

Robust DiSE

Dr. Xunhua Wang

Share

Partial result

Threshold t

of servers: n

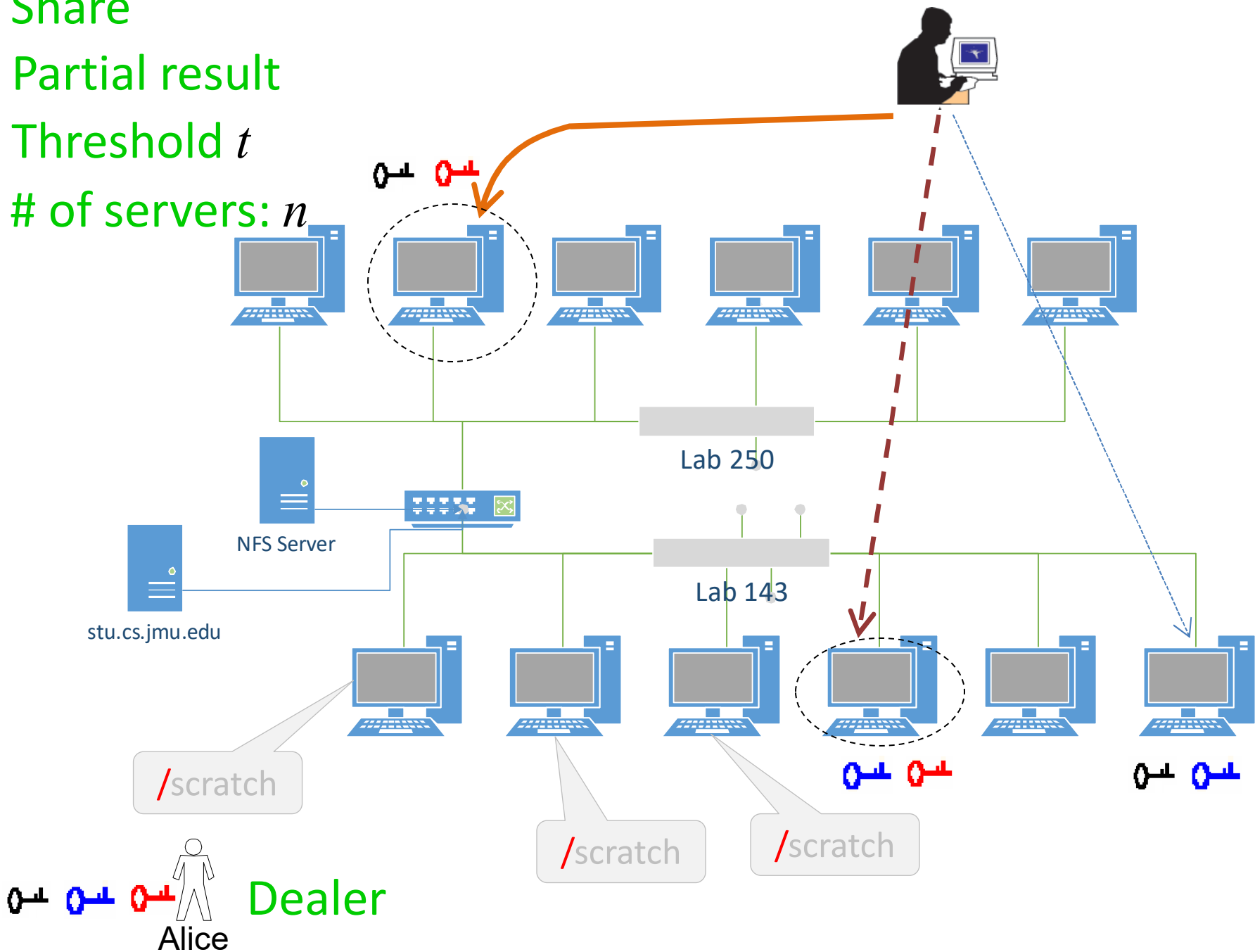
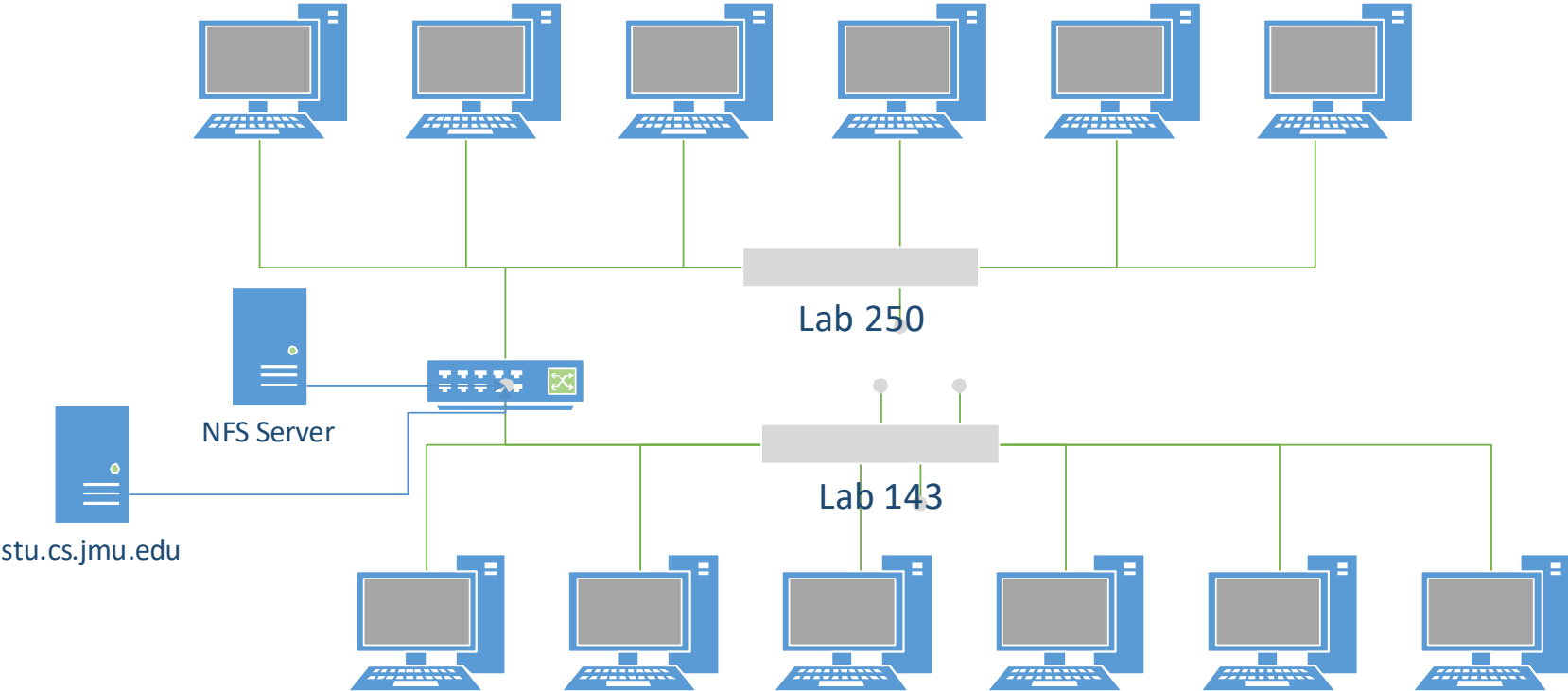


Table 1: Symmetric key assigned for $(t = 3, n = 5)$

Server	Assigned keys					
A	k_1	k_2	k_3	k_4	k_5	k_6
B	k_1	k_2	k_3	k_7	k_8	k_9
C	k_1	k_4	k_5	k_7	k_8	k_{10}
D	k_2	k_4	k_6	k_7	k_9	k_{10}
E	k_3	k_5	k_6	k_8	k_9	k_{10}

Table 2: Ω for $(t = 3, n = 5)$

Server	IDs of assigned keys					
A	1	2	3	4	5	6
B	1	2	3	7	8	9
C	1	4	5	7	8	10
D	2	4	6	7	9	10
E	3	5	6	8	9	10





Alice

Table 1: Symmetric key assigned for $(t = 3, n = 5)$

Server	Assigned keys					
A	k_1	k_2	k_3	k_4	k_5	k_6
B	k_1	k_2	k_3	k_7	k_8	k_9
C	k_1	k_4	k_5	k_7	k_8	k_{10}
D	k_2	k_4	k_6	k_7	k_9	k_{10}
E	k_3	k_5	k_6	k_8	k_9	k_{10}

Table 2: Ω for $(t = 3, n = 5)$

Server	IDs of assigned keys					
A	1	2	3	4	5	6
B	1	2	3	7	8	9
C	1	4	5	7	8	10
D	2	4	6	7	9	10
E	3	5	6	8	9	10

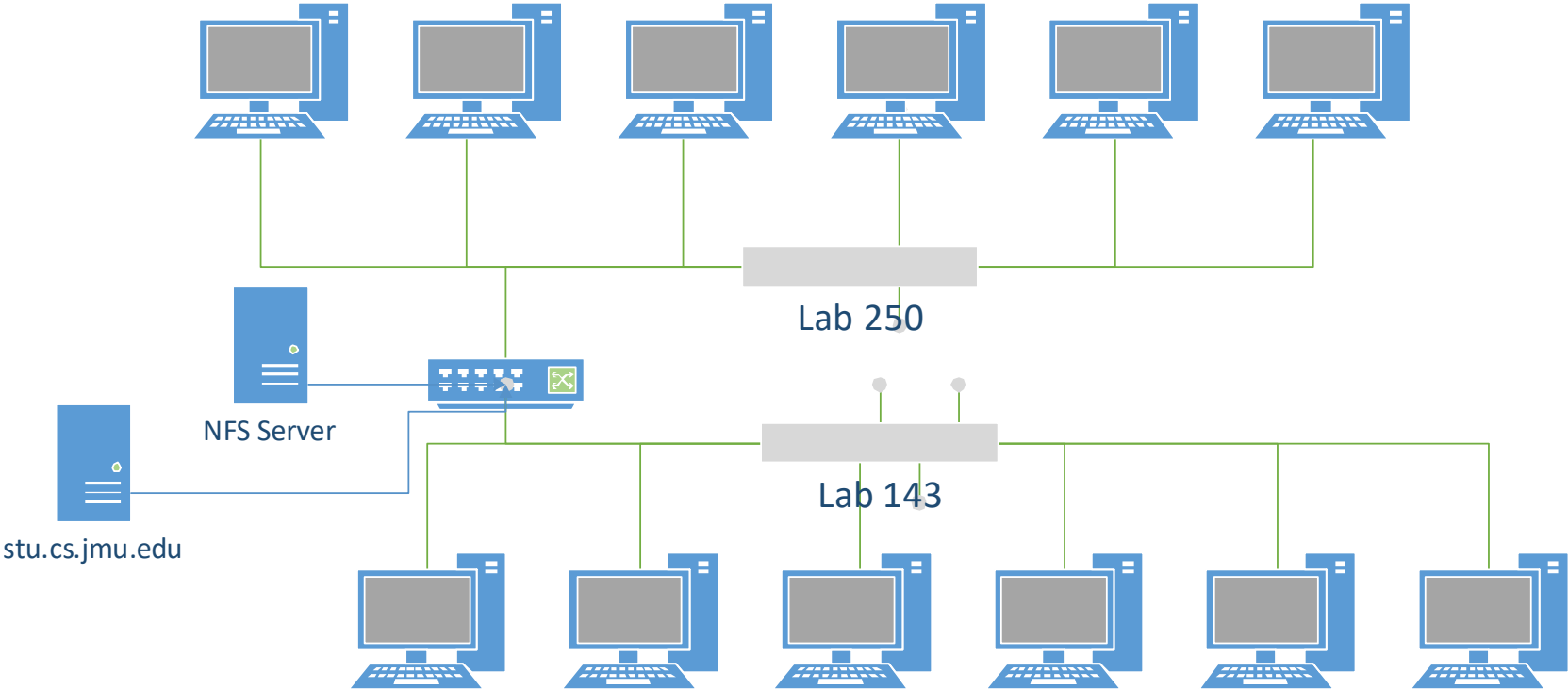


Table 3: Robust DiSE for $(t = 3, n = 5, \delta = 1)$

Participating servers	Partial results contributed									
B (initiator)	w_1	w_2	w_3				w_7	w_8	w_9	
C				w_4	w_5					
D				w_4		w_6				w_{10}
E					w_5	w_6				w_{10}



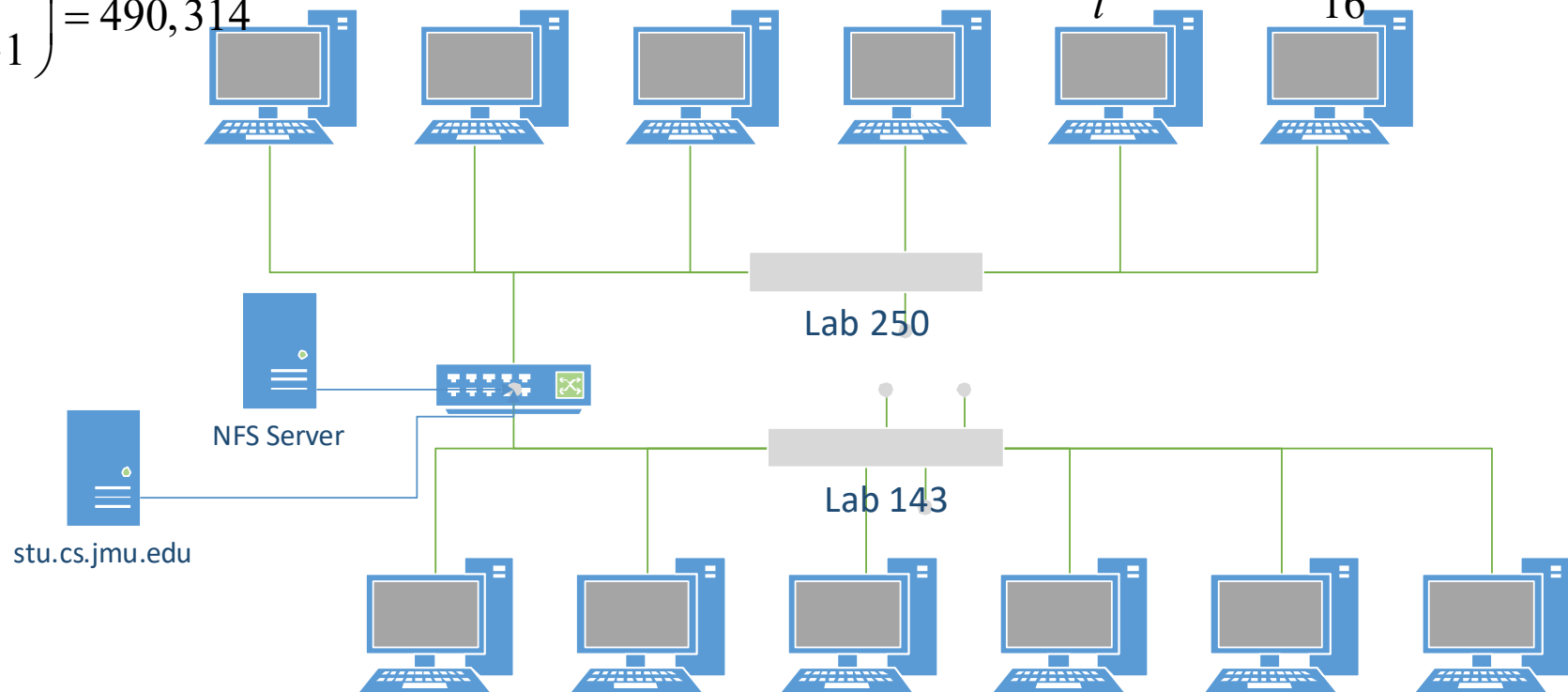
$t = 16, n = 24$

$$\binom{n}{t-1} = 1,307,504 \quad \frac{\binom{n}{t-1}}{t} = \frac{1,307,504}{16} = 81,719$$

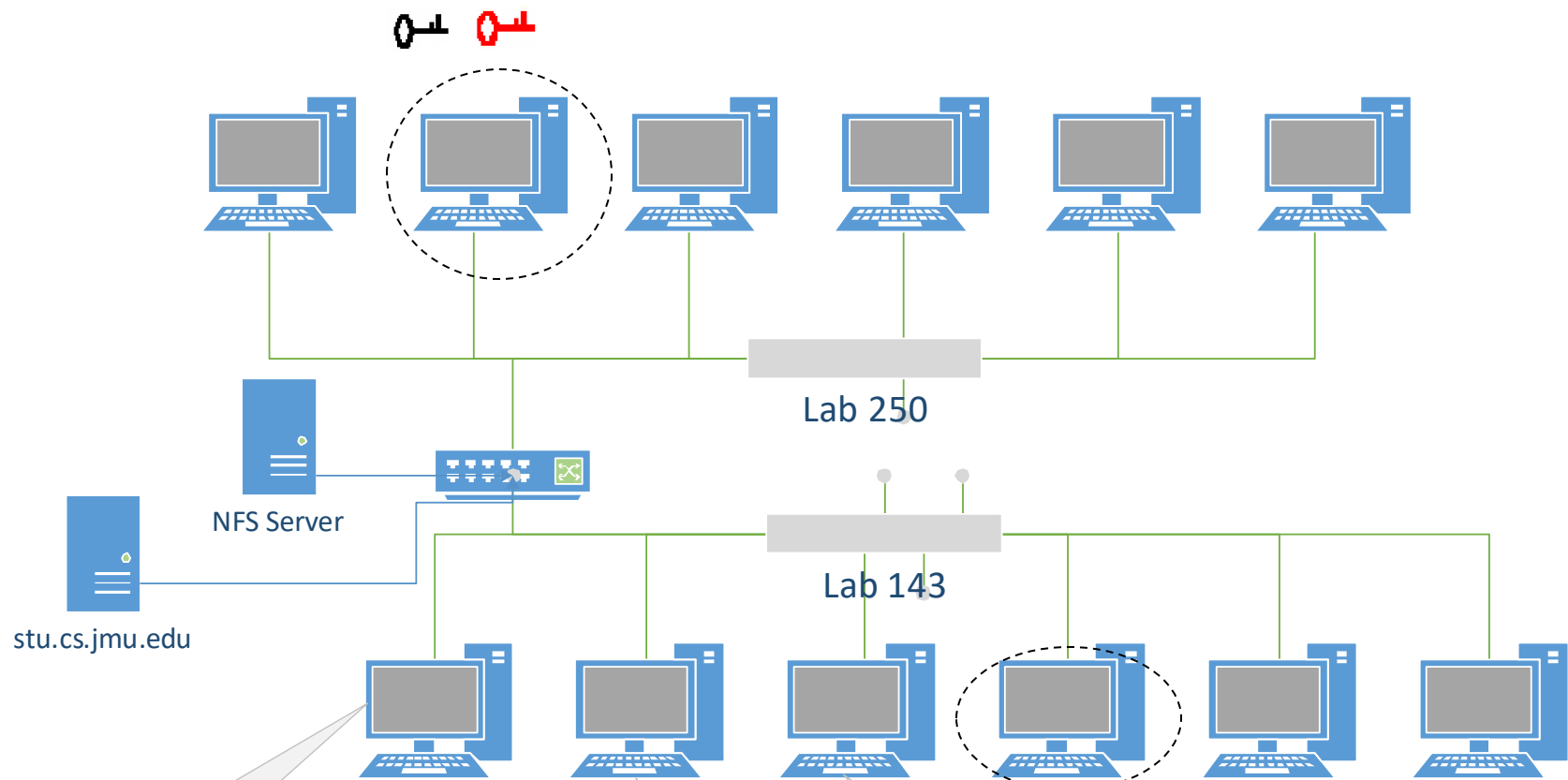
$$\binom{n-1}{t-1} = 490,314$$

$$\binom{n-1}{t-2} = 817,190$$

$$\frac{\binom{n-1}{t-2} \times 2}{t} = \frac{817,190 \times 2}{16} \approx 102,149$$



Alice



/scratch

/scratch

/scratch

key key key Alice Dealer