A note on the multivariate cryptosystem based on a linear code

Yasufumi Hashimoto [*]

Abstract

A new multivariate cryptosystem based on a linear code was proposed by Smith-Tone and Tone quite recently. This short note points out that it is a variant of UOV.

Keywords. multivariate public-key cryptosystems, linear code, UOV

Smith-Tone and Tone [2] proposed a new multivariate cryptosytem whose quadratic map is generated as follows. Let $n, k, p \geq 1$ be integers with $k < n$, q a power of prime and $\mathbf{F}_q$ a finite field of order q. For a rank k linear code C of length n over $\mathbf{F}_q$, denote by G the generator matrix in the standard form and H the corresponding parity check matrix, i.e. G, H are respectively $k \times n$ and $(n-k) \times n$ matrices with $G \cdot {}^tH = 0_{k,n-k}$. Choose $n \times (n-k)$ matrices $A_1, \dots, A_k$ over $\mathbf{F}_q$ and define $B_i := A_i H$, $F_i(\mathbf{x}) := {}^t\mathbf{x} B_i \mathbf{x}$ for $1 \leq i \leq k$, $\mathbf{x} = {}^t(x_1, \dots, x_n)$. Choose further p quadratic forms $Q_1(\mathbf{x}), \dots, Q_p(\mathbf{x})$ randomly and let T be an invertible $(k+p) \times (k+p)$ matrix over $\mathbf{F}_q$. The public key $P : \mathbf{F}_q^n \to \mathbf{F}_q^{k+p}$ of the proposed scheme is

$$P(\mathbf{x}) := T^t(F_1(\mathbf{x}), \dots, F_k(\mathbf{x}), Q_1(\mathbf{x}), \dots, Q_p(\mathbf{x})) .$$

See [2] for its decryption process in detail.

Let $\bar{G}$ be an $n \times n$ matrix with $\bar{G} := ({}^tG, *_{n,n-k})$. Since $H {}^tG = 0_{n-k,k}$, we see that

$$F_i(\bar{G}\mathbf{x}) = {}^t\mathbf{x} {}^t\bar{G} A_i H \bar{G} \mathbf{x} = {}^t\mathbf{x} \begin{pmatrix} 0_k & * \\ 0 & *_{n-k} \end{pmatrix} \mathbf{x} = {}^t\mathbf{x} \begin{pmatrix} 0_k & * \\ * & *_{n-k} \end{pmatrix} \mathbf{x}.$$

This means that $F_1(\mathbf{x}), \dots, F_k(\mathbf{x})$ are generated by $(k, n-k)$-type UOV polynomials [1], and then the proposed scheme is a plus of UOV.

Acknowledgment. The author was supported by JST Crest no.JPMJCR14D6 and JSPS Grant-in-Aid for Scientific Research (C) no.17K05181.

References

[1] A. Kipnis, J. Patarin, L. Goubin, Unbalanced oil and vinegar signature schemes, Eurocrypt'99, LNCS **1592** (1999), pp.206–222, extended in `http://www.goubin.fr/papers/OILLONG.PDF`, 2003.

[2] D. Smith-Tone, C. Tone, A. Petzoldt, J. Ding, L.C. Wang, A nonlinear multivariate cryptosystem based on a random linear code, `https://eprint.iacr.org/2019/1355`, 2019.

[*]Department of Mathematical Science, University of the Ryukyus, hashimoto@math.u-ryukyu.ac.jp