

---

**From:** Laura Maddison <ismaddison@gmail.com>  
**Sent:** Friday, February 9, 2024 9:58 AM  
**To:** pqc-comments  
**Cc:** pqc-forum  
**Subject:** Round 1 (Additional Signatures) OFFICIAL COMMENT: TUOV

Hello,

The submission of the Triangular Unbalanced Oil and Vinegar (TUOV) digital signature scheme to the NIST competition in 2023 claims that if the Multivariate Quadratic (MQ) problem (with suitable parameters) is hard, then the TUOV problem must also be hard. We show in our new pre-print why the proof fails and why the claimed theorem cannot be true in general.

The pre-print can be found here: <https://eprint.iacr.org/2024/193>

The invalidity of the security reduction does not however jeopardize the security of TUOV against known attacks, for which the author's provide a robust security analysis. These observations merely suggest that we cannot claim that TUOV is *more* secure than standard UOV.

Best regards,  
Laura Maddison

---

**From:** Boru Gong <gongboru@gmail.com>  
**Sent:** Tuesday, February 13, 2024 9:16 PM  
**To:** pqc-forum  
**Cc:** Laura Maddison; pqc-forum; pqc-comments; tuovsig@gmail.com  
**Subject:** Re: Round 1 (Additional Signatures) OFFICIAL COMMENT: TUOV

Dear Laura Maddison:

Thanks for your interest on TUOV. Unfortunately, there are **two fundamental mistakes** in your analysis, and hence your conclusion does not hold, as the following analysis shows.

**First**, Lemma 4.1 of [2024-193] is essential to reach your conclusion. In the proof of Lemma 4.1, you try to deduce the contradiction by analyzing the equality  $A_k = Q^T M_k Q$ .

Unfortunately, this equality is incorrect in general, and the correct one is  $A_k = \text{UT}(Q^T M_k Q)$  (cf. Eq. 3, page 12, TUOV specs v1.0). In fact,  $A_k$  is required to be upper-triangular, but the matrix product  $Q^T M_k Q$  may not be upper-triangular, and hence the UT operation comes into play.

Here is a simple **example**. Let  $(q,n,m) = (2,3,1)$ , and  $M_1 = [1 \ 1 \ 1; 0 \ 1 \ 1; 0 \ 0 \ 1]$ ,  $Q = [1 \ 0 \ 1; 0 \ 1 \ 1; 0 \ 0 \ 1]$ . Then it is routine to verify that  $Q^T M_1 Q = [1 \ 1 \ 1; 0 \ 1 \ 0; 1 \ 0 \ 0]$  is not upper-triangular, which implies the necessity of the UT operation.

**Second**, you disapprove Assertion 3.1 (i.e., Theorem 1 in TUOV specs v1.0) by arguing that it is necessary to show in the proof of Theorem 1 how an arbitrary  $(m^2/2, m, q)$ -MQ map  $M$  can be efficiently transformed into an  $(m^2/2, m, m/2, 3m/4, q)$ -TUOV central map; or more precisely, it is necessary to show how to find an affine invertible transformation  $\mathcal{Q}$  efficiently.

In fact, it suffices for us to prove the **mere existence** of such a desired  $\mathcal{Q}$ , as you read through the proof.

Boru Gong,

on behalf of the TUOV team

On Friday, February 9, 2024 at 10:58:41 PM UTC+8 Laura Maddison wrote:

Hello,

The submission of the Triangular Unbalanced Oil and Vinegar (TUOV) digital signature scheme to the NIST competition in 2023 claims that if the Multivariate Quadratic (MQ) problem (with suitable parameters) is hard, then the TUOV problem must also be hard. We show in our new pre-print why the proof fails and why the claimed theorem cannot be true in general.

The pre-print can be found here: <https://eprint.iacr.org/2024/193>

The invalidity of the security reduction does not however jeopardize the security of TUOV against known attacks, for which the author's provide a robust security analysis. These observations merely suggest that we cannot claim that TUOV is *more* secure than standard UOV.

---

**From:** pqc-forum@list.nist.gov on behalf of Laura Maddison <lmaddison@gmail.com>  
**Sent:** Friday, February 16, 2024 3:20 PM  
**To:** pqc-forum  
**Cc:** Boru Gong; Laura Maddison; pqc-forum; pqc-comments; tuo...@gmail.com  
**Subject:** [pqc-forum] Re: Round 1 (Additional Signatures) OFFICIAL COMMENT: TUOV

Dear Boru Gong,

Thank you for your response to my comment, and I do agree that I should have perhaps been clearer about the distinction between  $Q^T M_k Q$  before and after applying the UT operation. However, Theorem 1 of the TUOV specification can still be disproven by showing that the desired affine transformation  $\mathcal{Q}$  does not always exist.

In this example, we demonstrate an (8,4,2)-MQ map that cannot be transformed into an (8,4,2,3,2)-TUOV map. Note that these parameters satisfy the constraints given in the statement of Theorem 1.

Consider the following first two polynomials in the MQ map:

$f_1(\mathbf{x})$

$$= x_1^2 + x_1 x_2 + x_1 x_4 + x_1 x_5 + x_1 x_6 + x_1 x_7 + x_2^2 + x_2 x_6 + x_2 x_7 + x_2 x_8 + x_3^2 + x_3 x_7 + x_3 x_8 + x_4 x_5 + x_4 x_8 + x_5 x_7 + x_6 x_7 + x_7^2 + x_7 x_8$$

$f_2(\mathbf{x})$

$$= x_1^2 + x_1 x_2 + x_1 x_4 + x_1 x_5 + x_1 x_6 + x_1 x_7 + x_2^2 + x_2 x_6 + x_2 x_7 + x_2 x_8 + x_3^2 + x_3 x_7 + x_3 x_8 + x_4 x_5 + x_4 x_8 + x_5 x_7 + x_6 x_7 + x_7^2 + x_7 x_8 + x_8^2 + 1$$

$$= f_1(\mathbf{x}) + x_8^2 + 1$$

Then the matrices representing their quadratic parts are, respectively:

$$M_1 = [1\ 1\ 0\ 1\ 1\ 1\ 1\ 0; 0\ 1\ 0\ 0\ 0\ 1\ 1\ 1; 0\ 0\ 1\ 0\ 0\ 0\ 1\ 1; 0\ 0\ 0\ 0\ 1\ 0\ 0\ 1; 0\ 0\ 0\ 0\ 0\ 0\ 1\ 0; 0\ 0\ 0\ 0\ 0\ 0\ 1\ 0; 0\ 0\ 0\ 0\ 0\ 0\ 1\ 1; 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0]$$

$M_2 = [1\ 1\ 0\ 1\ 1\ 1\ 1\ 0; 0\ 1\ 0\ 0\ 0\ 1\ 1\ 1; 0\ 0\ 1\ 0\ 0\ 0\ 1\ 1; 0\ 0\ 0\ 0\ 1\ 0\ 0\ 1; 0\ 0\ 0\ 0\ 0\ 0\ 1\ 0; 0\ 0\ 0\ 0\ 0\ 0\ 1\ 0; 0\ 0\ 0\ 0\ 0\ 0\ 1\ 1; 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1]$

Consider an arbitrary affine transformation  $\mathcal{Q}$  as in the proof of Theorem 1 with top right 4x4 submatrix:

$$Q^{(2)} = [q_1\ q_2\ q_3\ q_4; q_5\ q_6\ q_7\ q_8; q_9\ q_{10}\ q_{11}\ q_{12}; q_{13}\ q_{14}\ q_{15}\ q_{16}]$$

Now, it is essential to note that the UT operation leaves the diagonal of a matrix unchanged, so the bottom right entry of  $Q^{(2)T}M_kQ^{(2)}$  (which is the bottom right entry of  $Q^{(2)T}M_kQ^{(2)}$ ) for  $k=1,2$  is also the bottom right entry of  $UT(Q^{(2)T}M_kQ^{(2)})$  (which is the bottom right entry of  $UT(Q^{(2)T}M_kQ^{(2)})$ ).

If we let  $a$  be the bottom right entry of  $Q^{(2)T}M_1Q^{(2)}$ , then

$$a = q_4^2 + q_4q_8 + q_4q_{16} + q_8^2 + q_{12}^2 + q_8 + q_{12} + q_{16}.$$

And if we let  $b$  be the bottom right entry of  $Q^{(2)T}M_2Q^{(2)}$ , then

$$\begin{aligned} b &= q_4^2 + q_4q_8 + q_4q_{16} + q_8^2 + q_{12}^2 + q_8 + q_{12} + q_{16} + 1 \\ &= a + 1 \end{aligned}$$

Since these entries are unchanged under the UT operation, and we require the two matrices  $UT(Q^{(2)T}M_kQ^{(2)})$  for  $k=1,2$  to have a row of zeroes at the bottom, we need both  $a$  and  $a+1$  to be equal to 0, which is a contradiction.

Therefore, there is no affine transformation  $\mathcal{Q}$  that transforms the given MQ map into a TUOV map, thus disproving Theorem 1 of the TUOV specifications.

Thank you,

Laura Maddison

On Tuesday, February 13, 2024 at 9:16:10 PM UTC-5 Boru Gong wrote:

---

**From:** Boru Gong <gongboru@gmail.com>  
**Sent:** Sunday, February 18, 2024 10:35 PM  
**To:** pqc-forum  
**Cc:** Laura Maddison; Boru Gong; pqc-forum; pqc-comments; tuo...@gmail.com  
**Subject:** Re: Round 1 (Additional Signatures) OFFICIAL COMMENT: TUOV

Dear Laura Maddison:

Thanks again for your interest on TUOV. Unfortunately, there is **a fundamental mistake** in your new analysis.

In fact, it is unreasonable to refute Theorem 1 by proposing a concrete counterexample solely, because the reduction in Theorem 1 is **probabilistic**.

Best regards,  
Boru Gong,  
on behalf of the TUOV team.

On Saturday, February 17, 2024 at 4:20:17 AM UTC+8 Laura Maddison wrote:

Dear Boru Gong,

Thank you for your response to my comment, and I do agree that I should have perhaps been clearer about the distinction between  $Q^T M_k Q$  before and after applying the UT operation. However, Theorem 1 of the TUOV specification can still be disproven by showing that the desired affine transformation  $\mathcal{Q}$  does not always exist.

In this example, we demonstrate an (8,4,2)-MQ map that cannot be transformed into an (8,4,2,3,2)-TUOV map. Note that these parameters satisfy the constraints given in the statement of Theorem 1.

Consider the following first two polynomials in the MQ map:

$f_1(\mathbf{x})$

$$= x_1^2 + x_1 x_2 + x_1 x_4 + x_1 x_5 + x_1 x_6 + x_1 x_7 + x_2^2 + x_2 x_6 + x_2 x_7 + x_2 x_8 + x_3^2 + x_3 x_7 + x_3 x_8 + x_4 x_5 + x_4 x_8 + x_5 x_7 + x_6 x_7 + x_7^2 + x_7 x_8$$

$f_2(\mathbf{x})$

---

**From:** Laura Maddison <ismaddison@gmail.com>  
**Sent:** Tuesday, March 5, 2024 12:32 PM  
**To:** pqc-forum  
**Cc:** Boru Gong; Laura Maddison; pqc-forum; pqc-comments; tuo...@gmail.com  
**Subject:** Re: Round 1 (Additional Signatures) OFFICIAL COMMENT: TUOV

Dear Boru Gong,

I would like to re-iterate that the removal of this reduction statement from the security analysis of TUOV does not suggest a security weakness.

For the reduction presented in Theorem 1 to be cryptographically relevant to the PQC standardization process, however I would argue that it should indeed be efficient. Indeed, because of the inefficiency of the transformation, the discovery of an efficient attack for the TUOV problem would not imply an efficient attack on the MQ problem.

What I show in the pre-print is that to execute the desired transformation and map a solution to TUOV to a solution to MQ, we must be able to solve a different, and indeed larger, instance of the MQ problem. So, in essence, Theorem 1 shows that:

TUOV not hard + MQ not hard  $\Rightarrow$  MQ not hard.

Best regards,

Laura Maddison

On Sunday, February 18, 2024 at 10:34:30 PM UTC-5 Boru Gong wrote:

Dear Laura Maddison:

Thanks again for your interest on TUOV. Unfortunately, there is a **fundamental mistake** in your new analysis.

In fact, it is unreasonable to refute Theorem 1 by proposing a concrete counterexample solely, because the reduction in Theorem 1 is **probabilistic**.

Best regards,  
Boru Gong,  
on behalf of the TUOV team.

On Saturday, February 17, 2024 at 4:20:17 AM UTC+8 Laura Maddison wrote:

Dear Boru Gong,

Thank you for your response to my comment, and I do agree that I should have perhaps been clearer about the distinction between  $Q^T M_k Q$  before and after applying the UT operation. However, Theorem 1 of the TUOV

---

**From:** Boru Gong <gongboru@gmail.com>  
**Sent:** Monday, April 8, 2024 2:03 PM  
**To:** pqc-forum  
**Cc:** Laura Maddison; Boru Gong; pqc-forum; pqc-comments; tuo...@gmail.com  
**Subject:** Re: Round 1 (Additional Signatures) OFFICIAL COMMENT: TUOV

Dear Laura Maddison:

Thanks for your interest in TUOV.

Unfortunately, your argument is still incorrect, and the transformation in our Theorem 1 works **efficiently**. To be more precise, this transformation is the **identity map**: when parameters are appropriately chosen, the probability that a random MQ map is a TUOV map is not negligible.

It is not surprising that this trivial transformation works in TUOV, and please refer to the security proofs of some classic public-key cryptographic schemes first and foremost.

Best regards,  
Boru Gong

On Wednesday, March 6, 2024 at 1:31:46 AM UTC+8 Laura Maddison wrote:

Dear Boru Gong,

I would like to re-iterate that the removal of this reduction statement from the security analysis of TUOV does not suggest a security weakness.

For the reduction presented in Theorem 1 to be cryptographically relevant to the PQC standardization process, however I would argue that it should indeed be efficient. Indeed, because of the inefficiency of the transformation, the discovery of an efficient attack for the TUOV problem would not imply an efficient attack on the MQ problem.

What I show in the pre-print is that to execute the desired transformation and map a solution to TUOV to a solution to MQ, we must be able to solve a different, and indeed larger, instance of the MQ problem. So, in essence, Theorem 1 shows that:

TUOV not hard + MQ not hard  $\Rightarrow$  MQ not hard.

Best regards,

Laura Maddison

On Sunday, February 18, 2024 at 10:34:30 PM UTC-5 Boru Gong wrote:

Dear Laura Maddison:

Thanks again for your interest on TUOV. Unfortunately, there is a **fundamental mistake** in your new analysis.