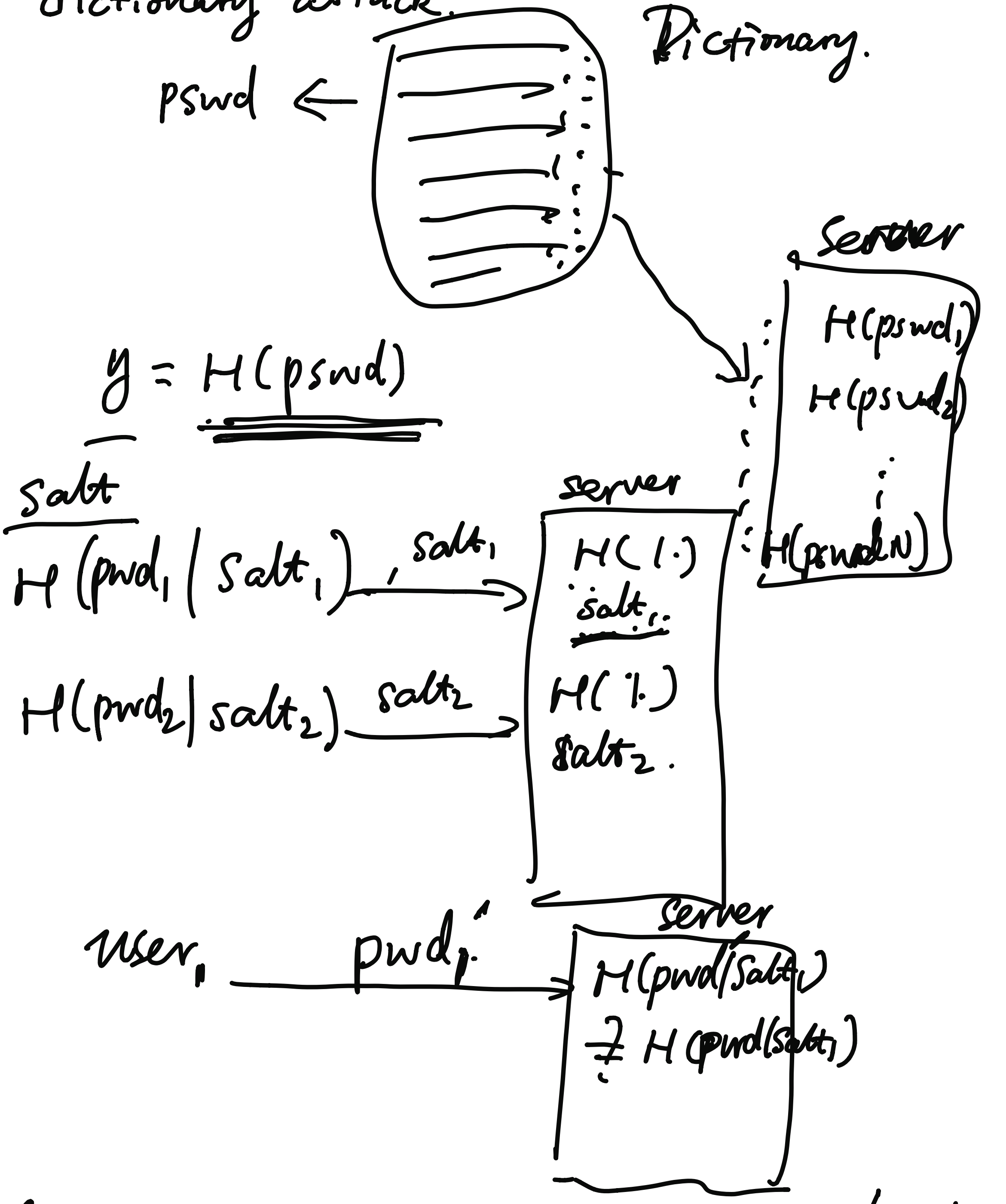
ECE 471/571 Hash Applications (Cont'd)

dictionary attack.



salt increases attacker's effort to break all pswds

One-way hash chain

(one-time password)

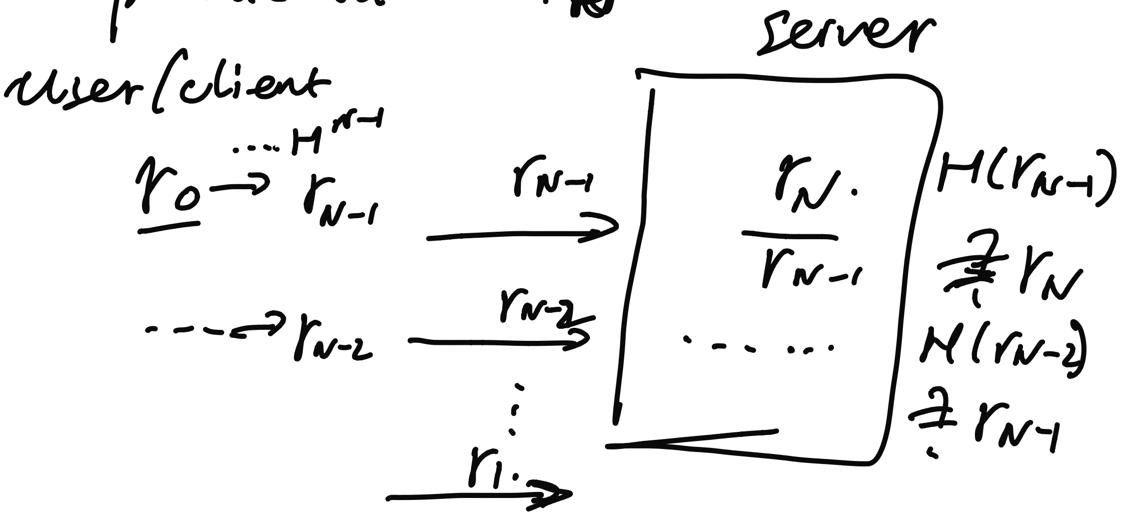
① . pick random r_0 . hash $H(\cdot)$

② . $r_{i+1} = H(r_i)$

$$r_N \xleftarrow{H.} r_{N-1} \cdots r_2 \xleftarrow{H} r_1 \xleftarrow{H} r_0$$

③ secret value r_0

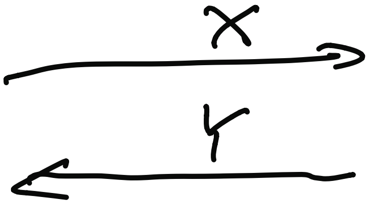
public value r_N



Commitment

A B

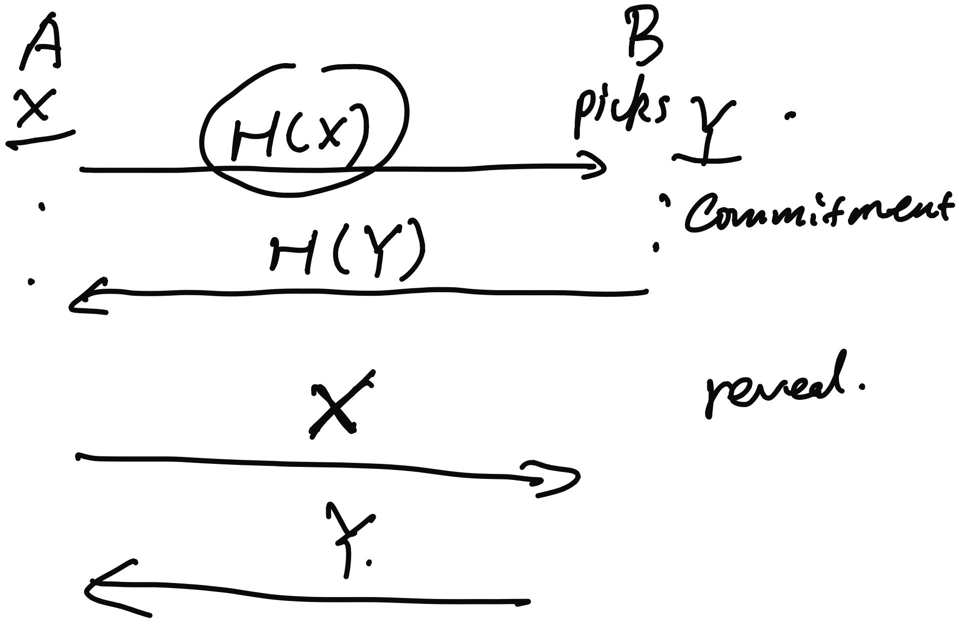
X Y



If X is odd
pick
Y is odd.

wins
X+Y is even

wins
X+Y is odd


A
B
X
picks Y
H(X)
Commitment
H(Y)
reveal.
X
Y.