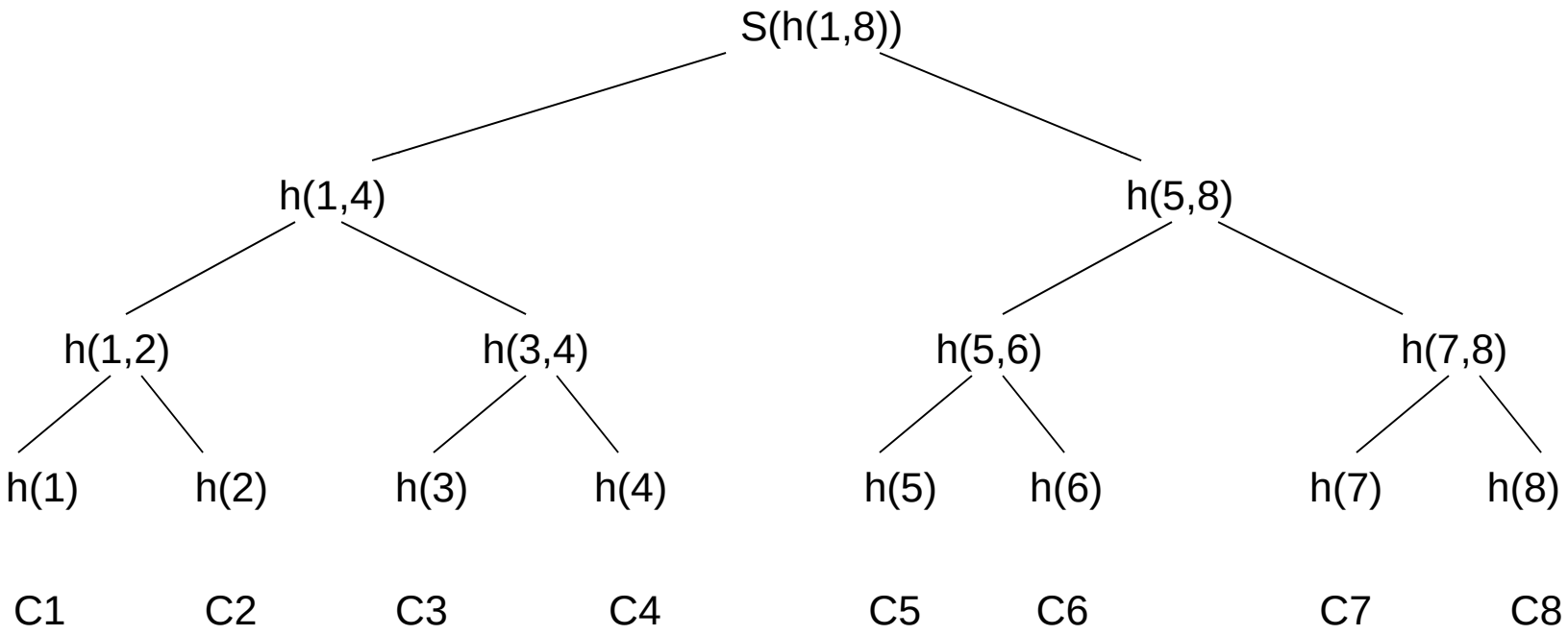
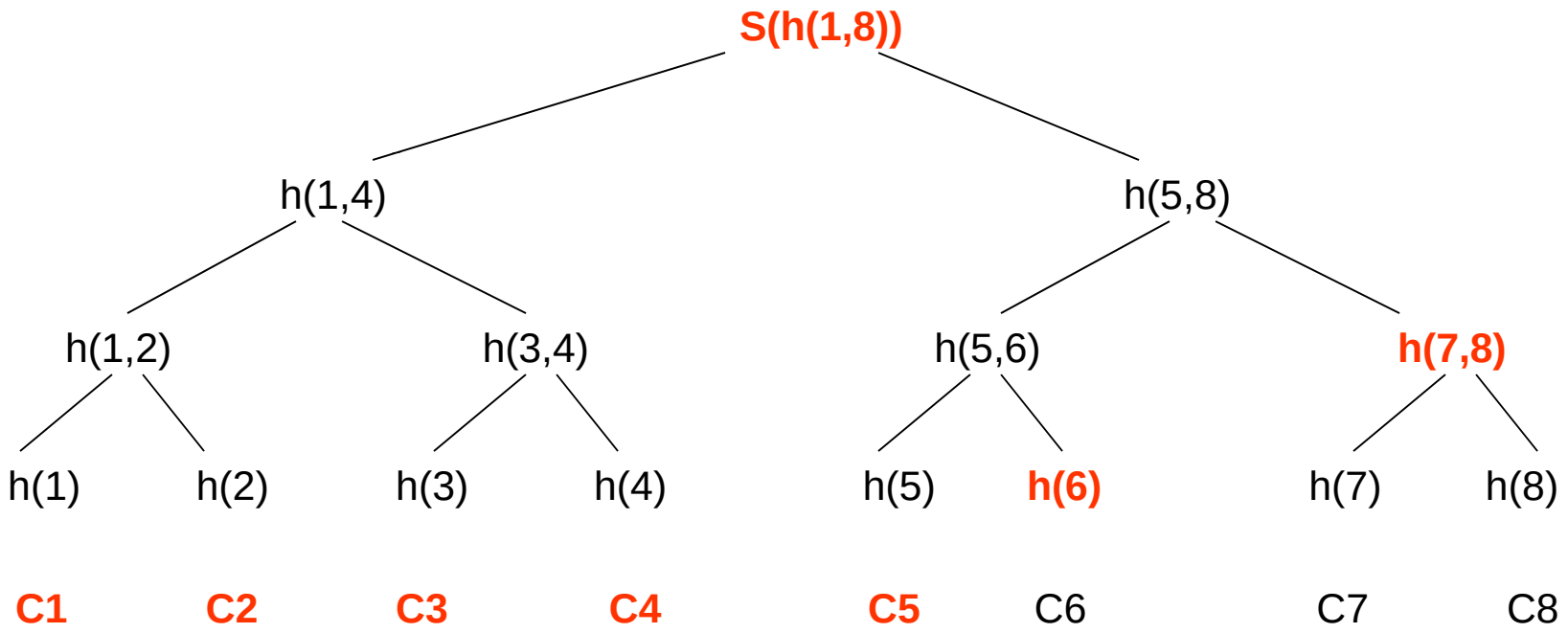
Review: Query Authentication

MHT



What needs to be returned for range query [C1, C4]?

MHT


S(h(1,8))
h(1,4)
h(5,8)
h(1,2)
h(3,4)
h(5,6)
h(7,8)
h(1)
h(2)
h(3)
h(4)
h(5)
h(6)
h(7)
h(8)
C1
C2
C3
C4
C5
C6
C7
C8

Signature Chain

- How about using the signature chaining scheme?

C1 C2 C3 C4 C5 C6 …

$h^{\alpha - r_{a-1} - 1}(r_{a-1})$

hash
U - α
times

$h^{r_{b+1} - \beta - 1}(r_{b+1})$

hash
β - L
times

- How about using the signature chaining scheme?

L C0 **C1** **C2** **C3** **C4** C5 … U

sig(C1) sig(C2) sig(C3) sig(c4) $\mathbf{h^{C5 - \beta - 1}(C5)}$

Signature chain: $sig(r_i) = s(h(g(r_{i-1}) \mid g(r_i) \mid g(r_{i+1})))$

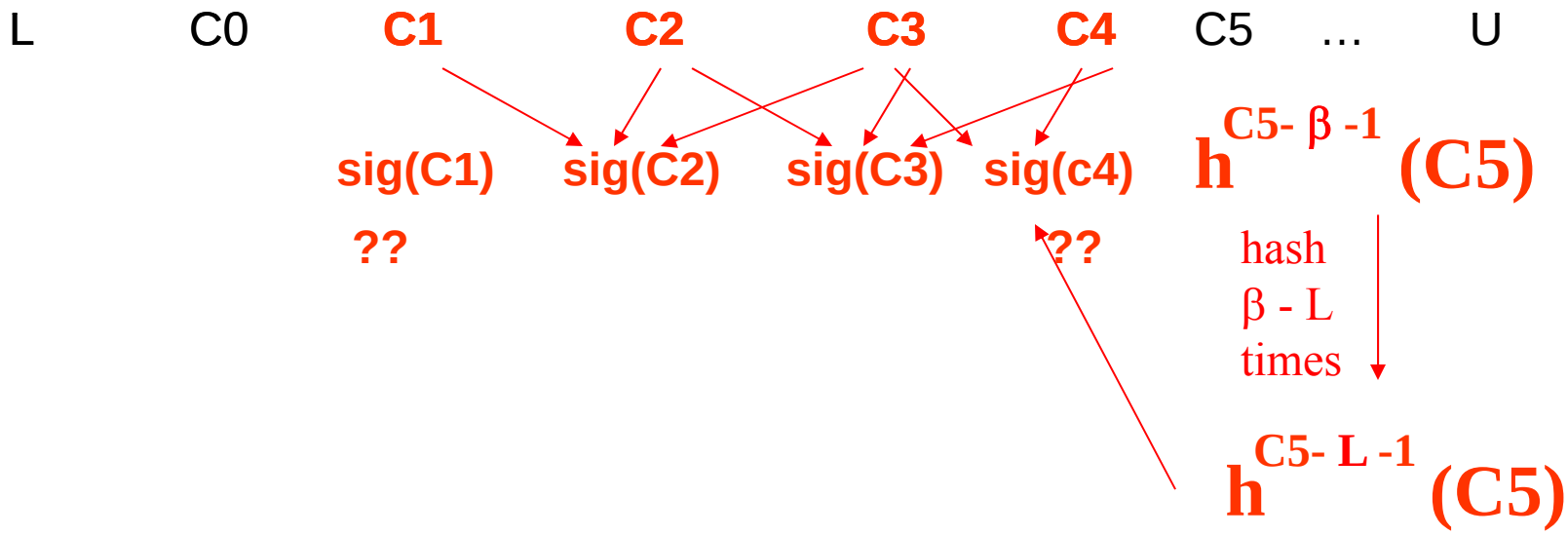
$h^{\alpha - r_{a-1} - 1}(r_{a-1})$

hash
U - α
times

$h^{r_{b+1} - \beta - 1}(r_{b+1})$

hash
β - L
times

- How about using the signature chaining scheme?



Signature chain: $sig(r_i) = s(h(g(r_{i-1}) \mid g(r_i) \mid g(r_{i+1})))$