# VDB部署方案

1. Vdb验证整体交互图



图1 vdb查询验证



图2 vdb更新数据

表1 Proxy需要持久保存的数据

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 类别 | 名称 | 含义 | 是否公开 | 保存位置 | 使用者 |
| 双线性对运算需要的的参数  只在初始化时使用 | type | 双线对类型 |  |  | Proxy |
| p | 群的阶(质数) |  |  | Proxy |
| h |  |  |  | Proxy |
| r |  |  |  | Proxy |
| sign1 |  |  |  | Proxy |
| sign0 |  |  |  | Proxy |
| VDB客户端参数 | q | 数据库大小 | 是 |  | Proxy |
| G1XG1->G2 | pairing | 具体双线性对 |  |  | Proxy |
| PP(p,q,G,g,hi,hij) | g | 生成元 | 是 |  | Proxy |
| zi | 随机ZZp里选的n个数 | 否 |  | Proxy |
| hi=g^(zi) |  | 是 |  | Proxy |
| hij=g^(zi\*zj) |  | 是 |  | 公有云 |
|  | y  SK | 随机从ZZp中选取 | 否 |  |  |
| PK(PP,Y,CR,C0) | Y=g^(y) |  |  |  | Proxy |
| CR  C0  C-1 | 验证初始值 |  |  | Proxy |
| T | 更新次数 |  |  | Proxy |
| 程序 | vdb\_client | Proxy上的执行代码 |  |  | proxy |

表2服务器需要保存的数据

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 类别 | 名称 | 含义 | 是否公开 | 保存位置 | 使用者 |
| aux(生成证据需要的参数)  S(PP,aux,DB) | H0 |  | 是 |  | Server |
| C-1 |  | 是 |  | server |
| C0 |  | 是 |  | server |
| T | 更新次数 | 是 |  | Server |
|  | hij | 计算证据需要，大小为O(N^2) | 是 |  | Server |
| 程序 | vdb\_server | 云服务器端准备证据的程序 |  |  | Server |

目前代码完成了基本函数功能，可以做为一个库来调用实现具体的交互过程。

现在有如下疑问：

1. 验证中客户端的程序将来是独立的进程还是要与proxy合并到一起？与proxy的交互接口还没有定义。
2. 服务器端程序是独立进程还是要与哪些程序合并在一起？交互接口没有定义。
3. 验证客户端与服务器之间的交互协议还没设计。(比如一次更新请求，客户端更新了，结果服务器更新时出现故障，导致服务器没有更新，这时客户端与服务器不一致).

4. 要存储的数据是存在数据库呢还是文件？ 有的数据是保密的，应该怎么处理？

5. 需要选择生成群的参数 (表1中的 p,h,r,sign0,sign1), 目前使用的是PBC库给的默认参数，需要写一个工具来专门生成参数吗？