1. OKCN-KEX (IND-CPA) 算法的推荐参数为 $m = 2, q = 7681, g = 4$. 这样根据 KC 参数要求的关系 $(2d+1)m < q(1-\frac{1}{g})$，可以计算得 $d < 1440$ 即可保证 KC 算法的正确性. 说明文档中给出的 OKCN-KEX 协议如下（其中 Algorithm 3 中应为 $E_\sigma \leftarrow S_\eta$.）:

Algorithm 1 $(\mathsf{pk}_1, \mathsf{sk}_1) \leftarrow \mathsf{KeyGen\text{-}Alice}(\mathsf{seed})$

$\mathbf{A} := \mathsf{Gen}(\mathsf{seed})$

$\mathbf{X}_1, \mathbf{E}_1 \leftarrow S_\eta^{l\times 1}$

$\mathbf{Y}_1 := \lfloor(\mathbf{A}\mathbf{X}_1 + \mathbf{E}_1)/2^{t_1}\rceil$

return $(\mathsf{pk}_1 := \mathbf{Y}_1, \mathsf{sk}_1 := \mathbf{X}_1)$

Algorithm 2 $(\mathsf{pk}_2, \mathsf{sk}_2) \leftarrow \mathsf{KeyGen\text{-}Bob}(\mathsf{seed})$

$\mathbf{A} := \mathsf{Gen}(\mathsf{seed})$

$\mathbf{X}_2, \mathbf{E}_2 \leftarrow S_\eta^{l\times 1}$

$\mathbf{Y}_2 := \lfloor(\mathbf{A}^T\mathbf{X}_2 + \mathbf{E}_2)/2^{t_1}\rceil$

return $(\mathsf{pk}_2 := \mathbf{Y}_2, \mathsf{sk}_2 := \mathbf{X}_2)$

Algorithm 3 $(\mathsf{ss}_2, \mathsf{signal}) \leftarrow \mathsf{KDF\text{-}Bob}(\mathsf{pk}_1, \mathsf{sk}_2)$

$\mathbf{E}_\sigma \leftarrow S_\eta^{l\times 1}$

$\boldsymbol{\Sigma}_2 := 2^{t_1}\mathbf{Y}_1^T\mathbf{X}_2 + \mathbf{E}_\sigma$

$(\mathbf{K}_2, \mathbf{V}) \leftarrow \mathsf{Con}(\boldsymbol{\Sigma}_2, \mathsf{params})$

return $(\mathsf{ss}_2 := \mathbf{K}_2, \mathsf{signal} := \mathbf{V})$

Algorithm 4 $\mathsf{ss}_1 \leftarrow \mathsf{KDF\text{-}Alice}(\mathsf{pk}_2, \mathsf{sk}_1, \mathsf{signal})$

$\boldsymbol{\Sigma}_1 := \mathbf{X}_1^T(2^{t_2}\mathbf{Y}_2)$

$\mathbf{K}_1 := \mathsf{Rec}(\boldsymbol{\Sigma}_1, \mathbf{V}, \mathsf{params})$

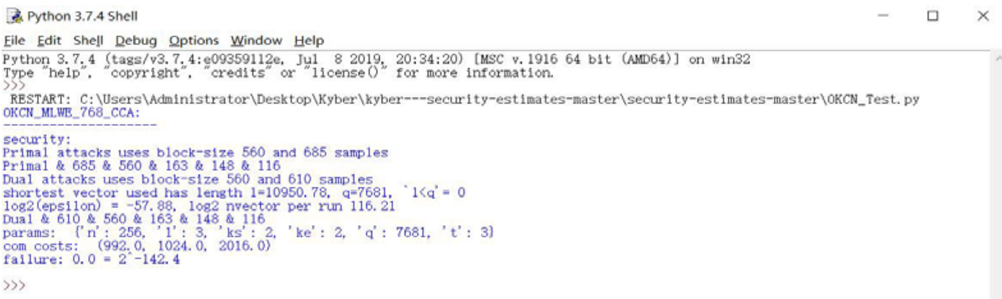
return $\mathsf{ss}_1 := \mathbf{K}_1$

算法使用的是分圆环 ${Z[x]}/{x^{256}+1}$，模的秩为 $l = 3$，MLWE 对应的误差分布为中心二项分布 S_2. 选取的参数 $t = t_1 = t_2 = 3$. 注意到 OKCN-KEX 输入 KC 的 Σ_1 和 Σ_2 之间的误差可以用说明文档中的方法作如下分析：记 $\varepsilon_1 = AX_1 + E_1 - 2^t\lfloor{(AX_1+E_1)}/{2^t}\rceil$，$\varepsilon_1 = A^TX_2 + E_2 - 2^t\lfloor{(A^TX_2+E_2)}/{2^t}\rceil$，则有

$$\begin{aligned}\boldsymbol{\Sigma}_1 - \boldsymbol{\Sigma}_2 &= \mathbf{X}_1^T(2^t\mathbf{Y}_2) - (2^t\mathbf{Y}_1^T\mathbf{X}_2 + \mathbf{E}_\sigma)\\ &= 2^t\mathbf{X}_1^T\lfloor(\mathbf{A}^T\mathbf{X}_2 + \mathbf{E}_2)/2^t\rceil - ((2^t\lfloor(\mathbf{A}\mathbf{X}_1 + \mathbf{E}_1)/2^t\rceil)^T\mathbf{X}_2 + \mathbf{E}_\sigma)\\ &= \mathbf{X}_1^T(\mathbf{A}^T\mathbf{X}_2 + \mathbf{E}_2 - \varepsilon_2) - ((\mathbf{A}\mathbf{X}_1 + \mathbf{E}_1 - \varepsilon_1)^T\mathbf{X}_2 + \boldsymbol{E}_\sigma)\\ &= \mathbf{X}_1^T(\mathbf{E}_2 - \varepsilon_2) - (\mathbf{E}_1 - \varepsilon_1)^T\mathbf{X}_2 - \mathbf{E}_\sigma\end{aligned}$$

注意到 $X_1, X_2, E_1, E_2 \leftarrow S_2^3$，$E_\sigma \leftarrow S_2$，且 $\varepsilon_1, \varepsilon_2$ 的无穷范数不超过 4. 所以，我们可以计算 $\Sigma_1 - \Sigma_2$ 的无穷范数的绝对上界，即 $||\Sigma_1 - \Sigma_2||_\infty \le \left||X_1^T \cdot E_2|\right|_\infty + \left||X_1^T \cdot \varepsilon_2|\right|_\infty + \left||E_1^T \cdot X_2|\right|_\infty + \left||\varepsilon_1^T \cdot X_2|\right|_\infty + \left||E_\sigma|\right|_\infty < 18436$. 注意到这是一个平凡的理论上界. 本竞选算法所选取的参数并不满足这个绝对上界，因而 OKCN-KEX 会有一定的概率出错（竞选算法的错误率分析一节，采用的是理想情况下的分析，即在 Nor-primal-D-MLWE(S_η) 假设情况下，我们可以近似地将 $\varepsilon_1, \varepsilon_2$ 的系数分布看成为区间 $[-2^{t-1}, 2^{t-1}]$ 上的均匀分布（更确切的说应为 $[-2^{t-1}, 2^{t-1})$ 上的均匀分布），此时，$\Sigma_1 - \Sigma_2$ 的系数服从的分布的期望为 0，

方差为 $2\cdot\mathrm{n}\cdot\mathrm{l}\cdot\left(\frac{\eta}{2}\right)^2+2\cdot\mathrm{n}\cdot\mathrm{l}\cdot\frac{\eta}{2}\cdot\frac{1}{3}\cdot2^{t-1}\cdot(2^{t-1}+1)+\frac{\eta}{2}=11777$). 这里, 我们可以使用类似于 Kyber 的方法, 使用脚本程序计算错误率的界 [BDK+17], 即计算 $\Pr[||\Sigma_1-\Sigma_2||_\infty>1440]$ 的上界. 我们采用 Kyber 开源的 python 脚本, 略作修改测试 OKCN-KEX, 得到的错误率结果约为 $2^{-142.4}$, 与文档声称的 $2^{-166.4}$ 的错误率大小不符, 但是仍比要求的 2^{-128} 要小得多. 我们的具体测试结果如下图:



.

2. 在认证密钥交换 (AKE) 的量子 random oracle (QROM) 方面，算法说明文档没有给出详细的安全性证明, 目前现有的基于 QROM 模型下的安全性证明归约损失较大, 对参数要求较高. 但这也是目前大多数 AKE 算法均面临的问题. 为了解决此类问题,[BDK+17]提出了一种新的归约思路, 给出了一种基于非标准假设的紧的归约, 然而假设的合理性仍需继续讨论. ([BDK+17] J.W. Bos et al.: CRYSTALS-Kyber: a CCA-secure module-lattice-based KEM. ePrint 2017/634.)