



# 南开大学作业纸

系别 计算机科学与技术 班级 计科一班 姓名 郭坤高 2021/2022 第 页

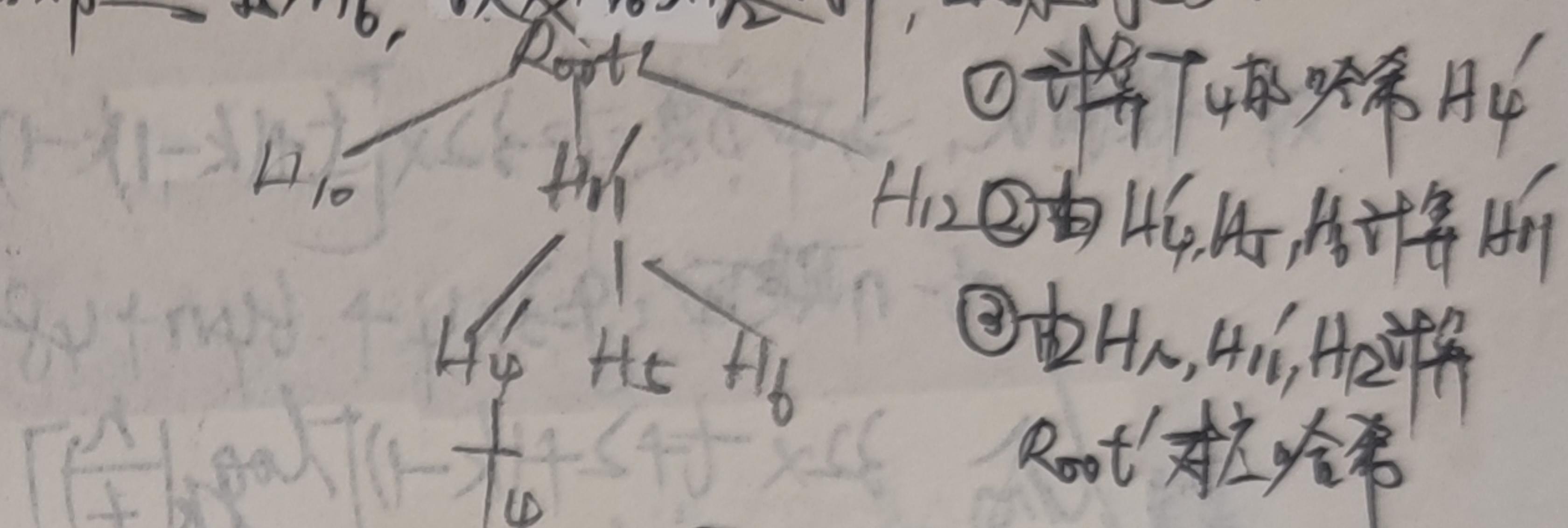
问题一：a. 构建如下所示之二叉merkle tree，(H表示哈希函数)，则根节点Root对应哈希值即为

$$Root = H_3 = H(H_0, H_1, H_2)$$

$$S = \{T_1, T_2, \dots, T_9\} \text{ 而承证。}$$

若要证明  $T_4$  在  $S$  中，则需要提供与  $T_4$  相邻的  $T_5, T_6$  对应的哈希值  $H_5, H_6$ ，以及  $H_5, H_6$  之父哈希值  $H_4$ 。

$$\begin{array}{c} H_0 = H(A_1, A_2, A_3) \\ H_1 = H(A_4, A_5, A_6) \\ H_2 = H(A_7, A_8, A_9) \\ H_3 = H(H_0, H_1, H_2) \\ H_4 = H(H_5, H_6, H_7) \\ H_5 = H(T_1, T_2, T_3) \\ H_6 = H(T_4, T_5, T_6) \\ H_7 = H(T_7, T_8, T_9) \end{array}$$



① 证明  $T_4$  对应哈希  $H_4$   
② 由  $H_4, H_5, H_6$  计算  $H_7$   
③ 由  $H_1, H_2, H_3$  计算  $H_0$   
Root' 对应哈希

④ 通过比较  $Root'$  与  $Root$  是否相等，即可知  $H_4$  是否在  $S$  中

包含在证明中取值为  $H_4, H_5, H_6, H_0, H_1, H_2$

b. 由merkle tree的结构和性质，证明  $S[i] = T_i$  为从下向上与其哈希值计算  $Root$  的过程。

这里将证明长度记为所有需要提供参与计算的节点数量。

则除去根节点  $T_0$  以下，每层需要  $k-1$  个节点，而merkle tree高为  $\lceil \log_k n \rceil + 1$ 。

∴ 证明长度  $L = 2 + (k-1) \lceil \log_k n \rceil$

c. 对应较大数  $n$  由于

$$\lim_{n \rightarrow \infty} \frac{2 + (k-1) \log_k n}{2 + 3 + \log_2 n} = \lim_{n \rightarrow \infty} \frac{\log_2 n}{\log_2 n} = \lim_{n \rightarrow \infty} \frac{n \ln 2}{n \ln 3} = \frac{\ln 2}{\ln 3} < 1$$

∴ 证明二叉merkle tree较好些

2. ∵  $Q$  是  $q$  阶循环群， $\therefore q^2 = 1$

$$\text{则 } Q = H(m)^X = H(m)^{x_1+x_2+x_3 \bmod q} = H(m)^{x_1+x_2+x_3 \bmod q} = H(m)^{x_1+x_2+x_3} = H(m)^{x_1 \oplus x_2 \oplus x_3} = H(m)^{x_1} \cdot H(m)^{x_2} \cdot H(m)^{x_3} = Q_1 \cdot Q_2 \cdot Q_3$$

即 Bob 需要将 3 人的部分签名加起来求得 m 的签名

3. 需要证  $p_{ki}$  对应方案的节点是否在 merkle tree 中，由问题一，验证  $p_{ki}$  存在于需要树中其他相关节点签名，还需要计算  $p_{ki}$  对应签名，即根据  $p_{ki}$  对应方案的私钥对应的签名，即  $\sigma_{ij}, \sigma_{i2}, \sigma_{i3}$ ，其中  $\sigma_{ij} = H(m)^{x_{ij}}$ ，且满足  $p_{ki} = H(m)^{x_i}$ ， $x_i = x_{i1} + x_{i2} + x_{i3} \bmod q$

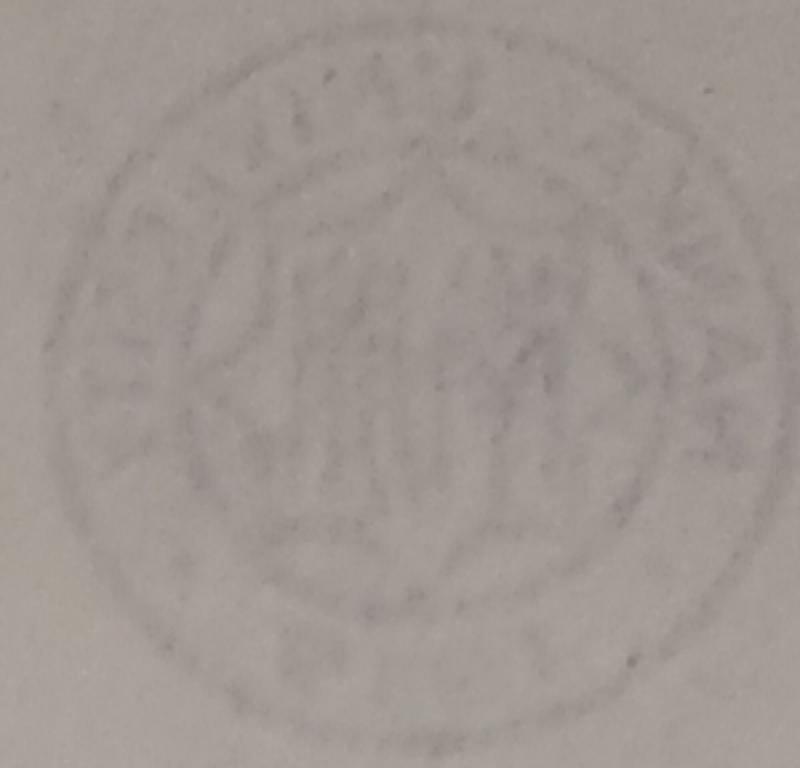
总结如：需要树中其他相关节点签名及三方签名  $\sigma_{ij}, \sigma_{i2}, \sigma_{i3}$

3. 证明 merkle tree 验证的 2 方案，证明长度  $= 2 + (k-1) \lceil \log_k n \rceil$ ，耗费字节： $32 \times (2 + (k-1) \lceil \log_k n \rceil)$

$$= 2 + (k-1) \lceil \log_k 10 \rceil \text{ 计算公钥花费字节：} 3 \times 32 = 96 \text{ (最终结果记在树中)}$$

(未下页)

# 毕业设计



$k=2$  时证明长度收时最近(代入既往)

因此该方案长度字节数 =  $32 \times (t+2+(k-1)\log_k(10)) = 32 \times (5+4) = 288$  字节  
 而脚本证高:  $3 \times 4 + 5 \times 64 + 3 \times 48 = 476$  字节 > 288  
 (包含 3-5 及高输出冗余)  
 $\therefore$  该方案有更少字节数

$$\begin{aligned}
 \text{对一般情况,} \rightarrow \text{该方案 } f = 32 \times \left[ t + 2 + (k-1) \log_k \left( \frac{n}{t} \right) \right], \text{ 当 } n \text{ 大时, } f \leq 32 \times \left[ \frac{1}{2} + 2 + (k-1) \log_k \left( \frac{n}{\frac{1}{2}} \right) \right] \\
 = 32 \left( \frac{1}{2} + 2 + (k-1) \log_k \left( \frac{n!}{(\frac{n}{2})! (\frac{n}{2})!} \right) \right) \\
 \approx 32 \left( \frac{1}{2} + 2 + (k-1) \log_k \left( \frac{\sqrt{2\pi n} \left( \frac{n}{e} \right)^n}{\left( \frac{n}{2} \right)^n} \right) \right) \\
 = 32 \left( \frac{1}{2} + 2 + (k-1) \log_k \left( 2^{\frac{n}{2}} \cdot n^{-\frac{1}{2}} \right) \right) \\
 \stackrel{k=2}{=} 32 \left[ \frac{1}{2} + 2 + \log_2 \left( \frac{2^n}{\sqrt{\pi n}} \right) \right] \\
 = 16n + 96 + 32(n - \frac{1}{2}) - 16 \log_2 n \\
 = 48n + 80 - 16 \log_2 n
 \end{aligned}$$