# 新しいランダム多次多変数型公開鍵暗号の構成法

大阪学院大学 情報学部
笠原 正雄

# Abstract

本論文では、$g$次$n$変数連立方程式に基づく公開鍵暗号(RSE($g$)PKC)の新しいクラスを提案する。すなわち本論文では、$g \geq 2$として、

1. 3種類のランダムな1次→2次変換に基づく、新しいクラスの$g$次$n$変数暗号(K(I)・RSE($g$)PKCと呼ぶ)の一般的な構成法を提案する。提案手法では、全ての段階で、代数的1次→$g$次変換を使用していない。
2. K(I)・RSE($g$)PKCの中で特に部分2次変換に正則性を要求しないK(I)・RSSE($g$)PKCを提案する。
3. K(I)・RSE($g$)PKC、 K(I)・RSSE($g$)PKCでは、暗号文長を$n$として、n次元のランダムノイズベクトルを付加して暗号化している。
4. K(I)・RSSE($g$)PKC暗号が、大きなランダム性を与えられ、かつ部分2次変換のサイズが大となっていることによって、グレブナー基底(GB)攻撃、Patarin攻撃、Braeken-Wolf-Preneel攻撃等の従来の優れた攻撃に対し、強い耐性を有し得ることを明らかにする。

# Toy Example

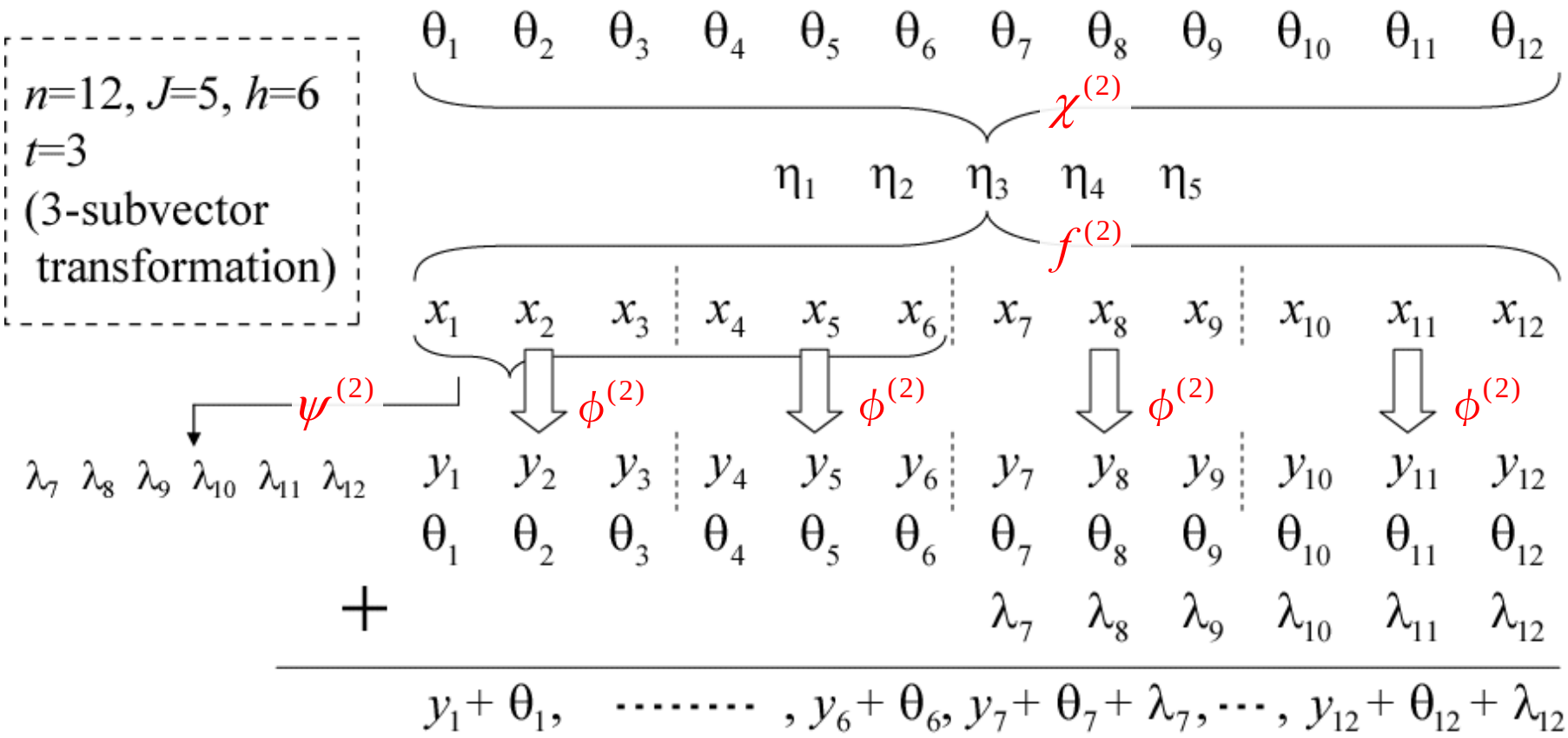


Fig. 1: Toy example for fundamental scheme.

# Definition 1

The following transformation:

$$\Phi(X) = Y, \qquad (5)$$

is referred to as “non-singular”, if and only if the transformation has the following inverse transformation:

$$\Phi^{(-1)}(Y) = X, \qquad (6)$$

for any given $Y$ in a unique manner. On the other hand if the inverse-transformed value does not exist in a unique manner, for a given $Y$, the transformation is referred to as “singular”.

# Message Structure

$$\boldsymbol{m} = (m_1, m_2, \cdots, m_k) \text{ over } \mathbb{F}_2,$$
$$\boldsymbol{m}_\rho = (m_1, m_2, \cdots, m_k, h_1, \cdots, h_g) \text{ over } \mathbb{F}_2,$$

where

$$(h_1, h_2, \cdots, h_g) = h(m_1, m_2, \cdots, m_k)$$

and $h(m_1, m_2, \cdots, m_k)$ is a hash function.

$$\boldsymbol{m}_\rho \cdot A = \boldsymbol{x} = (x_1, x_2, \cdots, x_n),$$
$$\boldsymbol{x} = (X_1, \cdots, X_H; X_{H+1}, \cdots, X_N)$$

where $X_i = (x_{i1}, x_{i2}, \cdots, x_{it})$.

# Random Transformation $\phi^{(2)}$

$$
\begin{aligned}
y_{i1} &= \phi_{i1}^{(2)}(x_{i1}, x_{i2}, \cdots, x_{it}), \\
&\vdots \\
y_{ij} &= \phi_{ij}^{(2)}(x_{i1}, x_{i2}, \cdots, x_{it}), \\
&\vdots \\
y_{it} &= \phi_{it}^{(2)}(x_{i1}, x_{i2}, \cdots, x_{it}).
\end{aligned}
$$

# Random Transformation $f^{(2)}$

Given $(x_1, x_2, \cdots, x_n)$, the following transformation is performed:

$$
\begin{aligned}
\eta_1 &= f_1^{(1)}(x_1, x_2, \cdots, x_n), \\
&\vdots \\
\eta_i &= f_i^{(1)}(x_1, x_2, \cdots, x_n), \\
&\vdots \\
\eta_J &= f_J^{(1)}(x_1, x_2, \cdots, x_n).
\end{aligned}
$$

# Random Transformation $\chi^{(2)}$

Given $(\eta_1, \eta_2, \cdots, \eta_J)$, the following quadratic transformation is performed:

$$\begin{aligned}
\theta_1 &= \chi_1^{(2)}(\eta_1, \eta_2, \cdots, \eta_J), \\
&\vdots \\
\theta_i &= \chi_i^{(2)}(\eta_1, \eta_2, \cdots, \eta_J), \\
&\vdots \\
\theta_J &= \chi_n^{(2)}(\eta_1, \eta_2, \cdots, \eta_J).
\end{aligned}$$

$J$ is chosen so that $\theta_i$'s may be linear independent.

# Random Transformation $\psi^{(2)}$

Given $(x_1, x_2, \cdots, x_h)$, the following random transformation is performed:

$$\begin{aligned}
\lambda_{h+1} &= \psi^{(2)}_{h+1}(x_1, x_2, \cdots, x_h), \\
&\vdots \\
\lambda_{h+i} &= \psi^{(2)}_{h+i}(x_1, x_2, \cdots, x_h), \\
&\vdots \\
\lambda_{n} &= \psi^{(2)}_{n}(x_1, x_2, \cdots, x_h),
\end{aligned}$$

where $h=Ht$.

# Final Transformation

From $\{x_i\}$, $\{\theta_i\}$ and $\{\lambda_i\}$, we have the following vector over $\mathbb{F}_2$:

$$\boldsymbol{v} = (y_1 + \theta_1, \cdots, y_h + \theta_h, y_{h+1} + \theta_{h+1} + \lambda_{h+1}, \cdots, y_n + \theta_n + \lambda_n)$$

In the following, we shall denote the $i$-th component of $\boldsymbol{v}$ by $v_i$.

The following final transformation is now performed, yielding a set of public keys:

$$\boldsymbol{v}B = (K_1, K_2, \cdots, K_n),$$

where $B$ is an n × n non-singular matrix over $\mathbb{F}_2$.

# Set of Keys

Public Keys : $K = \{K_i\}$

Secret Keys : $\phi^{(2)}, f^{(1)}, \chi^{(2)}, \psi^{(2)}, A, B$

# Toy Example

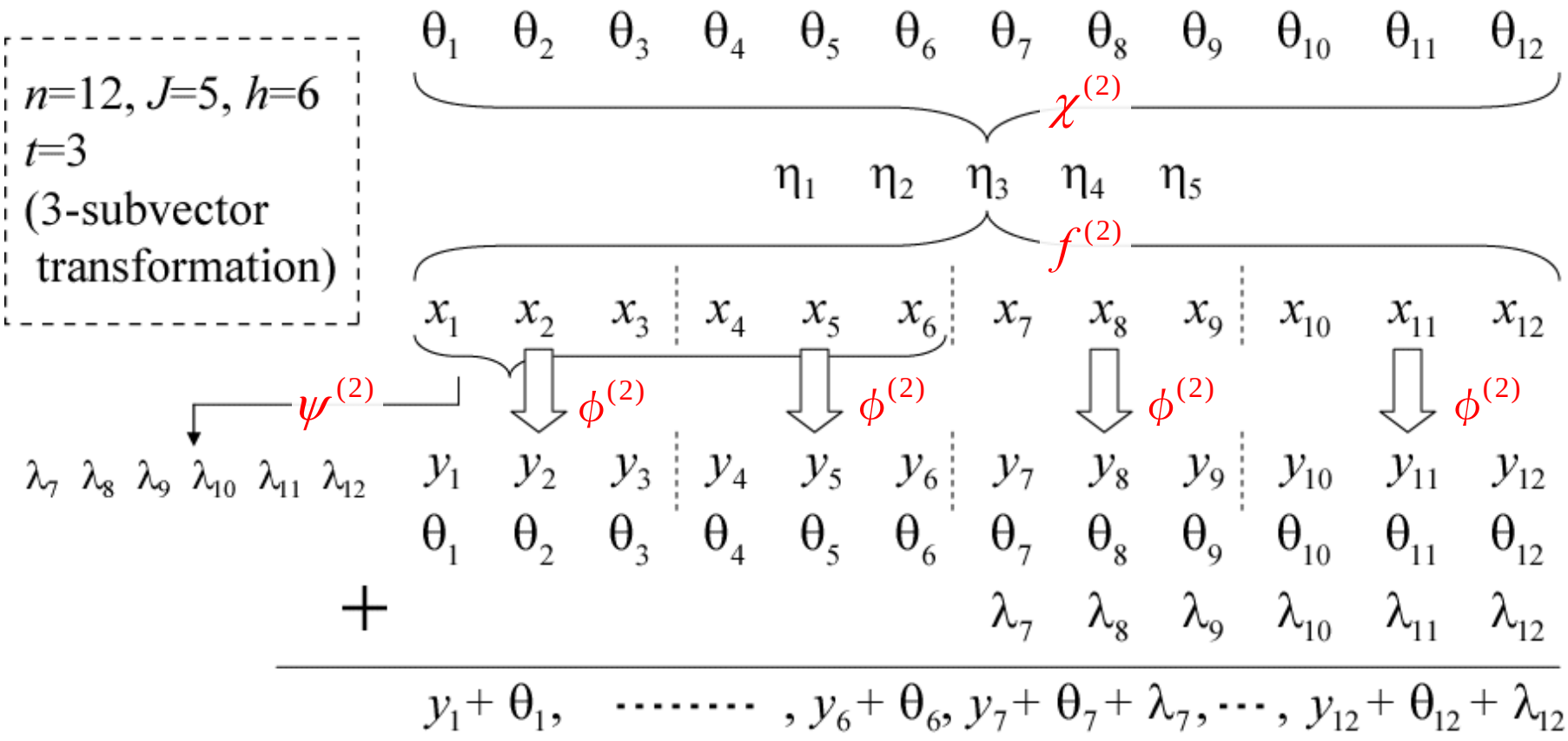


Fig. 1: Toy example for fundamental scheme.

# Definition 2

The ambiguity of transformation $\Phi^{(g)}$, $|\Phi^{(g)}|$ is defined as

$$|\Phi^{(g)}| = \log_2 \#\Phi^{(g)} \quad \text{(bits)}.$$

where $\#\Phi^{(g)}$ is the number of different transformation.

# Comparison

Table 1: Comparison

| $t$ | $\lvert\Phi^{(2)}\rvert_u$ (bits) | $\lvert \not{\Phi}^{(2)}\rvert$ |
|---|---|---|
| 3 | 9 | 8.6 |
| 4 | 24 | 11.5 |

# Ambiguity

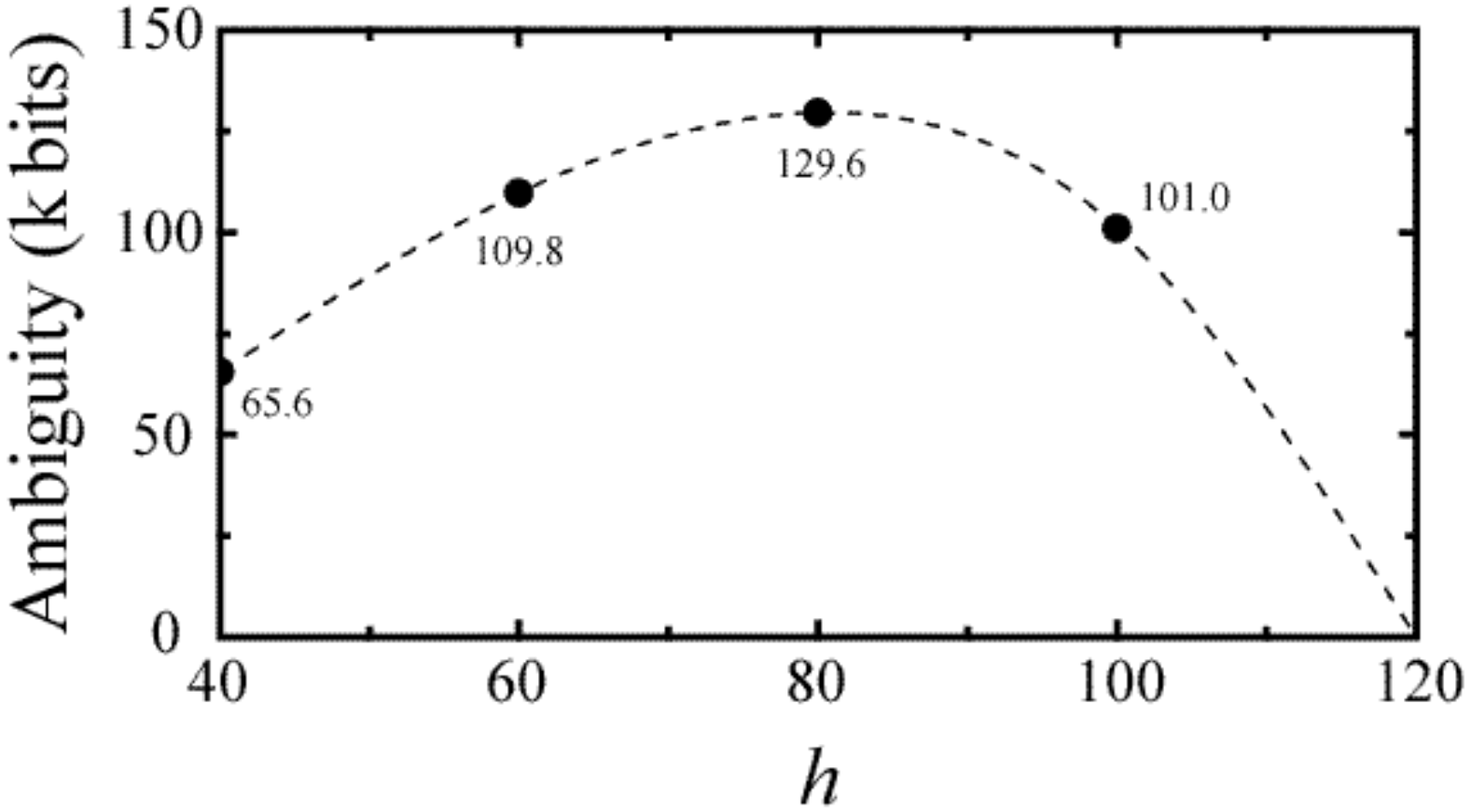


Fig. 2: Ambiguity of $\psi^{(2)}$ added on $\boldsymbol{v}$.

# Example of $|\boldsymbol{v}_t|$

For example, $|\boldsymbol{v}_t|$ for $t$=3 and 4 are given as follows:

$$|\boldsymbol{v}_3| = 8.6 + 360 = 368.6 \text{ (bits)},$$
$$|\boldsymbol{v}_4| = 11.5 + 480 = 491.5 \text{ (bits)},$$

yielding sufficiently large value.

## K·RSSE(*g*)PKC – K·RSE(*g*)PKC using singular SE's –

Given $X_i$ ($i$=1,2,$\cdots$,N), the following transformation is performed under the condition that all the coefficients of $y_i^{(g)}$ are given in a random manner:

$$
\begin{aligned}
y_{i1} &= \phi_{s,i1}^{(2)}(x_{i1}, x_{i2}, \cdots, x_{it}), \\
&\vdots \\
y_{ij} &= \phi_{s,ij}^{(2)}(x_{i1}, x_{i2}, \cdots, x_{it}), \\
&\vdots \\
y_{it} &= \phi_{s,it}^{(2)}(x_{i1}, x_{i2}, \cdots, x_{it}),
\end{aligned}
$$

where we assume $20 \lesssim t \lesssim 40$.

# Expectation of Number of Decodings

**Expectation of number of decodings for each $\Phi_S^{(2)}$, $E(\boldsymbol{x}_t)$**

$N(\boldsymbol{x}_t|\boldsymbol{y}_t)$: Number of different $\boldsymbol{x}_t$'s given randomly to $\boldsymbol{y}_t$.

$P_N(i)$: Probability that $N(\boldsymbol{x}_t|\boldsymbol{y}_t)$ takes on value $i$.

$$P_N(0) \cong \mathrm{e}^{-1},$$

$$P_N(i) \cong \frac{1}{i!} P_N(0),$$

$$E(\boldsymbol{x}_t) \cong \mathrm{e} \cdot P_N(0) = 1.$$

# Example of $E(x_t)$ and $|\phi_s^{(2)}|$

$$
\begin{aligned}
|\varphi_s^{(2)}| &= 4200 \ \text{(bits)}, \quad (t = 20) \\
&= 13950 \ \text{(bits)}, \quad (t = 30) \\
&= 32800 \ \text{(bits)}, \quad (t = 40)
\end{aligned}
$$

For comparison,

$$
\left.
\begin{aligned}
|\varphi_s^{(2)}| &= 8.6 \ \text{(bits)}, \quad (t = 3) \\
&= 11.5 \ \text{(bits)}, \quad (t = 4)
\end{aligned}
\right\} \text{Non-singular trans.}
$$

# Simplified Version of K·RSSE(g)

We have seen that the transformation $\chi^{(2)}$ and $\phi_s^{(2)}$ yield a large ambiguity on any components of $(X_1, X_2, \cdots, X_N)$. As we have given in Remark I, the large ambiguity of transformation $\psi^{(2)}$ can be only given on $(X_{H+1}, X_{H+2}, \cdots, X_N)$, the using of the transformation can be omitted without deteriorating the security of K(I)·RSSE($g$)PKC.

In this simplified version of K(I)·RSSE($g$)PKC where $\psi^{(2)}$ is omitted, the ambiguity given on any components of $(X_{H+1}, X_{H+2}, \cdots, X_N)$ on the basis of $\chi^{(2)}$ and $\phi_s^{(2)}$ is given by $120 \cdot 30 + 13950 = 17550$, yielding a sufficiently large value.

# Concluding Remarks

(1) An $n$-dimensional noise vector $\theta=(\theta_1, \theta_2, \cdots, \theta_n)$ has no step-wise triangular structure.

(2) The vector $(y_1, y_2, \cdots, y_n)$ has no step-wise triangular structure.

(3) The addition of $(\lambda_{h+1}, \lambda_{h+2}, \cdots, \lambda_n)$ on $(y_{h+1}, y_{h+2}, \cdots, y_n)$ yields a unite-step triangular structure. On this matter, it is recommended that the step width $t$ may meet the relation: $t = n/2 \gtrsim 60$.

(4) The using of a quadratic random transformation of a large width $t$ result in a singular transformation with probability almost 1.0. As the result, when performing the inverse transformation, the repetition of decoding is required. However, we have shown that the number of total repetition is surprisingly small.

# Table 2: Examples of K(I)·RSSE(g)PKC

Table 2: Examples of K(I)·RSSE(g)PKC

| | | |
|---|---|---|
| Number of variables, $n$ | 120 | 128 |
| Width of transformation, $t$ | 24 | 32 |
| Size of public key, $S_{PK}$ | 108.9 KB | 132.1 KB |
| Total size of decoding tables, $S_T$ | 96 MB | 128 GB* |

(* A very large value at the present standard (Sept. 2007).)