1.FatSeal算法基于NTRU格上的SIS问题，即求解的一个非零向量解，且。然而，容易发现即为满足条件的解，其中的各项系数均为0或1。因此在上述限制条件下，该问题并非困难问题。可通过进一步修改限制条件，如改为，以确保该问题困难。(实际上，安全性证明中两种情形下给出的解均满足)

2.FatSeal算法可能会遭受以下侧信道攻击：

在签名算法中，需要检验和是否超过范围，因此首先需要计算*af*和*ag*，找出其系数最大项，进行检验。

一般而言，找出系数最大项的过程如下所示：

for(int i = 0, max = 0; i < x.length(); i++) {

if(max < x[i]) {

max = x[i];

}

}

当max已经为最大值后，后续不会再进行赋值运算，只需进行比较运算，而理论上赋值运算需要的时间比比较运算多，因此敌手可以通过对该操作的运行时间分析，得到*af*和*ag*系数最大项的位置。

以*af*为例，该最大项可以表示为，由于a的系数均为0或1，因此该最大项为*f*的若干系数之和，且由于*f*的系数取自{-1,0,1}，因此可以认为这些系数中1（或-1）的数量较多，0的数量较少。通过对同一私钥产生多个签名的过程进行分析，统计*f*的各项系数出现的频率，敌手猜测出现频率较高的系数为1或-1，出现频率较低的系数为0。

然而该攻击的可行性需要对敌手猜测的系数正确的概率进行分析，以及讨论敌手能够得到最大项位置的假设是否成立，因此仅供参考。