**OKCN-KEX：基于格的通用和模块化的密钥协商**

**程序问题说明**

我们在检视OKCN-KEX的程序实现时，发现了一个小的疏漏。具体来说，程序中出现的问题出现在 kex.c 文件迪138行

memcpy(skb, pb, AKCN\_SECRETKEYBYTES);

语句中，我们将 pb 错误的写成了 mb， 正确的应该是 pb， 下图 红框部分已经改成正确的形式。由于我们在进行程序自测试的时候， 自测试程序也写错了，所以在内部测试的时候通过了。现在 程序和自测试程序都已经改正。



**OKCN-KEX团队**

**2019年11月13日**