A note on Tensor Simple Matrix Encryption Scheme

Yasufumi Hashimoto *

Abstract

The simple matrix encryption scheme (Tao-Diene-Tang-Ding, PQCrypto 2013) has a problem of decryption failures. Quite recently, Petzoldt-Ding-Wang (http://eprint.iacr.org/2016/010) proposed a new version of this scheme called the tensor simple matrix encryption scheme to remove decryption failures by using a tensor product of two small matrices as its secret key. However, it is much weaker than the original scheme. In this note, we show that the tensor simple matrix encryption scheme is equivalent to a weak version of the original simple matrix encryption scheme.

Keywords. multivariate public-key cryptosystems, simple matrix encryption scheme (SMES), tensor simple matrix encryption scheme (TSMES), post-quantum cryptography

1 Introduction

The simple matrix encryption scheme (SMES, in short) proposed by Tao-Diene-Tang-Ding [3] is one of multivariate public key cryptosystems (MPKCs). While it is efficient and (presently) secure against known attacks, decryption failures occur with non-negligible probability [1, 4]. To remove decryption failures, Petzoldt-Ding-Wang [2] proposed a new version of this scheme called the tensor simple matrix encryption scheme (TSMES, in short). The idea is that one uses a tensor product of two small matrices as a secret key to enable the sender to check the decryptability of his/her plain-texts without knowing the secret key. However, it is a bad choice of the secret key. In this note, we show that TSMES is equivalent to a weak example of SMES.

2 Simple matrix encryption scheme

In this section, we introduce the simple matrix encryption scheme.

Let $\mathbb{F}$ be a finite field and q its order. For an integer $s \geq 1$, denote by $n := s^2$, $m := 2n$ and $\mathrm{M}_s(\mathbb{F})$ the set of $s \times s$ matrices of $\mathbb{F}$-entries. Now the one-to-one maps $\varphi : \mathbb{F}^n \to \mathrm{M}_s(\mathbb{F})$ and $\psi : \mathrm{M}_s(\mathbb{F}) \times \mathrm{M}_s(\mathbb{F}) \to \mathbb{F}^m$ are given as follows.

$$\varphi(x_1, \ldots, x_n) = \left(x_{i+(s-1)j}\right)_{1 \leq i,j \leq s},$$
$$\psi\left(\left(y_{i+(s-1)j}\right)_{1 \leq i,j \leq s}, \left(y_{n+i+(s-1)j}\right)_{1 \leq i,j \leq s}\right) = (y_1, \ldots, y_m)^t.$$

*Department of Mathematical Science, University of the Ryukyus/JST CREST, hashimoto@math.u-ryukyu.ac.jp

For two matrices $\mathcal{B}, \mathcal{C} \in \mathrm{M}_n(\mathbb{F})$ and a vector $x \in \mathbb{F}^n$, define the five matrices A, B, C, E_1, E_2 and the quadratic map $\mathcal{F} : \mathbb{F}^n \to \mathbb{F}^m$ by

$$A = A(x) := \varphi(x), \qquad B = B(x) := \varphi(\mathcal{B}x), \qquad C = C(x) := \varphi(\mathcal{C}x),$$
$$E_1 = E_1(x) := AB, \qquad E_2 = E_2(x) := AC, \qquad \mathcal{F}(x) := \psi(E_1, E_2).$$

Then the *original* simple matrix encryption scheme [3] is constructed as follows.

Simple Matrix Encryption Scheme.

Secret keys: Two matrices $\mathcal{B}, \mathcal{C} \in \mathrm{M}_n(\mathbb{F})$ and two invertible linear maps $\mathcal{S} : \mathbb{F}^m \to \mathbb{F}^m$, $\mathcal{T} : \mathbb{F}^n \to \mathbb{F}^n$.

Public key: The quadratic map $\mathcal{P} := \mathcal{S} \circ \mathcal{F} \circ \mathcal{T} : \mathbb{F}^n \to \mathbb{F}^m$.

Encryption. For a plain-text $\mathbf{d} \in \mathbb{F}^n$, the cipher-text is $\mathbf{c} := \mathcal{P}(\mathbf{d}) \in \mathbb{F}^m$.

Decryption. Let $\bar{E}_1, \bar{E}_2 \in \mathrm{M}_s(\mathbb{F})$ be matrices given by $\left(\bar{E}_1, \bar{E}_2\right) = \psi^{-1}\left(\mathcal{S}^{-1}(\mathbf{c})\right)$. If $\bar{E}_1$ is invertible, find $y \in \mathbb{F}^n$ such that $B(y)\bar{E}_1^{-1}\bar{E}_2 = C(y)$. If $\bar{E}_1$ is not invertible and $\bar{E}_2$ is invertible, find $y \in \mathbb{F}^n$ such that $C(y)\bar{E}_2^{-1}\bar{E}_1 = B(y)$. If $\bar{E}_1, \bar{E}_2$ are not invertible, find $y, z \in \mathbb{F}^n$ such that $\varphi(z)\bar{E}_1 - B(y) = \varphi(z)\bar{E}_2 - C(y) = 0$. Then the plain-text is $\mathbf{d} = \mathcal{T}^{-1}(y)$.

We call it the $(\mathcal{B}, \mathcal{C}, \mathcal{S}, \mathcal{T})$-SMES. Remark that y (and z) are found by linear operations. However, if $A(\mathcal{T}\mathbf{d})$ is not invertible, such (y, z) cannot be found since $\varphi(z)$ corresponds to the inversion of $A(\mathcal{T}\mathbf{d})$. To avoid the situation that $\det A(\mathcal{T}\mathbf{d}) = 0$, Petztoldt et al. [2] proposed the following new idea called the *tensor* simple matrix encryption scheme.

Tensor Simple Matrix Encryption Scheme.

Secret key: Two matrices $\mathcal{B}, \mathcal{C} \in \mathrm{M}_n(\mathbb{F})$, two invertible smaller matrices $T_1, T_2 \in \mathrm{M}_s(\mathbb{F})$ and an invertible linear map $\mathcal{S} : \mathbb{F}^m \to \mathbb{F}^m$. Put $\mathcal{T} := T_1 \otimes T_2$.

Public key: The quadratic map $\mathcal{P} := \mathcal{S} \circ \mathcal{F} \circ \mathcal{T} : \mathbb{F}^n \to \mathbb{F}^m$.

Encryption: For a plain-text $\mathbf{d} \in \mathbb{F}^n$, check whether $A(\mathbf{d})$ is invertible. If it is invertible, the cipher is $\mathbf{c} = \mathcal{P}(\mathbf{d})$. If not, the cipher is $\mathbf{c} = \mathcal{P}(\mathbf{d}')$ where $\mathbf{d} \in \mathbb{F}^n$ is a minor change of $\mathbf{d}$ such that $A(\mathbf{d}')$ is invertible.

Decryption: Decrypt the cipher $\mathbf{c}$ and get $\mathbf{d}'$ similarly. Note that decryption failures never occur since $A(\mathcal{T}\mathbf{d}') = T_1 A(\mathbf{d}') T_2^t$ is invertible. After that, correct $\mathbf{d}'$ to get the plain-text $\mathbf{d}$.

We call it the $(\mathcal{B}, \mathcal{C}, \mathcal{S}, T_1, T_2)$-TSMES. See §3 of [2] for the details of how to change $\mathbf{d}$ to $\mathbf{d}'$ in the encryption process and how to correct $\mathbf{d}'$ to $\mathbf{d}$ in the decryption process.

3 Weakness of Tensor Simple Matrix Encryption Scheme

In this section, we show the following theorem, which means that the TSMES is much weaker than the original SMES.

Theorem 3.1. *For matrices $\mathcal{B}, \mathcal{C} \in \mathrm{M}_n(\mathbb{F})$ and invertible matrices $\mathcal{S} \in \mathrm{M}_m(\mathbb{F})$, $T_1, T_2 \in \mathrm{M}_s(\mathbb{F})$, there exist matrices $\mathcal{B}', \mathcal{C}' \in \mathrm{M}_n(\mathbb{F})$ and an invertible matrix $\mathcal{S}' \in \mathrm{M}_m(\mathbb{F})$ such that the $(\mathcal{B}, \mathcal{C}, \mathcal{S}, T_1, T_2)$-TSMES is equivalent to the $(\mathcal{B}', \mathcal{C}', \mathcal{S}', I_n)$-SMES, where $I_n \in \mathrm{M}_n(\mathbb{F})$ is the identity matrix.*

Proof. By the construction of the public key, we see that the public key $\mathcal{P}$ of the $(\mathcal{B}, \mathcal{C}, \mathcal{S}, \mathcal{T})$-SMES is described as follows.

$$\mathcal{P}(x) = \mathcal{S}\psi\left(\varphi(\mathcal{T}x)\varphi(\mathcal{B}\mathcal{T}x), \varphi(\mathcal{T}x)\varphi(\mathcal{C}\mathcal{T}x)\right).$$

When $\mathcal{T} = T_1 \otimes T_2$, the map $\mathcal{P}$ is given by

$$\mathcal{P}(x) = \mathcal{S}\psi\left(T_1\varphi(x)T_2^t\varphi(\mathcal{B}\mathcal{T}x), T_1\varphi(x)T_2^t\varphi(\mathcal{C}\mathcal{T}x)\right),$$

since $\varphi\left((T_1 \otimes T_2)x\right) = T_1\varphi(x)T_2^t$. It is easy to see that

$$\begin{aligned} T_2^t\varphi(y) =& \varphi\left((T_2^t \otimes I_s)y\right), \\ \psi\left(T_1L_1, T_1L_2\right) =& (T_1 \otimes I_{2s})\psi(L_1, L_2) \end{aligned}$$

for $y \in \mathbb{F}^n$ and $L_1, L_2 \in \mathrm{M}_s(\mathbb{F})$. Then we have

$$\mathcal{P}(x) = \mathcal{S}'\psi\left(\varphi(x)\varphi\left(\mathcal{B}'x\right), \varphi(x)\varphi\left(\mathcal{C}'x\right)\right)$$

with $\mathcal{B}' := (T_2^t \otimes I_s)\mathcal{B}\mathcal{T}$, $\mathcal{C}' := (T_2^t \otimes I_s)\mathcal{C}\mathcal{T}$ and $\mathcal{S}' := \mathcal{S}(T_1 \otimes I_{2s})$. We thus conclude that the $(\mathcal{B}, \mathcal{C}, \mathcal{S}, T_1, T_2)$-TSMES is equivalent to the $(\mathcal{B}', \mathcal{C}', \mathcal{S}', I_n)$-SMES. □

4 Conclusion

We show in this note that the TSMES is much weaker than the original SMES. The problem of decryption failures still remains on SMES.

Acknowledgment. The author is partially supported by JSPS Grant-in-Aid for Young Scientists (B) no. 26800020.

References

[1] J. Ding, A. Petzoldt, L.C. Wang, The cubic simple matrix encryption scheme, PQCrypto 2014, LNCS **8772** (2014), pp. 76–87.

[2] A. Petzoldt, J. Ding, L.C. Wang, Eliminating decryption failures from the simple matrix encryption scheme, http://eprint.iacr.org/2016/010, 2016.

[3] C. Tao, A. Diene, S. Tang, J. Ding, Simple matrix scheme for encryption, PQCrypto 2013, LNCS **7932** (2013), pp. 231–242.

[4] C. Tao, H. Xiang, A. Petzoldt, J. Ding, Simple Matrix - a multivariate public key cryptosystem (MPKC) for encryption, Finite Fields and Their Applications **35** (2015), pp. 352–368.