Analysis of TPL Signature Scheme

Terry Shue Chien Lau, Chik How Tan, and Theo Fanuela Prabowo

Temasek Laboratories,
National University of Singapore,
5A Engineering Drive 1, #09-02,
Singapore 117411
{tsltlsc,tsltch,tsltfp}@nus.edu.sg

Abstract. Tan et al. proposed a rank metric code-based signature (TPL) in the 2018 International Symposium on Information Theory and Its Application [3]. Their proposal has compact key size (8.29KB, 1.97KB and 2.90KB for public key, private key and signature respectively) compared to other code-based signature submitted to the NIST call for Post-Quantum Cryptography Standardization at 128-bit post-quantum security level. This short paper aims to discuss the practical security of the TPL signature. In particular, we describes how to recover the private key in TPL with practical simulations. Our experimental results show that we are able to recover the private key of TPL in less than 23 milliseconds for all the proposed schemes at 82-bit, 98-bit and 129-bit post-quantum security level.

Keywords: Post-quantum Signatures · Cryptanalysis · Key Recovery Attack · Public-key Encryption

1 Introduction

Tan et al. proposed a rank metric code-based signature, namely the TPL signature scheme in the 2018 International Symposium on Information Theory and Its Application [3]. Their proposal has compact key size (8.29KB, 1.97KB and 2.90KB for public key, private key and signature respectively) compared to other code-based signature submitted to the NIST call for Post-Quantum Cryptography Standardization at 128-bit post-quantum security level.

This short paper aims to discuss the security of the TPL signature. By extending the idea of our previous work in [2], we recover the private key $(\boldsymbol{e_1}, \ldots, \boldsymbol{e_l})$ in TPL. Using multiple signature $\sigma_j = (\boldsymbol{c}_j, \boldsymbol{t}_{j,1}, \ldots, \boldsymbol{t}_{j,l})$ collected for $1 \leq j \leq w$, we first recover a support basis for $\boldsymbol{e_i}$ from $\boldsymbol{t}_{1,i}, \ldots, \boldsymbol{t}_{w,i}$. Then, we recover a support matrix for $\boldsymbol{e_i}$ from the public key H and $\boldsymbol{s_i}$. We show the result of the simulations of our attack at the end of paper. The full version of our paper will be made available later.

Notation. The following are some notations in this paper:

- Denote the rank weight of a vector $\boldsymbol{x} \in \mathbb{F}_{q^m}^n$ as $\mathrm{rk}(\boldsymbol{x})$.

– Denote $\mathcal{H}_{\mathsf{A},\mathsf{B}} : \mathsf{A} \to \mathsf{B}$ as a collision-resistant hash function.
– Denote $\mathcal{E}_{n,r} = \{\boldsymbol{g} \in \mathbb{F}_{q^m}^n \mid \mathrm{rk}(\boldsymbol{g}) = r\}$.
– Let X be a finite set, we write $\boldsymbol{x} \xleftarrow{\$} X$ to denote assignment to $\boldsymbol{x}$ of an element randomly sampled from the uniform distribution on X.

2 TPL Signature Scheme

The TPL signature scheme is described as follows:

TPL.Setup: Let $m, n, k, d, r_1, r_2, l, l_{\mathcal{H}}$ be positive integers such that $m > n > k$, $l_{\mathcal{H}} \geq m \geq \lceil \frac{l_{\mathcal{H}}}{l} \rceil$ and $r_2 \leq r_1 \leq \lfloor \frac{d-1}{4} \rfloor$. Let $q = 2$.

TPL.Gen: Let $\mathcal{H}_{\mathsf{A},\mathsf{B}}$ be a collision-resistant hash function where $\mathsf{A} = \left(\mathbb{F}_{q^m}^{n-k}\right)^l \times \{0,1\}^* \times \mathbb{F}_{q^m}^{(n-k)\times n} \times \left(\mathbb{F}_{q^m}^{n-k}\right)^l$ and $\mathsf{B} = \{0,1\}^{l_H}$. Let $H \in \mathbb{F}_{q^m}^{(n-k)\times n}$ be a parity check matrix of a random linear code $\mathcal{C}$ with minimum distance at least d. For $1 \leq i \leq l$, choose random $\boldsymbol{e_i} \xleftarrow{\$} \mathcal{E}_{n,r_1}$ where $r_1 \leq \lfloor \frac{d-1}{4} \rfloor$. Compute $\boldsymbol{s_i} = \boldsymbol{e_i} H^T$. Output public key, $\mathsf{pk} = (H, \boldsymbol{s_1}, \ldots, \boldsymbol{s_l})$ and the private key, $\mathsf{sk} = (\boldsymbol{e_1}, \ldots, \boldsymbol{e_l})$.

TPL.Sign: To sign a message $\boldsymbol{m}$, choose random $\boldsymbol{u_i} \xleftarrow{\$} \mathcal{E}_{n,r_2}$ for $1 \leq i \leq l$. Compute $\boldsymbol{c} = (c_0, c_1, \ldots, c_{l_{\mathcal{H}}-1}) = \mathcal{H}(\boldsymbol{u_1} H^T, \ldots, \boldsymbol{u_l} H^T, \boldsymbol{m}, H, \boldsymbol{s_1}, \ldots, \boldsymbol{s_l})$ where $c_j \in \mathbb{F}_q$ for $0 \leq j \leq l_{\mathcal{H}} - 1$. For $1 \leq i \leq l$, define

$$\hat{c}_i := \left(c_{(i-1)m \bmod l_{\mathcal{H}}}, c_{(i-1)m+1 \bmod l_{\mathcal{H}}}, \ldots, c_{(i-1)m+m-1 \bmod l_{\mathcal{H}}}\right)$$

and consider $\hat{c}_i$ as an element in $\mathbb{F}_{q^m}$. Then compute $\boldsymbol{t_i} := \boldsymbol{u_i} + \hat{c}_i \boldsymbol{e_i}$. If the last k coordinates of $\boldsymbol{t_i}$ are all zero for all $1 \leq i \leq l$, then repeat the whole signature generation above. Otherwise output the signature as $(\boldsymbol{c}, \boldsymbol{t_1}, \ldots, \boldsymbol{t_l})$.

TPL.Vrfy: To verify a signature $(\boldsymbol{c}, \boldsymbol{t_1}, \ldots, \boldsymbol{t_l})$ with $\mathsf{pk} = (H, \boldsymbol{s_1}, \ldots, \boldsymbol{s_l})$, the verifier first checks whether the last k coordinates of $\boldsymbol{t_i}$ are all zero for $1 \leq i \leq l$. If it is true, then reject the signature. Otherwise, check whether $\mathrm{rk}(\boldsymbol{t_i}) \overset{?}{\leq} r_1 + r_2$ for $1 \leq i \leq l$. If one of them is false, then reject the signature. Otherwise, proceed to compute $\hat{c}_i \in \mathbb{F}_{q^m}$ from $\boldsymbol{c} = (c_0, \ldots, c_{l_{\mathcal{H}}-1})$ for $1 \leq i \leq l$, and compute $\boldsymbol{v_i} = \boldsymbol{t_i} H^T - \hat{c}_i \boldsymbol{s_i}$. Check whether $\boldsymbol{c} \overset{?}{=} \mathcal{H}(\boldsymbol{v_1}, \ldots, \boldsymbol{v_l}, \boldsymbol{m}, H, \boldsymbol{s_1}, \ldots, \boldsymbol{s_l})$. If it is true, then accept the signature, otherwise, reject the signature.

In Tan et al.'s proposal, they consider $H = [I_{n-k} \mid X] \in \mathbb{F}_{q^m}^{n-k}$ where $X^T \in \mathbb{F}_{q^m}^{k\times(n-k)}$ is a Cauchy matrix satisfying [3, Theorem 3(b) & (d)]. The following table is the parameters proposed in [3]:

Instance	m	n	k	r_1	r_2	l	pks	sks	ss	PQSec
TPL-I	570	50	10	10	6	1	3.56K	0.78K	1.02K	82
TPL-II	650	58	10	12	6	1	4.71K	1.06K	1.59K	98
TPL-III	850	78	10	17	8	1	8.29K	1.97K	2.90K	129

Table 1. Parameters of TPL. The public key size, private key size and signature size (in bytes) is denoted by pks, sks and ss respectively.

3 Key Recovery Attack on TPL

Recall that for a vector $\boldsymbol{e} = (e_1, \ldots, e_n) \in \mathbb{F}_{q^m}^n$ with $\mathrm{rk}(\boldsymbol{e}) = r_1$, there exists a vector $\hat{\boldsymbol{e}} = (e_1, \ldots, e_{r_1}) \in \mathbb{F}_{q^m}^{r_1}$ with $\mathrm{rk}(\hat{\boldsymbol{e}}) = r_1$ and a $r_1 \times n$ matrix E over $\mathbb{F}_q$ with $\mathrm{rk}(E) = r_1$ such that $\boldsymbol{e} = \hat{\boldsymbol{e}}E$. Note that $\hat{\boldsymbol{e}}$ and E are non unique. We call $\hat{\boldsymbol{e}}$ and E satisfying $\boldsymbol{e} = \hat{\boldsymbol{e}}E$ as a support basis and a support matrix for $\boldsymbol{e}$ respectively. We denote the support space of $\boldsymbol{e}$, $\mathsf{Supp}(\boldsymbol{e}) = \langle e_1, \ldots, e_n \rangle$ as the subspace of $\mathbb{F}_{q^m}$ generated by the coordinates of $\boldsymbol{e}$.

We extend the idea of [1, Algorithm 1] and the attack method in [2] to solve for a support basis of $\boldsymbol{e_i}$ for $1 \leq i \leq l$. Given $\boldsymbol{a} = \boldsymbol{b}C \in \mathbb{F}_{q^m}^{n-k}$ with $\langle c_{ij} \rangle_{1 \leq i \leq n, 1 \leq j \leq n-k}$ (of dimension d) known, the [1, Algorithm 1] is to solve for $\boldsymbol{b} \in \mathbb{F}_{q^m}^n$ with $\mathrm{rk}(\boldsymbol{b}) \leq r$. In our case, we are given a vector $\boldsymbol{t_i} = \boldsymbol{u_i} + \hat{c}_i \boldsymbol{e_i}$ and an element $\hat{c}_i \in \mathbb{F}_{q^m}$, we are supposed to solve for $\boldsymbol{e_i}$.

There are two parts in our attack on TPL. In the first part of attack in [2], only one signature is needed to recover a support basis for the secret key. Here, we require multiple signature $\sigma_j = (\boldsymbol{c}_j, \boldsymbol{t}_{j,1}, \ldots, \boldsymbol{t}_{j,l})$ to recover a support basis for the vector $\boldsymbol{e_i}$ from $\boldsymbol{t}_{j,i}$ for $1 \leq j \leq w$ in the first part. The second part is to recover a support matrix for $\boldsymbol{e}_i$ from the public key component H and $\boldsymbol{s_i}$. Once we have recovered a support basis and a support matrix for $\boldsymbol{e_i}$, we can then recover the private key component $\boldsymbol{e_i}$.

Step 1: Recover a Support Basis for $\boldsymbol{e_i}$.

Let $\boldsymbol{\sigma_1} = (\boldsymbol{c_1}, \boldsymbol{t_{1,1}}, \ldots, \boldsymbol{t_{1,l}})$ be a signature generated in TPL.Sign. Let $\boldsymbol{e_i} = (e_{i,1}, \ldots, e_{i,n})$. Notice that

$$\begin{aligned} & \boldsymbol{t_{1,i}} = \boldsymbol{u_{1,i}} + \hat{c}_{1,i} \boldsymbol{e_i} \\ \Rightarrow \quad & \hat{\boldsymbol{t}}_{\boldsymbol{1,i}} = (\hat{t}_{1,i,1}, \ldots, \hat{t}_{1,i,n}) := (\hat{c}_{1,i})^{-1} \boldsymbol{t_{1,i}} = (\hat{c}_{1,i})^{-1} \boldsymbol{u_{1,i}} + \boldsymbol{e_i} \\ \Rightarrow \quad & \langle e_{i,1}, \ldots, e_{i,n} \rangle \subset \langle \hat{t}_{1,i,1}, \ldots, \hat{t}_{1,i,n} \rangle. \end{aligned}$$

Similarly, for another signature $\boldsymbol{\sigma_2} = (\boldsymbol{c_2}, \boldsymbol{t_{2,1}}, \ldots, \boldsymbol{t_{2,l}})$, we have $\langle e_{i,1}, \ldots, e_{i,n} \rangle \subset \langle \hat{t}_{2,i,1}, \ldots, \hat{t}_{2,i,n} \rangle$. By collecting w signatures $\sigma_1, \ldots, \sigma_w$, we have

$$\langle e_{i,1}, \ldots, e_{i,n} \rangle = \bigcap_{j=1}^{w} \langle \hat{t}_{j,i,1}, \ldots, \hat{t}_{j,i,n} \rangle.$$

Since $\mathrm{rk}(\boldsymbol{e_i}) = r_1$, we can deduce a support basis $\{\hat{e}_1, \ldots, \hat{e}_{r_1}\}$ for the vector space $\langle e_{i,1}, \ldots, e_{i,n} \rangle$.

Step 2: Recover a Support Matrix for $\boldsymbol{e_i}$.

With a support basis computed, we consider the $\boldsymbol{s_i}$ from the public key and form the linear system $\boldsymbol{s_i} = (\hat{e}_1, \ldots, \hat{e}_{r_1}) E_i H^T$. This linear system has $n-k$ equations over $\mathbb{F}_{q^m}$, with $r_1 \times n$ unknown variables over $\mathbb{F}_q$. Now consider the linear system under $\mathbb{F}_q$, we have the number of equations is $m(n-k)$ and number of unknown variables is $r_1 n$. Since $m(n-k) > r_1 n$, we can solve for a support matrix E_i, thus giving us $\boldsymbol{e_i} = (\hat{e}_1, \ldots, \hat{e}_{r_1}) E_i$ in polynomial time.

Simulations of Our Attack on TPL. We consider all the parameters of TPL given in [3] and perform simulations of our key recovery attack. The experimental results of our key recovery attack are presented in Table 2. The experiments were performed using Magma V2.20-5 running on a 3.4 GHz Intel(R) Core$^{\text{TM}}$ i7 processor with 16GB of memory.

We experimented with all the three sets of proposed parameters: TPL-I, TPL-II and TPL-III. For each parameter, we measured the time taken (denoted as "KRA Time") and the number of signatures collected to recover the private key with our algorithm. Table 2 presents the average timing of 100 experiments for each parameter.

Instances	Signatures Collected, w	Claimed Security	KRA Time
TPL-I	2	82	8 milliseconds
TPL-II	2	98	15 milliseconds
TPL-III	2	129	23 milliseconds

Table 2. Simulations results of our key recovery attack on TPL

Our key recovery attack is able to recover the private key of all the TPL schemes on an average time of less than 23 milliseconds.

4 Concluding Remark

We have discuss the practical security of the TPL signature scheme. In particular, we have proposed a key recovery attack to recover the private key $\mathsf{sk} = (\boldsymbol{e_1}, \ldots, \boldsymbol{e_l})$ for the TPL signature scheme. Our attack is efficient in a way that it does not only attack the parameters, but also attack the structure of the system. More specifically, we can always determine a support basis for the private key $\boldsymbol{e_i}$, due to the properties that $r_1 \leq \left\lfloor \frac{d-1}{4} \right\rfloor$ and $r_1 n < m(n-k)$. In conclusion, TPL is an insecure signature scheme.

References

1. P. Gaborit, O. Ruatta, J. Schrek, G. Zémor, "New results for rank-based cryptography," in *Progress in Cryptology* (AFRICACRYPT 2014), pp. 1-12.
2. T. S. C. Lau, and C. H. Tan. Key Recovery Attack on Rank Quasi-Cyclic Code-based Signature Scheme. arXiv preprint:1902.00241. Available at `https://arxiv.org/abs/1902.00241`
3. C. H. Tan, T. F. Prabowo, and T. S. C. Lau, "Rank Metric Code-based Signature," in *International Symposium on Information Theory and Its Application* (ISITA 2018), pp. 70-74.