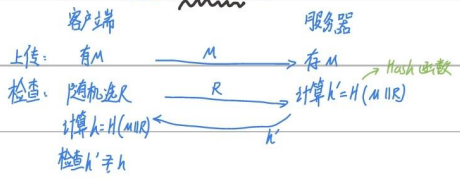
2021302181156 赵伯俣

设计一个方案

目的：检查服务器是否完整地保存了 M



问题：若 H 是 PPT 上的迭代结构 Hash 函数

说明上述方案不安全，并且修改使其安全

随 M 也可以出 h'

要解决的问题：服务器在没有 M 的情况下能够返回 $h'=H(M\|R)$

服务器在得到 M 后 找到 M 的第 $L-2$ 块 链接迭代后的结果记为 CV_{L-1}

我们知道 $H(M)=f(M_{L-1}, CV_{L-1})$

将 CV_{L-1} 和 M_{L-1} 保存，

等到要求发送 h' 时 将 R 拼在 M_{L-1} 后运算 $H(M_{L-1}\|R, CV_{L-1})$ 得到 h' 发送

即可保证既不完整保存 M 又可以发送出 h'

修改：客户端发送 R 后要求服务器返回 $h''=H(M_0\|R_0\|M_b\|R_b\|M_{2b}\|R_{2b}\cdots)$

其中内容的意思是将 M 每隔 b 位取一位 与 R 每隔 b 位取一位 拼接后

进行 Hash 运算，这样要求服务器必须完整保存 M 才可以输出正确值

方法2：客户端发送 R 后要求服务器返回 $h''=H(M')$

其中 M' 是由随机数 R 充当种子生成的一串随机序列来选取 M 的不同位

要求服务器从 M 中随机选取得到的 M' Hash 后得到 $h''=H(M')$ 返回

总的修改思路：将服务器要返回的 h' 的自变量分散到 M 中的一部分上，迫使

服务器只能保存完整的 M 才能返回正确的值。