Construction of a new class of SE(g)PKC

- Along with some notes on *K*-Matrix・PKC –

Faculty of Informatics, Osaka Gakuin University

Masao Kasahara

kasahara@utc.osaka-gu.ac.jp

Order of Presentation

1. $K_I \cdot \mathrm{SE}(g)\mathrm{PKC}$ —— △

2. $K_{II} \cdot \mathrm{SE}(g)\mathrm{PKC}$ —— △

3. $K_{III} \cdot \mathrm{SE}(g)\mathrm{PKC}$ —— ○

---

4. $\tilde{K} \cdot \mathrm{SE}(g)\mathrm{PKC}$ —— ○

Preliminary

Message $\boldsymbol{u} = (u_1, u_2, \cdots, u_n)$ over F_{2^m} :

$$\Phi(\boldsymbol{u}) \to \boldsymbol{v} = (v_1, v_2, \cdots, v_n),$$

where $v_i \in F_2$.

$$\boldsymbol{V} = (V_1, V_2, \cdots, V_n),$$

where $V_i \in F_{2^m}$.

$$\tilde{V}(X) = \alpha_1 V_1 + \alpha_2 V_2 X + \cdots + \alpha_L V_L X^{L-1},$$
$$\tilde{V}(X)^e = W_1 + W_2 X + \cdots + W_J X^{J-1} + \cdots + W_L X^{L-1} \bmod G(X).$$

$K_I \cdot SE(g)PKC$

$$(W_1, W_2, \cdots, W_J)L_A = (K_1, K_2, \cdots, K_J),$$

where $W_J \in \{W_i\} - \{W_i\}_{\text{sub}}$.

$$(w_{J+1,1}, \cdots, w_{J+1,m}; \cdots; w_{(L-1)m+1,1}, \cdots, w_{(L-1)m+1,m})L_A$$
$$= (k_{J+1,1}, \cdots, k_{Lm,m}),$$

Public Key: $\{K_i\}, \{k_i\}$

Secret Key: $G(X), \{\alpha_i\}, L_A$

Example 1

$K_I \cdot \mathrm{SE}(g)\mathrm{PKC}:$

$$n = 96, m = 8, L = 12, J = 8, e = 3$$

Sizes of public keys, $S_{\mathrm{PK}}(K)$ and $S_{\mathrm{PK}}(k)$, are given by

$$S_{\mathrm{PK}}(K) = {}_{12}\mathrm{H}_3 \cdot mJ = 23296 \quad \text{(bits)}$$

and

$$S_{\mathrm{PK}}(k) = {}_{96}\mathrm{H}_2 \cdot m(N - J) = 148992 \quad \text{(bits)},$$

respectively.

Total sizes of public keys are given by

$$S_{\mathrm{PK}}(K) + S_{\mathrm{PK}}(k) = 172288 \quad \text{(bits)},$$

yielding shorter public key.

$K_{II} \cdot SE(g)PKC$

$$\tilde{V}(X) = \alpha_1 V_1^{d_1} + \alpha_2 V_2^{d_2} X + \cdots + \alpha_L V_L^{d_L} X^{L-1},$$

where d_i is a positive integer.

$$\tilde{V}^e(X) = \tilde{U}_1 + \tilde{U}_2 X + \cdots + \tilde{U}_L X^{L-1} \bmod G(X).$$

Letting an $L \times L$ non-singular matrix over F_{2^m} be L_C, we have

$$(\tilde{U}_1, \tilde{U}_2, \cdots, \tilde{U}_L) L_C = (U_1, U_2, \cdots, U_L).$$

Example 2

$K_{II} \cdot \mathrm{SE}(g)\mathrm{PKC}:$

$$V(X) = \alpha_1 V_1^3 + \alpha_2 V_2 X,$$

$$\tilde{V}(X)^3 = \tilde{U}_1 + \tilde{U}_2 X \quad \mathrm{mod} \quad \Gamma_1 + \Gamma_2 X + X^2,$$

$$L_D = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix},$$

$$U_1 = \alpha \tilde{U}_1 + \gamma \tilde{U}_2$$

$$U_2 = \beta \tilde{U}_1 + \delta \tilde{U}_2,$$

$$U_1^{(L)} = \alpha\alpha_1^3 V_1^9 + (\alpha\Gamma_1\Gamma_2\alpha_2^3 + \gamma\Gamma_1\Gamma_2 + \gamma\Gamma_3^3)V_2^3,$$

$$U_1^{(H)} = \gamma\alpha_1^2 V_1^6 V_2 + (\alpha\Gamma_1\alpha_1\alpha_2^2 + \gamma\Gamma_2\alpha_1\alpha_2^2)V_1^3 V_2^2,$$

$$U_2^{(L)} = \beta\alpha_1^3 V_1^9 + (\beta\Gamma_1\Gamma_2\alpha_2^3 + \delta\Gamma_1\Gamma_2 + \delta\Gamma_3^3)V_3^3,$$

$$U_2^{(H)} = \delta\alpha_1^2\alpha_2 V_1^6 V_2 + (\beta\Gamma_1\alpha_1\alpha_2^2 + \delta\Gamma_2\alpha_1\alpha_2^2)V_1^3 V_2^2.$$

Set of Key

Public Key:

$\{K_i + k_i\}$, where k_i is given by $k_i = (k_{i1}, k_{i2}, \cdots, k_{im})$.

Secret Key:

$\{\alpha_i\}, \{d_i\}, G(X), L_D$

Example 3

$K_{II} \cdot \text{SE}(g)\text{PKC}:$

$$m = 5, \lambda = 12, L = 23, e = 3, d_i = \begin{cases} 3; (i = 1,2,\cdots,12) \\ 1; (i = 13,14,\cdots,23) \end{cases}.$$

Number of low-degree terms, N_L : $N_L = 90.$

Number of high-degree terms, N_H : $N_H = 2510.$

The size of public key $\{k_i\}$: $S_k = 177100$ (bits).

The size of public key $\{K_i\}$: $S_K = 288650$ (bits).

The size of public key, S_{PK} : $S_{\text{PK}} = 465750$ (bits).

Size of Public Key

Table1: Size of public key for reduced version of $K_{II} \cdot \mathrm{SE}(g)\mathrm{PKC}$ in Example 3.

SK_d	SK_1	SK_2	SK_3	SK_4	Total size
Size (in bits)	2645	765325	1138500	897000	2803470
Number of terms in an expanded equation	115	6655	9900	7800	24470

$K_{III} \cdot SE(g)PKC$

$$k_i = (k_{i1}, \cdots, k_{iq}, \cdots, k_{im}), \quad (i = 1, 2, \cdots, L),$$

$$k_{i,q_i} = \sum_{i,j,(i \neq j)} \lambda_{ij,q_i} v_i v_j + \sum_i \lambda_{i,q_i} v_i,$$

$$r_{i,q_i} = \sum_{i,j,(i \neq j)} r_{ij,q_i} v_i v_j + \sum_i r_{i,q_i} v_i.$$

Public Key:

$$\{K_i + (k_{i1}, \cdots, k_{iq_i} + r_{iq_i}, \cdots, k_{im})\}, \{r_{i,q_i}\}$$

Secret Key:

$$\{\alpha_i\}, \{d_i\}, G(X), L_D, \{q_i\}$$

$\tilde{K} \cdot SE(g)PKC$

$$\tilde{K} = \begin{bmatrix} \alpha'_{11} & \lambda_2\alpha_{11} & & \lambda_k\alpha_{11} & \alpha''_{11} \\ & & & & \\ \alpha'_{1k} & \lambda_2\alpha_{1k} & & \lambda_k\alpha_{1k} & \alpha''_{1k} \\ R_1 & R_2 & & R_k & R_{k+1} \end{bmatrix},$$

where α'_{1j} and α''_{1j} are given as

$$\alpha'_{1j} + \alpha''_{1j} = \alpha_{1j},$$

and

$$R_1 + R_{k+1} = 0.$$

$\widetilde{K} \cdot SE(g)PKC$

$$E = (E_1, E_2, \cdots, E_k, E_{k+1}),$$

$$U = (U_1, U_2, \cdots, U_k, U_{k+1}),$$

$$E_i = W_1 + W_2 + \cdots + W_p,$$

$$W_i = \alpha_i V_{i1}^{(i1)} \cdot V_{i2}^{(i2)} \cdots\cdots V_{ig}^{(ig)}.$$

$\tilde{K} \cdot SE(g)PKC$

$$E\tilde{K} + U = (Z_1, Z_2, \cdots, Z_{k+1}),$$

$$\begin{aligned}
Z_1 &= E_1\alpha'_{11} + \cdots + E_k\alpha'_{1k} + E_{k+1}R_1 + U_1 \\
&\vdots \\
Z_i &= E_1\lambda_i\alpha'_{11} + \cdots + E_k\lambda_i\alpha_{1k} + E_{k+1}R_i + U_i \\
&\vdots \\
Z_k &= E_1\lambda_k\alpha'_{11} + \cdots + E_k\lambda_k\alpha_{1k} + E_{k+1}R_k + U_k \\
Z_{k+1} &= E_1\alpha''_{11} + \cdots + E_k\alpha''_{1k} + E_{k+1}R_{k+1} + U_{k+1}
\end{aligned}$$

Example 4

$\widetilde{K}\cdot\mathrm{SE}(g)\mathrm{PKC}$ over $F_{2^{31}}$:

$$L = 11$$

$$\#\{U_i^{(L)}\} = {}_L\mathrm{H}_2 + {}_L\mathrm{H}_1 = 77,$$

$$\#\{E_i, U_i\} = 200,$$

$$S_{\mathrm{PK}} = 200\cdot 3\cdot 31\cdot 11 = 204600\ (\mathrm{bits}),$$

$$\rho = \frac{|m|}{|c|} = \frac{9}{11} = 0.82.$$

Conclusion

- We have presented three new classes of SE(g)PKC.
- We have shown that K_{III}•SE(g)PKC can be secure against both GB attack and Patarin's attack.
- We have presented $\tilde{K} \cdot \mathrm{SE}(g)\mathrm{PKC}$.
- Various studies have been left on $\tilde{K} \cdot \mathrm{SE}(g)\mathrm{PKC}$.
- The present author would like to report on the studies in near future.

Appendix I

K-Matrix PKC in Section 5.2 of Ref. 1 is not secure.

In Ref. 1, letting S be $k \times k$ matrix $S\tilde{K} = M$ is publicized.

Letting k+1 symbols error vector of weight e and message vector, m cipher text C is given by

$$C = eM + m.$$

It is easy to see that we can obtain the following matrix $\tilde{M}$ of rank 1:

$$XMY = \tilde{M}$$

Consequently, we have

$$(eXM + m)Y = e\tilde{M} + mY,$$

yielding message m.

Ref. 1:M. Kasahara, IEICE Technical Report of IEICE, ISEC 2005-171, pp.113-118, (2006-03).