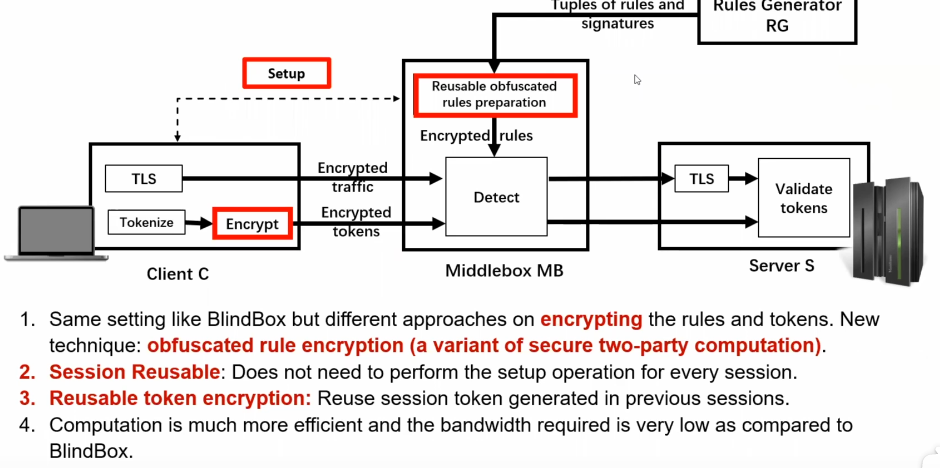
Privdpi

相对于blindbox，提出了可重复使用的方案

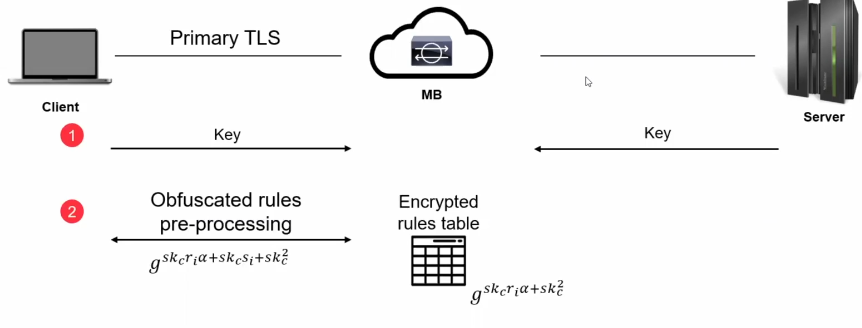
Blindbox的每次会话都需要进行setup步骤和加密规则，这些花费是巨大的需要大概97s的时间和50GB的空间



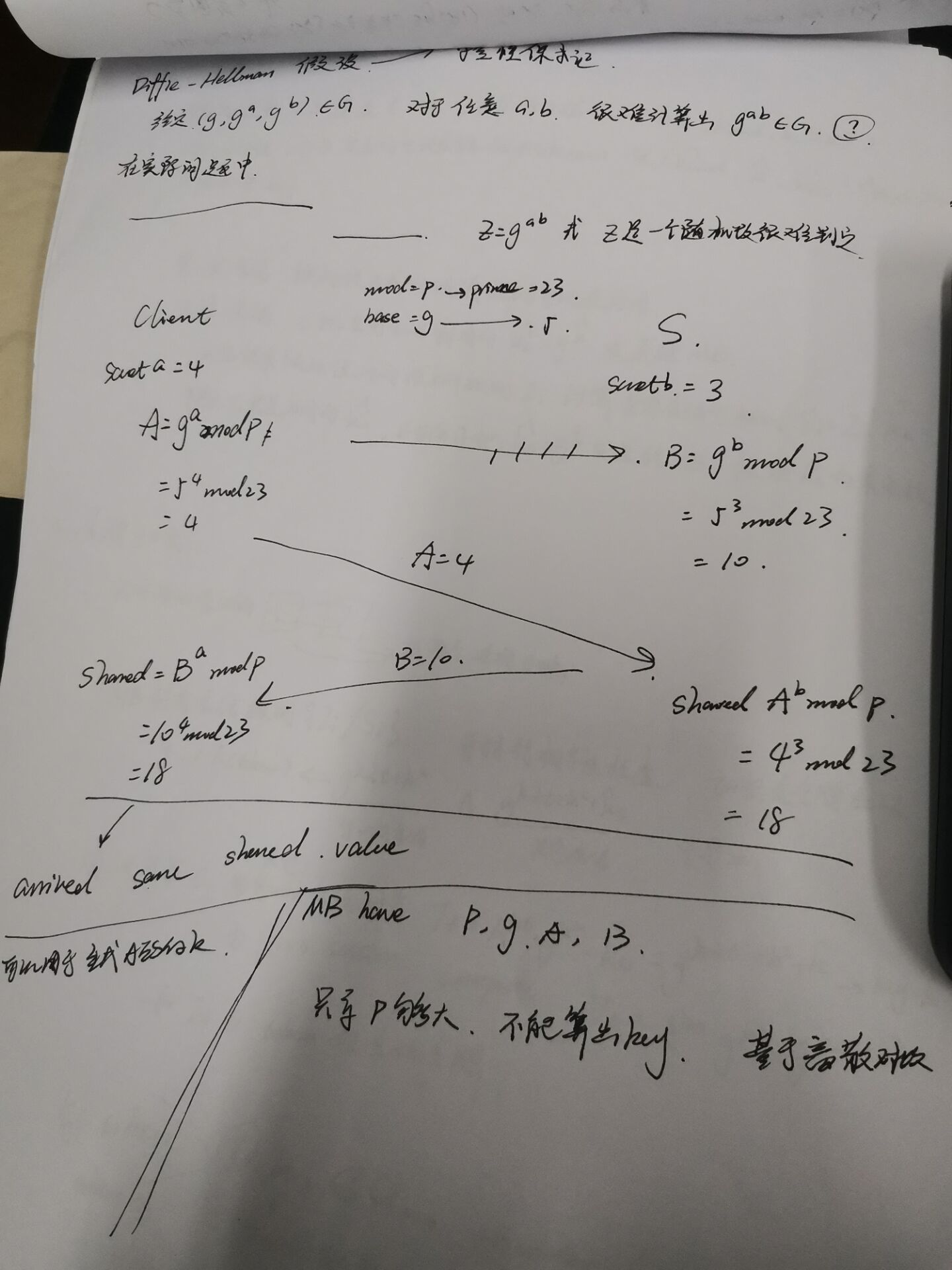
1. 设置和blindbox很像，新的区别是使用了模糊规则
2. 并不是每个规则都需要进行setup，只有新连接到MB的需要进行setup
3. Token也不需要每个都重新计算，token也是可以重用的
4. 相比blindbox来说需要的带宽更小，也更有效率

CS使用sk生成三个key：Krand：用于生成随机性种子，之后CS生成的随机数相同，K用于生成可重用的模糊规则，Ktls，常规的tls会话密钥

Setup

  
setup步骤的安全保证：是CDH假设。MB无法根据自己定义的ri计算新对可重用规则

CDH假设的



Privdpi关于token加密的改变，滑动窗口只对一个单词的首位两个token截取，减少了生成无用token的数量。