待値は 1 となる．乱数多項式にある制約を設けることにより，平文と暗号文の対応が一対一になるような乱数多項式が存在すると考えられるが，このような乱数多項式の構成については今後の課題としたい．

4.　ま と め

本稿では，RSE(2)PKC の幾つかの拡張法を提案した．提案した何れの方式も，並列復号をすることが必要であり，RSE(2)PKC よりも復号時間を多く必要とするが，RSE(2)PKC よりも少なくとも安全性が向上していると考えられる．

文　献

[1] M. Kasahara and R. Sakai, " A Construction of Public Key Cryptosystem for Realizing Ciphertext of size 100 bit and Digital Signature Scheme", IEICE Trans. Vol. E87-A,1,pp102-109, (2004-01).

[2] M. Kasahara and R. Sakai : "Notes on public key cryptosystem based on multivariate polynomials of high degree", Technical Report of IEICE, ISEC 2001-64 (2001-9).

[3] M. Kasahara and R. Sakai : " A Construction of 100 bit Public-Key Cryptosystem and Digital Signature Scheme", Proc. of SCIS2003,C8-2,(2003-01).

[4] N. T. Courtois, "The HFE public key encryption and signature", http://www.hfe.info.

[5] T. Matsumoto and H. Imai : "Public quadratic Polynomial-tuples for efficient signature-verification and message-encryption", Proc. of Eurocrypt '88, Springer-Verlag, 419-453, (1989).

[6] N. Koblitz : "Algebraic Aspects of Cryptography", Springer-Verlag Berlin Heidelberg,(1998).