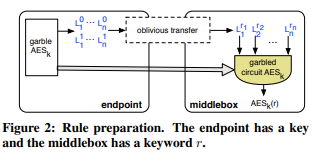
Blindbox

通信中希望做到的是：privacy+functionality，即希望隐私得到保护的同时，同时允许第三方机构检测通信中流量中的行为。

步骤：

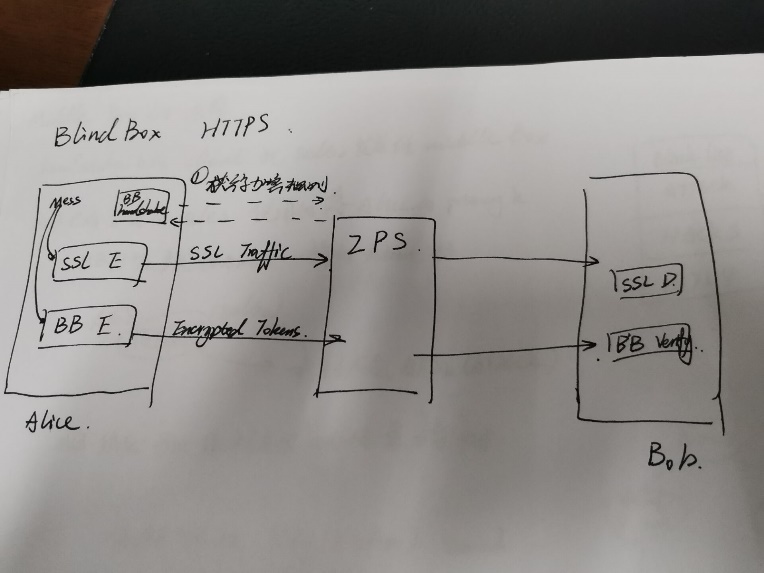
1. Setup

Client提供key，MB提供rule，共同计算出一个使用key作为AES密钥的规则r的加密使用OT+GC）



Token的匹配和处理

1. 发送方把msg使用滑动窗口划分为token
2. 把这些token加密后发送给MB，MB将得到的token与自己的保存的加密规则匹配
3. 通过前面提到的加salt方式，避免词频被泄露



信任模型

