1 Basic Thoughts

Let $1 < k \in \mathbb{Z}$. Let R be the ring of integers of some cyclotomic field (say 512 for Kyber compatibility).

In this security game, we receive from $\mathcal{A}$ some $\mathbf{A} \in R_q^{k \times k}, \mathbf{b} \in R_q^k$, both of which can potentially be any value.

We sample uniformly random $\mathbf{A}_0, \mathbf{A}_1 \in R_q k \times k$, gaussians $\mathbf{r} \leftarrow \chi^k$, $\mathbf{e} \leftarrow \chi^k$, $\hat{e} \leftarrow \chi$, $\beta \leftarrow \{0, 1\}$

and send back

$$\mathbf{A}_0, \mathbf{A}_1, \mathbf{u} := \mathbf{A}_\beta \mathbf{r} + \mathbf{e}, \mathbf{v} := \mathbf{b}^t \mathbf{r} + \hat{e}.$$

It is necessary for security that a malicious adversary will have negligible advantage in distinguishing $\beta = 0$ from $\beta = 1$.

I *believe* that requiring $\mathbf{A}$ to be invertible won't kill the protocol?

We should be able to do a straightforward if not too efficient porting of the extended-LWE internals found in Brakerski et al's "Classical Hardness of Learning with Errors" paper [BLP$^+$13].

2 Extended LWE

Recall from the formulation of the problem as in Brakerski et al's paper [BLP$^+$13] that the extended-LWE assumption (reformulated for arbitrary dimension module lattices over arbitrary base rings) is as follows.

Definition 2.1. *Let $\mathcal{Z} \subseteq R^k$. The adversary $\mathcal{A}$ can choose an arbitrary $\mathbf{z} \in \mathcal{Z}$, and sends it to the challenger.*

The challenger returns

$$(\mathbf{A}, \mathbf{b}, \langle \mathbf{e}, \mathbf{z} \rangle + \hat{e})$$

and the adversary must distinguish between two cases. In the first case $\mathbf{A}$ is chosen uniformly at random, $\mathbf{s}, \mathbf{e} \leftarrow \chi^k$, $\hat{e} \leftarrow \zeta$ (which may be the same as χ or may be uniquely 0) and $\mathbf{b} := \mathbf{A}^t \mathbf{s} + \mathbf{e}$.

In the second case, everything besides $\mathbf{b}$ is chosen in the same way, but $\mathbf{b}$ is chosen uniformly at random and independently of everything else.

3 Reducing Security of Protocol to Hardness of Extended LWE

We can use an $\mathcal{A}$ breaking the PQ-PAKE described above to attack extended LWE as follows.

Proof. We receive from the PQ-PAKE adversary $(\tilde{\mathbf{A}} \in R_q^{k \times k}, \tilde{\mathbf{b}} \in R_q^k)$.

Let $\mathbf{z} = \tilde{\mathbf{b}}$, and send $\mathbf{z}$ to the extended-LWE challenger, receiving back $\mathbf{A} \in R_q^{k \times k}, \mathbf{b}, y := \langle \mathbf{e}, \mathbf{z} \rangle + \hat{e}$.

Abort if $\mathbf{A}$ is not invertible (with non-negligible probability it should be invertible).

Otherwise, test the adversaries behavior for both $\beta = 0$ and $\beta = 1$ upon setting $\mathbf{A}_\beta = \mathbf{A}^{-1}$, $\mathbf{u} := \mathbf{A}^{-t}\mathbf{b}$, $v := y$, $\mathbf{A}_{1-\beta} \leftarrow R_q^{k\times k}$ uniformly at random.

If the extended-LWE instance was the first case above, then we have that

$\mathbf{u} := \mathbf{A}^{-t}\mathbf{e} + \mathbf{s} = \mathbf{A}_\beta^t\mathbf{e} + \mathbf{s}$ and $v := \tilde{\mathbf{b}}^t\mathbf{e} + \hat{e}$, so we have perfectly simulated the PQ-PAKE security game, and $\mathcal{A}$ will have a non-negligible advantage in distinguishing $\beta = 0$ from $\beta = 1$.

However, if the extended-LWE instance was the uniform case above (where the returned $\mathbf{b}$ is chosen uniformly and independently), then, since $\mathbf{A}$ is invertible and $\mathbf{b}$ is chosen uniformly at random and independently, $\mathbf{u}$ will be statistically indistinguishable from uniform over the view of $\mathcal{A}$, meaning that nothing whatsoever about β is leaked to the adversary and so the adversary will have 0 advantage in distinguishing $\beta = 0$ from $\beta = 1$.

It remains to show that this formulation of extended-LWE can be reasonably seen as hard.

4 Reducing Extended-(M)-LWE to (Lower Dimension) (M)-LWE

Using similar arguments as in the Classical Hardness of Learning with Errors Paper, we should be able to show that breaking $\mathsf{Ext\text{-}LWE}_{R,k,q}$ is no easier than breaking $\mathsf{LWE}_{R,k-1,q}$ (with slightly less noise).

4.1 First Is Errorless (M)-LWE

We refer to the paper above for the definition of this problem, namely the first ring element of $\mathbf{b}$ is errorless, and we show that $\mathsf{1st\ Errorless\ LWE}_{R,k,q,\alpha}$ is no easier than breaking $\mathsf{LWE}_{R,k-1,q,\alpha}$.

Lemma 4.1. *There is an efficient transformation/reduction from* $\mathsf{M\text{–}LWE}_{R,k-1,q,\alpha}$ *with uniform secrets to* $\mathit{1st\ Errorless\ MLWE}_{R,k-1,q,\alpha}$ *with uniform secrets.*

Proof. We begin with access to an $\mathsf{LWE}_{R,k-1,q,\alpha}$ oracle. For simplicity, we assume $q \in \mathbb{Z}$ is prime, the proof can be adapted if necessary.

First, we sample $\mathbf{a}' \leftarrow R_q^k$ uniformly at random. We then find an $\hat{\mathbf{a}} \in R_q^k$ such that

1. The coordinates of $\hat{\mathbf{a}}$ generate all of R, namely that $\sum_{i\in[k]}^{\langle \hat{a}_i\rangle} = R$ where $\langle hata_i \rangle$ is the principal ideal generated by a_i.
2. There exists $\kappa \in R_q$ such that $\mathbf{a}' = \kappa\hat{\mathbf{a}}$.

We can efficiently find such a $\hat{\mathbf{a}}$ and κ by using the CRT (Chinese Remainder Theorem) decomposition (see, e.g. [SV11] for the necessary lattice cryptography-oriented background).

Since the number theoretic transform to switch from coefficient representation to CRT representation can be computed extremely efficiently [LN16], we may assume that each element of $\mathbf{a}'$ is already in CRT representation.

Concretely (assuming we have sampled), we compute the number theoretic transform of every element

Let S be the set of coefficient positions (in the CRT representation) j such $a'_{ij} = 0$ for all $i \in [k]$.

Then we may set (note that $\hat{a}_{ij}$ means the jth coefficient in the CRT representation of the ith element of $\hat{\mathbf{a}}$)

$$\hat{a}_{ij} = \begin{cases} a'_{ij} & \text{if } j \notin s \\ 1 & \text{if} j \in S \end{cases}$$

and

$$\kappa_j = \begin{cases} 1 & \text{if } j \notin S \\ 0 & \text{otherwise} \end{cases}$$

The remainder of the proof mostly follows [BLP+13]. We create a matrix $U \in R_q^{k \times k}$ (invertible over R_q) such that its leftmost column is $\hat{\mathbf{a}}$. Such as matrix exists, and can be found efficiently. TO-DO: If there's no obvious faster way, we can choose the rest of the columns at random and show it has a non-negligible chance of being invertible

[ACPS09] The rest of the proof for first-is-errorless LWE should be a straightforward mapping of the Classical Hardness paper.

4.2 Extended-LWE

I don't really feel like writing this last step out in module form before we've had a chance to discuss but it seems like it should work as well.

References

[ACPS09] Benny Applebaum, David Cash, Chris Peikert, and Amit Sahai. Fast cryptographic primitives and circular-secure encryption based on hard learning problems. In *CRYPTO*, pages 595–618, 2009.

[BLP+13] Zvika Brakerski, Adeline Langlois, Chris Peikert, Oded Regev, and Damien Stehlé. Classical hardness of learning with errors. In *STOC*, pages 575–584, 2013.

[LN16] Patrick Longa and Michael Naehrig. Speeding up the number theoretic transform for faster ideal lattice-based cryptography. In *Cryptology and Network Security: 15th International Conference, CANS 2016, Milan, Italy, November 14-16, 2016, Proceedings 15*, pages 124–139. Springer, 2016.

[SV11] N.P. Smart and F. Vercauteren. Fully homomorphic SIMD operations. Cryptology ePrint Archive, Report 2011/133, 2011. `http://eprint.iacr.org/`.