

bds管理方案

在联盟网络中，超级管理员拥有bds的所属权和使用权。该文档给出了超级管理员对bds管理的技术方案，主要思路是利用秘密共享(secret sharing)对bds进行分片管理，考虑参诚实模型和恶意模型两种情况。这里假设有N个参与方，阈值为T。

一、诚实模型

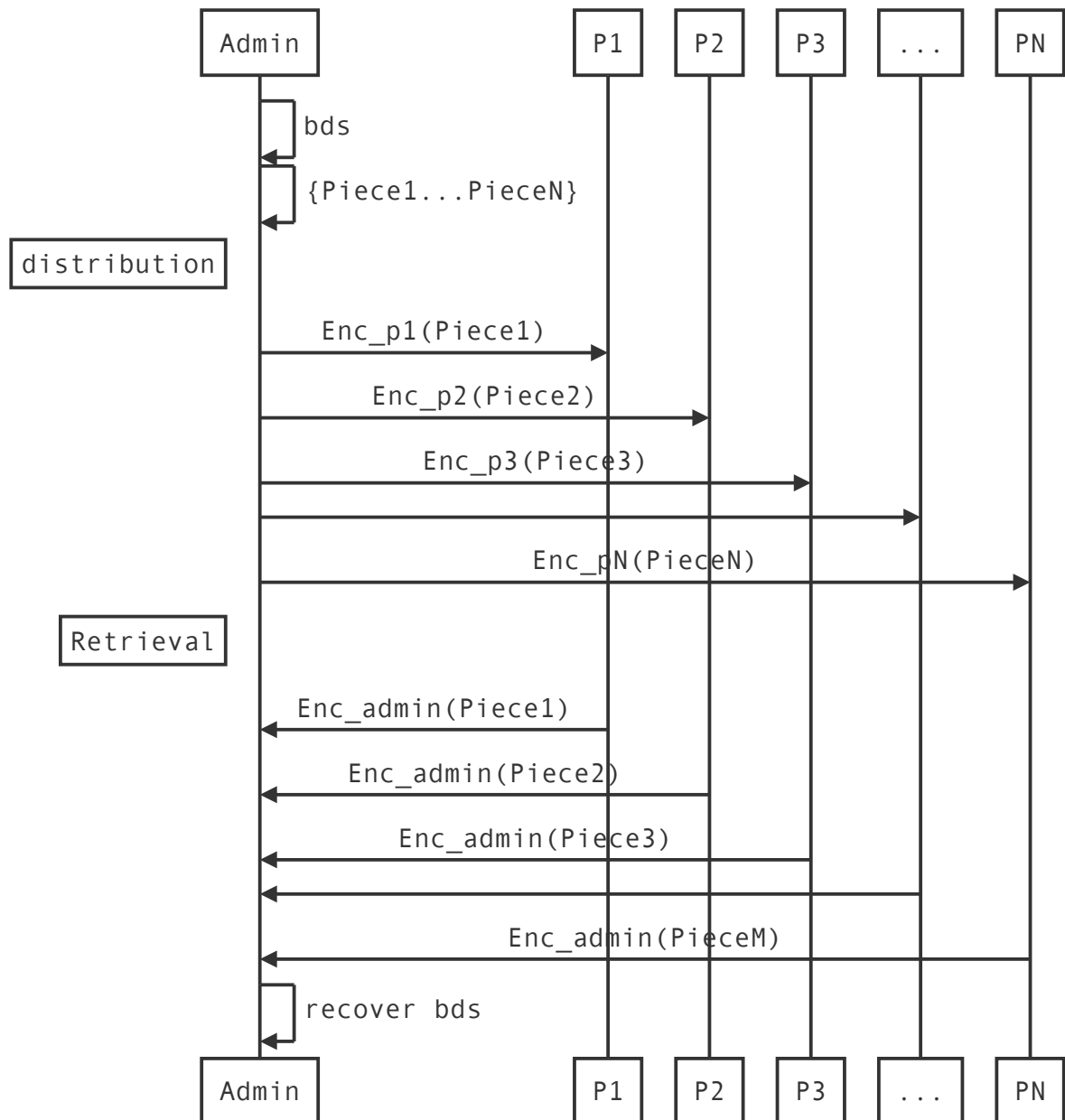
在这种情况下，参与方不会作恶。

bds分发过程如下：

- 1、超级管理员随机生成bds
- 2、管理员将bds拆分为N个分片
- 3、利用N个参与方的公钥分别对N个分片进行加密
- 4、将分片分别下发给N个参与方

bds恢复过程如下：

- 1、超级管理员发起bds恢复请求
- 2、各参与方将分片用超级管理员公钥加密并发送给超级管理员
- 3、超级管理员解密出分片明文并恢复出原始bds



二、恶意模型

在这种情况下，参与方可能作恶，篡改分片内容并返回给超级管理员。这里假设超级管理员不存储任何 bds 相关信息，只掌握自身公私钥(Prvkey, Pubkey)，即，管理员只能通过分片内容恢复 bds。同时，恶意参与者的数目小于 $\min(T, N - T)$ ，即：作恶者不可能联合起来恢复出 bds，且管理员可以得到足够多正确的分片恢复出 bds。

该 bds 管理方案比诚实模式多了分片的完整性验证过程。这里用管理员的私钥和分片内容计算 HMAC，保证任何参与方无法伪造分片并通过完整性验证。

bds 分发过程如下：

- 1、超级管理员随机生成 bds
- 2、管理员将 bds 拆分为 N 个分片

- 3、管理员对N个分片分别计算HMAC(Prvkey, Piece), 并将结果拼接到分片末尾
- 4、利用N个参与方的公钥分别对N个分片进行加密
- 5、将分片分别下发给N个参与方

bds恢复过程如下：

- 1、超级管理员发起bds恢复请求
- 2、各参与方将分片用超级管理员公钥加密并发送给超级管理员
- 3、超级管理员解密出分片明文和HMAC值，利用Prvkey和分片明文计算HMAC值并进行比对，确保返回的分片和原始的分片是相同的
- 4、超级管理员利用分片恢复出原始bds

