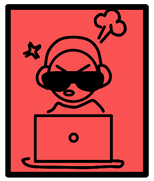
A can create n puzzles with O(n) effort.

B can solve 1 puzzle with O(n) effort.



Attacker needs to solve puzzles until correct ID (+ matching key) is found

→ on average: n/2 puzzles, meaning $O(n^2)$ effort