Dear Designers and all,

We group found that the following statement claimed by the designers is not true.

"even if the hard problems in lattice, such as CVP and SIS, can be efficiently solved, the secret values or private key in Compact-LWE still cannot be efficiently recovered. This allows Compact-LWE to choose very small dimension parameters, such as n = 8 in our experiment"

We group find a ciphertext-only attack against CompactLWE. More precisely, given a ciphertext, we can recover the corresponding message, without knowing the private key, by solving some (approximation-)CVP instance. Since the parameters recommended by the authors are small, we just need to solve (approximation-)CVP with a 128-dimensional lattice, which can be done efficiently with the lattice basis reduction algorithm. In our experiments, we can decrypt all the ciphertexts. So we make sure that CompactLWE with the small parameters recommended in the paper is NOT secure. The designers should enlarge the parameters to ensure the security.

The main steps of our attack is as following:

Step 1: Given a Compact-LWE ciphertext \( c=(l, d, lpk, lpk') \), find a short enough vector \( l = (l_1', l_2', \hat{\ldots}, l_m') \) by lattice basis reduction algorithm, such that

\[
\sum_{i=0}^m l_i' a_i = l_a;
\sum_{i=0}^m l_i' pk_i = lpk \mod q;
\sum_{i=0}^m l_i' pk_i' = lpk' \mod q.
\]

Step 2: Compute \( \sum_{i=0}^m l_i' u_i \), if \( l \) is short enough, then we can show that \( \sum_{i=0}^m l_i' u_i = \sum_{i=0}^m l_i u_i \), where \( \sum_{i=0}^m l_i u_i \) is the correct value that can be used to decrypt the ciphertext. So we can use \( \sum_{i=0}^m l_i' u_i \) to recover the message.

The designers also considered the attack to ciphertexts in their paper. However, they thought that one need to guess the exact \( l \) to recover the message. Due to our attack, we find that we do not need to guess the exact \( l \), a short \( l' \) can also help recover the message very well.
If there is something we miss, please tell us, thank you!

Best regards,

Haoyu Li, Renzhang Liu, Yanbin Pan, Tianyuan Xie
Dear designers, dear all,

The following sage script decrypts ciphertexts without the secret key.

https://gist.github.com/xagawa/ee91d51a56bda5292235e52640f57707

This attack is an extension of the plaintext-recovery attack in
https://ia.cr/2017/742
and the same as the Li-Liu-Pan-Xi attack.

Regards,
Jonathan, Mehdi, and Keita

-------
Jonathan Bootle, Mehdi Tibouchi, and Keita Xagawa
Hi Haoyu Li, Renzhang Liu, Yanbin Pan, Tianyuan Xie,

Would like to share you code? So your attack can be confirmed more conveniently. If this attack can be confirmed, we will change our scheme slightly by avoiding the use of u_{i} in the calculation of pk_{i} and pk_{i}' and will try your attack again.

Thanks.

Regards,
Dongxi Liu

---

Dear Designers and all,

We group found that the following statement claimed by the designers is not true.
"even if the hard problems in lattice, such as CVP and SIS, can be efficiently solved, the secret values or private key in Compact-LWE still cannot be efficiently recovered. This allows Compact-LWE to choose very small dimension parameters, such as n =8 in our experiment"

We group find a ciphertext-only attack against CompactLWE. More precisely, given a ciphertext, we can recover the corresponding message, without knowing the private key, by solving some (approximation-)CVP instance. Since the parameters recommended by the authors are small, we just need to solve (approximation-)CVP with a 128-dimensional lattice, which can be done efficiently with the lattice basis reduction algorithm. In our experiments, we can decrypt all the ciphertexts. So we make sure that CompactLWE with the small parameters recommended in the paper is NOT secure. The designers should enlarge the parameters to ensure the security.

The main steps of our attack is as following:

**Step 1:** Given a Compact-LWE ciphertext c=(la, d, lpk,lpk'), find a short enough vector l= (l'_1,l'_2,\ldots,l'_m) by lattice basis reduction algorithm, such that \sum_{i=0}^{m} l'_i*a_i = la ;
I already sent a mail but let me send it again.

Dear designers and all,

The following sage script decrpts ciphertexts without the secret key.
https://gist.github.com/xagawa/ee91d51a56bda5292235e52640f57707

This attack is an extension of the plaintext-recovery attack in https://ia.cr/2017/742
and the same as the Li-Liu-Pan-Xi attack.

Regards,
Jonathan, Mehdi, and Keita

--------------------
Jonathan Bootle, Mehdi Tibouchi, and Keita Xagawa

--
You received this message because you are subscribed to the Google Groups "pqc-forum" group.
To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+unsubscribe@list.nist.gov.
Visit this group at https://groups.google.com/a/list.nist.gov/group/pqc-forum/.
Dear Jonathan, Mehdi, and Keita,

Thanks. Your script will be very helpful. We will have a look.

Regards,
Dongxi
Dear all,

For the sake of completeness, let me add to Keita's comment that the attack below (together with a full key recovery attack on the parameters of ia.cr/2017/685) is accepted for publication at CT-RSA 2018. We will update our eprint paper shortly to provide timings, etc., for the parameters in the NIST submission.

Based on our analysis, it seems very unlikely that the ways in which Compact-LWE departs from standard LWE-based schemes can improve security, and in particular that a reasonable level of security is somehow achievable in the very low dimensions proposed so far, even with further tweaks to the construction.

Best regards,

--

Jonathan, Mehdi and Keita.
Dear all,

Thank Keita very much for sharing his code!

Our paper about the attack against NIST Compact-LWE has been posted by Cryptology ePrint Archive as [https://eprint.iacr.org/2018/020](https://eprint.iacr.org/2018/020).

Thank Prof. Lepoint very much for telling us Bootle and Tibouchi's work ([https://eprint.iacr.org/2017/742](https://eprint.iacr.org/2017/742)) against the former version of Compact-LWE (ia.cr/2017/685) when we submitted our paper to ePrint with exactly the same title with their paper. Prof. Lepoint asked us to change the title, cite their paper and make some comparison, and we did so. We found that the there are many differences between the former version and the current version submitted to NIST, and we guess that some changes are due to Bootle and Tibouchi's former attack.

If we understand Mehdi correctly, we think their work accepted by CT-RSA2018 is the attack above against the former version of Compact-LWE, but NOT the NIST version, since by the paper submission deadline (Oct 1st (12.00 GMT) 2017) of CT-RSA2018, the NIST version had not appeared anywhere to our best knowledge, and they did not propose any comments to NIST or the designers before ours. We think we should make this point clear so that our attack indeed makes sense.

If we miss something, please tell us, thank you very much!

Best regards,
Haoyu, Renzhang, Yanbin, Tianyuan

---

From: Mehdi Tibouchi
Date: 2018-01-06 13:49
To: Xagawa Keita
CC: pqc-comments; pqc-forum
Subject: Re: [pqc-forum] OFFICIAL COMMENT: Compact LWE

Dear all,

For the sake of completeness, let me add to Keita's comment that the attack below (together with a full key recovery attack on the parameters of ia.cr/2017/685) is accepted for publication at CT-RSA 2018. We will update our eprint paper shortly to provide timings, etc., for the parameters in the NIST submission.

Based on our analysis, it seems very unlikely that the ways in which Compact-LWE departs from standard LWE-based schemes can improve security, and in particular that a reasonable level of security is somehow achievable in the very low dimensions proposed so far, even with further tweaks to the construction.