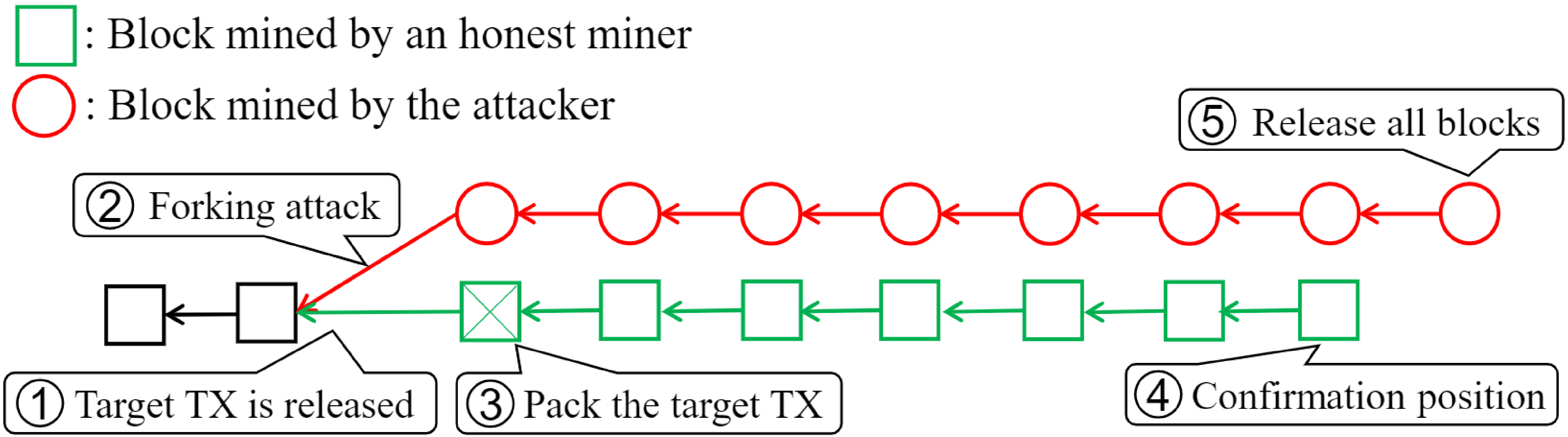
中山大學
SUN YAT-SEN UNIVERSITY

Revisiting Double-Spending Attacks on the Bitcoin Blockchain: New Findings

Jian Zheng, Huawei Huang, Canlin Li, Zibin Zheng, Song Guo*
School of Computer Science and Engineering, Sun Yat-Sen University, Guangzhou, China
*Department of Computing, The Hong Kong Polytechnic University, Hong Kong.

Presentation for IWQoS 2021

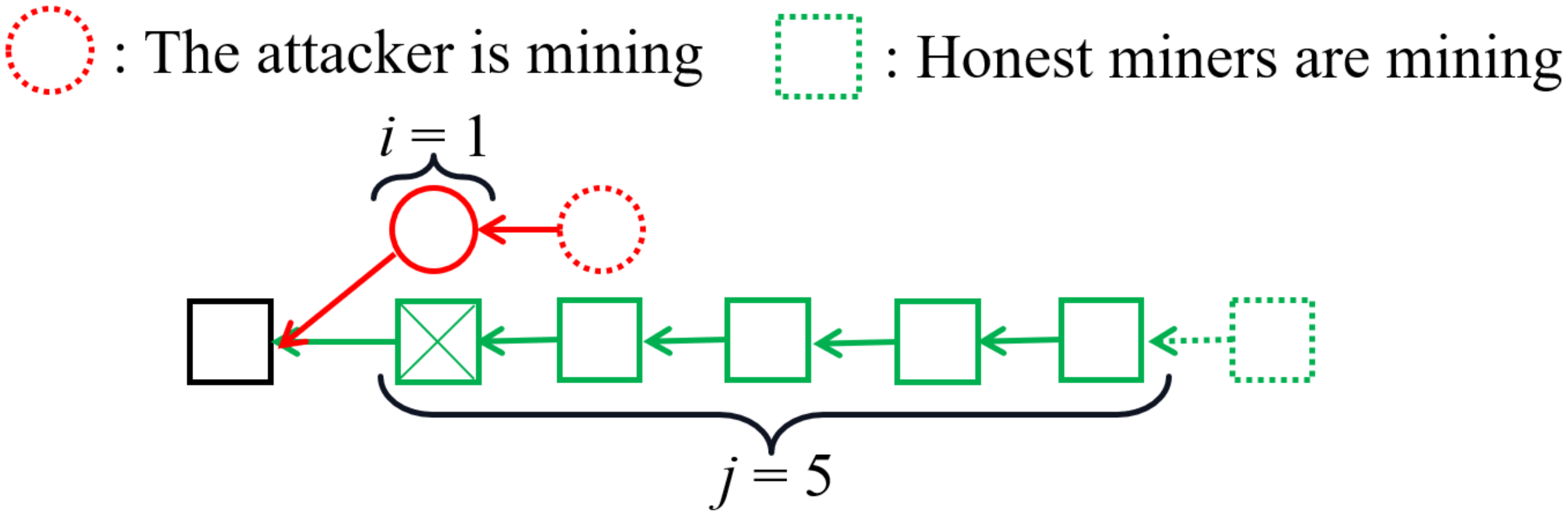
Double-Spending Attack



Our contribution

- **Adaptive DSA**: Adaptive Double-Spending Attack
- Profit-maximized attack strategy by Stochastic Dynamic Programming (SDP)
- Analytical model for simulation

An unfavourable situation to the attacker

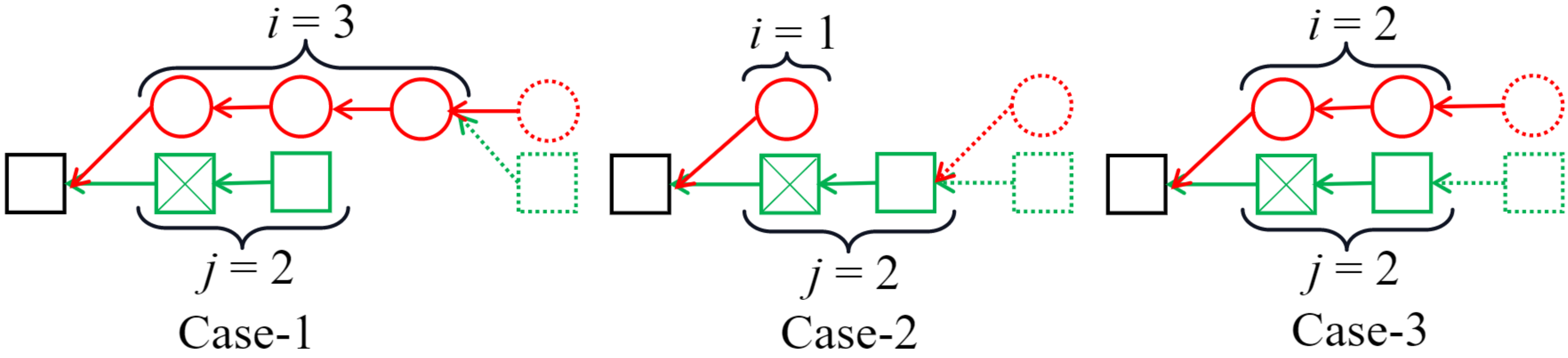


- The transaction has not been confirmed in $S_{1,5}$.

- **Should the attacker give up?**

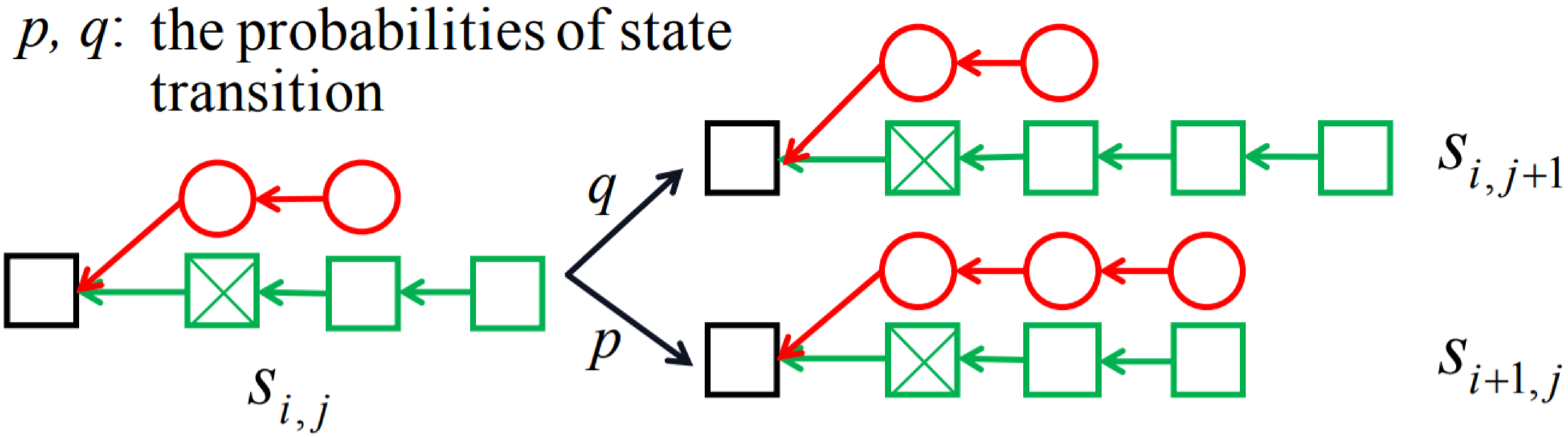
Attack decision: Quit or Keep

- **0**: Quit attacking



Attack decision: Quit or Keep

- **1:** Keep attacking



Attack-Decision Matrix

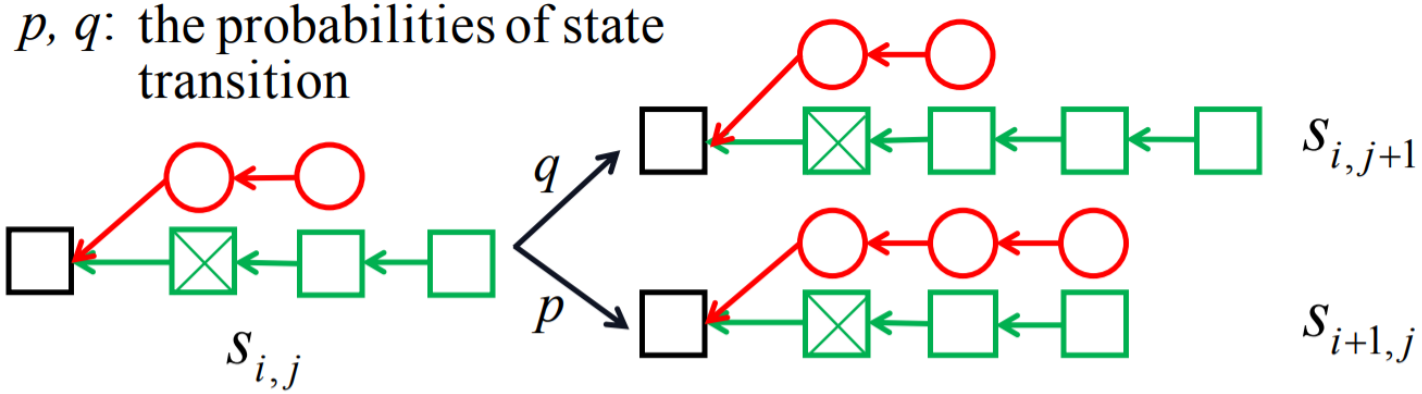
- **Variables:** $d_{i,j} \in \{0, 1\}$
  - **0**: Quit attacking
  - **1**: Keep attacking
- **Profit:** $f(\{d_{i,j}\})$
- **Tools:**
  - Occurrence-Probability Matrix
  - Reward Matrix

$d_{i,j}$	0	1	2	3	4	5	6
0	?	?	?	?	?	?	0
1	?	?	?	?	?	?	0
2	?	?	?	?	?	?	0
3	?	?	?	?	?	?	0
4	?	?	?	?	?	?	0
5	?	?	?	?	?	?	0
6	0	0	0	0	0	0	

Occurrence-Probability Matrix

$$P_{i,j} = \begin{cases} 1, \text{ if } i = j = 0; \\ d_{i-1,j} \cdot p \cdot P_{i-1,j}, \text{ if } j = 0 \text{ or } i = z; \\ d_{i,j-1} \cdot q \cdot P_{i,j-1}, \text{ if } i = 0 \text{ or } j = z; \\ d_{i-1,j} \cdot p \cdot P_{i-1,j} + d_{i,j-1} \cdot q \cdot P_{i,j-1}, \text{otherwise.} \end{cases} \quad (1)$$

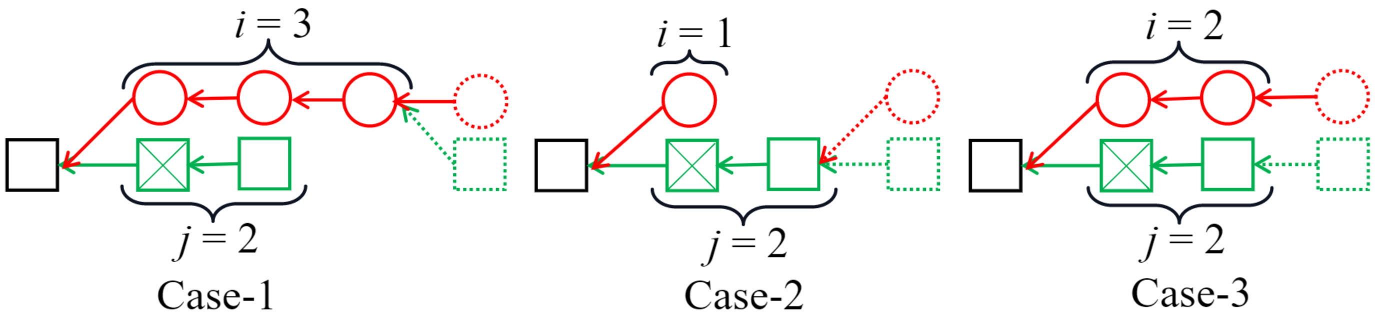
p, q: the probabilities of state transition



$P_{i,j}$	0	1	2	3	4	5	6
0	1	?	?	?	?	?	?
1	?	?	?	?	?	?	?
2	?	?	?	?	?	?	?
3	?	?	?	?	?	?	?
4	?	?	?	?	?	?	?
5	?	?	?	?	?	?	?
6	?	?	?	?	?	?	

Reward Matrix

$$R_{i,j} = \begin{cases} -(i+j)\cdot cost, \text{ if } i < j; \\ i \cdot d - (i+j)\cdot cost, \text{ if } z > i > j; \\ p \cdot i \cdot d - (i+j)\cdot cost, \text{ if } z > i = j; \\ p[b + d(z+1) - (i+j+1)\cdot cost] + q \cdot R_{i,j+1}, \\ \quad \text{if } i = z, j \leq z-2; \\ p[b + d(z+1) - (i+j+1)\cdot cost] + \\ \quad q[p(b + z\cdot d) - 2z \cdot cost], \text{ if } i = z, j = z-1. \end{cases} \tag{2}$$



$R_{i,j}$	0	1	2	3	4	5	6
0	?	?	?	?	?	?	?
1	?	?	?	?	?	?	?
2	?	?	?	?	?	?	?
3	?	?	?	?	?	?	?
4	?	?	?	?	?	?	?
5	?	?	?	?	?	?	?
6	?	?	?	?	?	?	

Profit-Maximization Problem

- **0**: Quit attacking
- **1**: Keep attacking

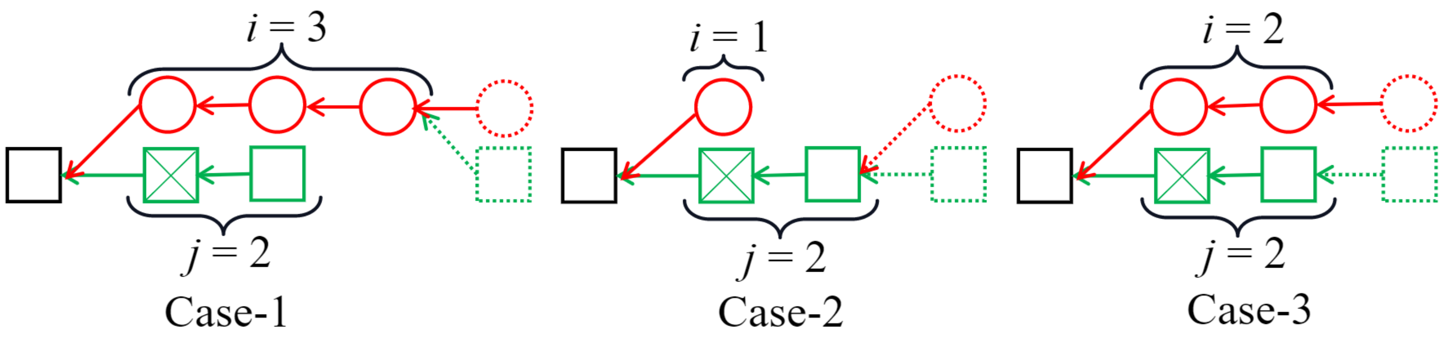
$$d_{i,j} \in \{0,1\}$$

$$\max \ f(\{d_{i,j}\}) = \sum_{i=0}^{z} \sum_{j=0}^{z} (1 - d_{i,j}) \cdot P_{i,j} \cdot R_{i,j}$$

Stochastic Dynamic Programming (SDP)

- $d_{i,j}$=0, quit attacking

$$J_n(s_{i,j}) = J_{n+1}(s'_{i,j}) = \begin{cases} 0, & \text{if } 0 \le i < j \le z-1; \\ i \cdot d, & \text{if } 0 \le j < i \le z-1; \\ p \cdot i \cdot d, & \text{if } 0 \le i = j \le z-1. \end{cases}$$



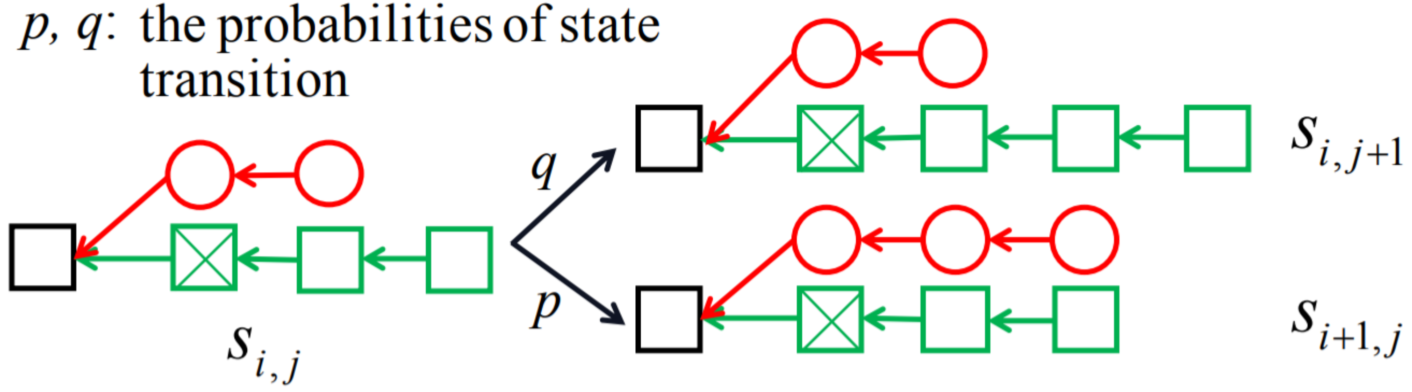
$J_n(s_{i,j})$	0	1	2	3	4	5	6
0	?	?	?	?	?	?	?
1	?	?	?	?	?	?	?
2	?	?	?	?	?	?	?
3	?	?	?	?	?	?	?
4	?	?	?	?	?	?	?
5	?	?	?	?	?	?	?
6	?	?	?	?	?	?	

Stochastic Dynamic Programming (SDP)

- $d_{i,j}$=1, keep attacking

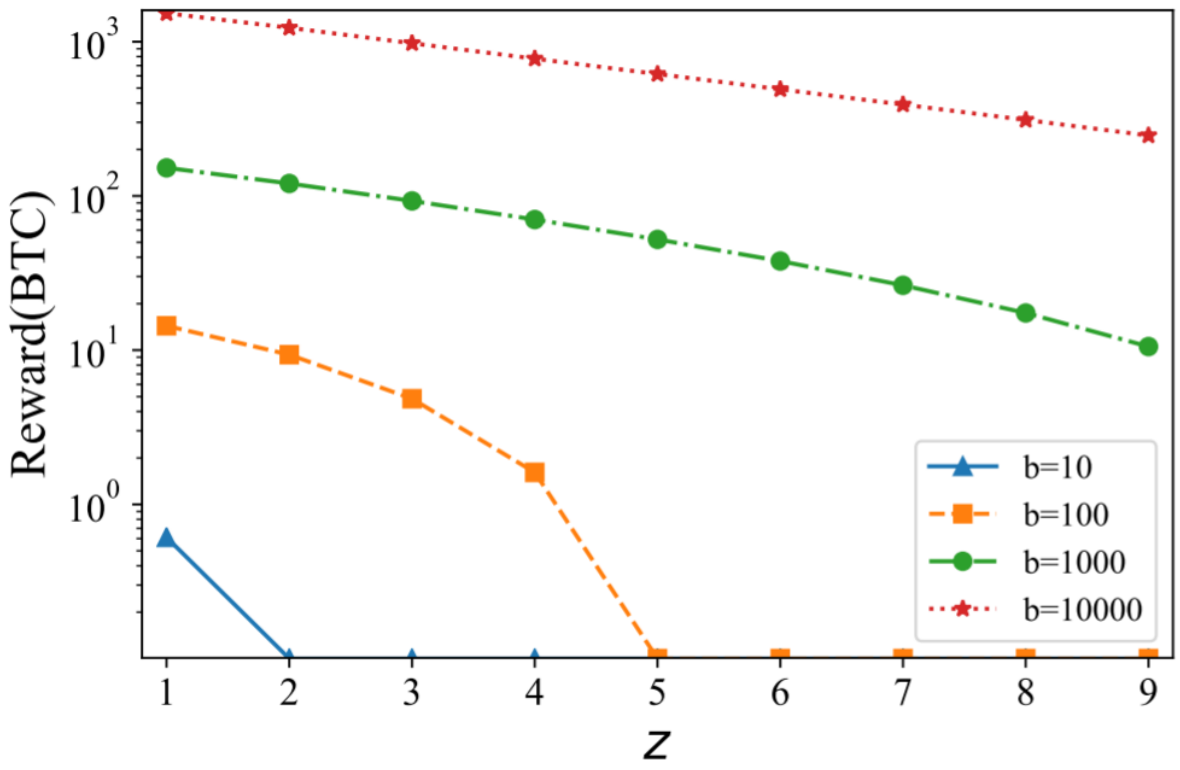
$$J_n(s_{i,j}) = -cost + p \cdot J_{n+1}(s_{i+1,j}) + q \cdot J_{n+1}(s_{i,j+1})$$

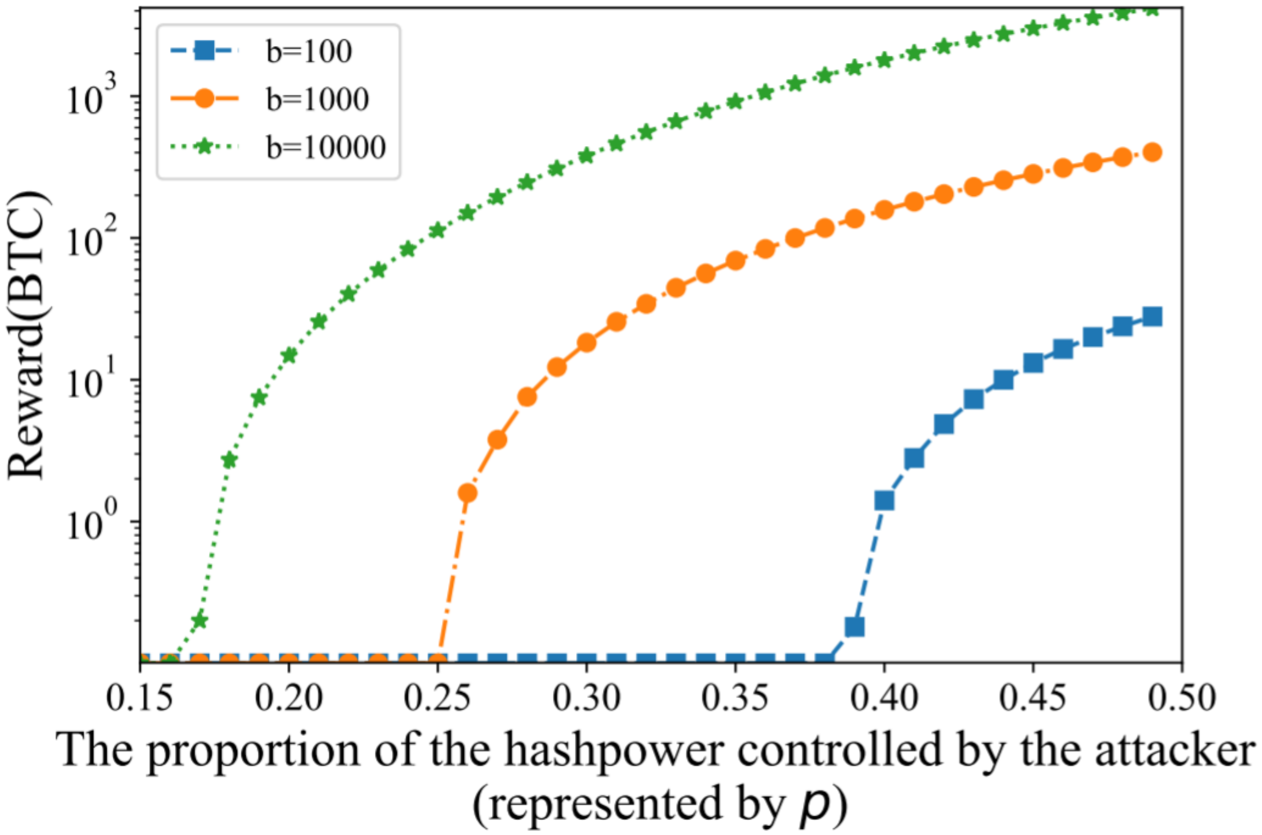
p, *q*: the probabilities of state transition



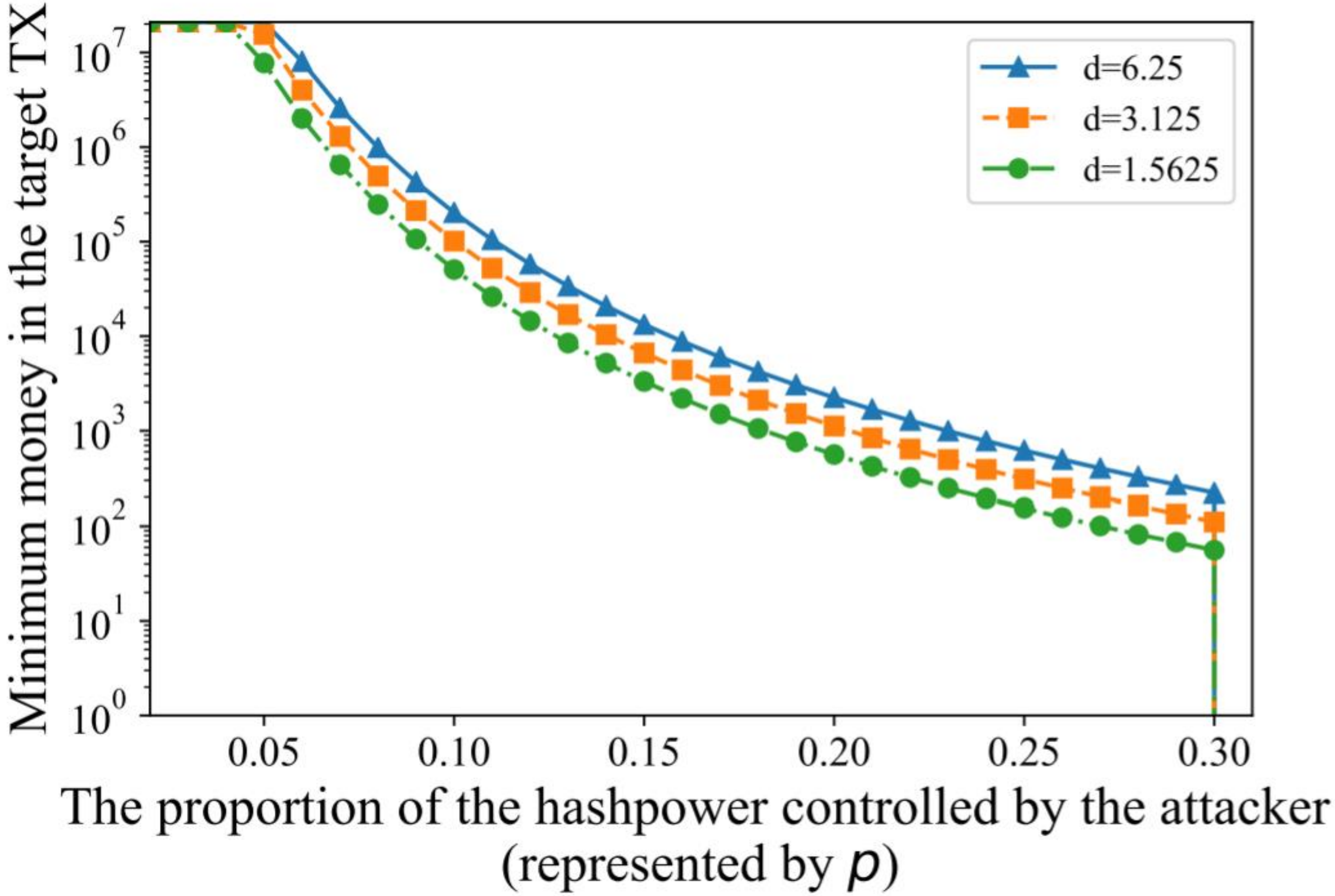
$J_n(s_{i,j})$	0	1	2	3	4	5	6
0	?	?	?	?	?	?	?
1	?	?	?	?	?	?	?
2	?	?	?	?	?	?	?
3	?	?	?	?	?	?	?
4	?	?	?	?	?	?	?
5	?	?	?	?	?	?	?
6	?	?	?	?	?	?	

Performance Evaluation





Performance Evaluation



Conclusion

- **Adaptive DSA**: new threat to PoW-based blockchains
- 50% is not enough
- More strategies in the double-spending attack

Thanks

HuangLab@SYSU http://xintelligence.pro/