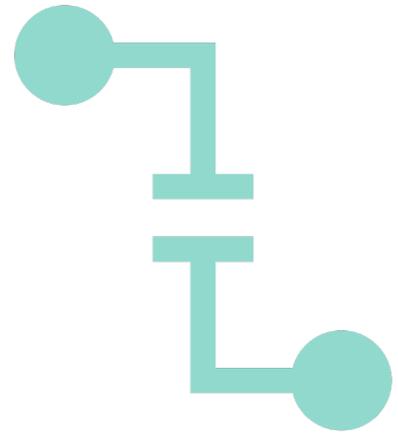
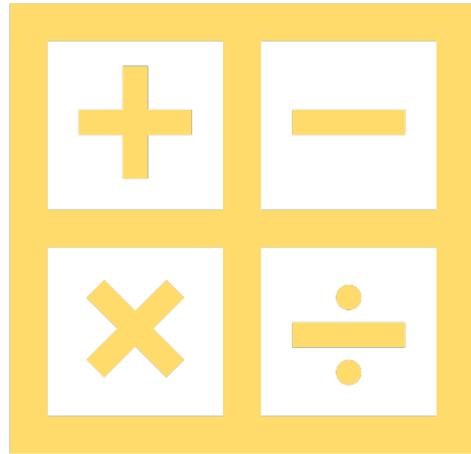
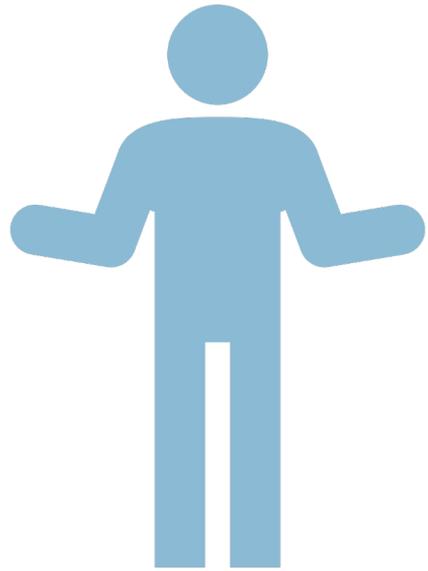
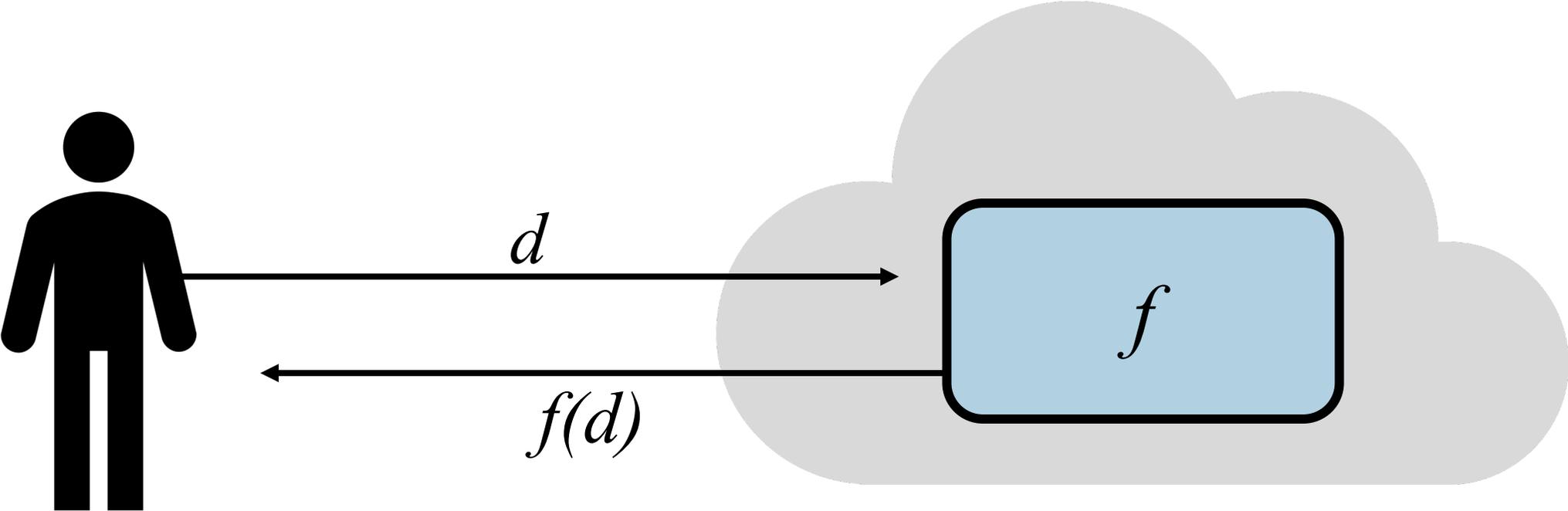


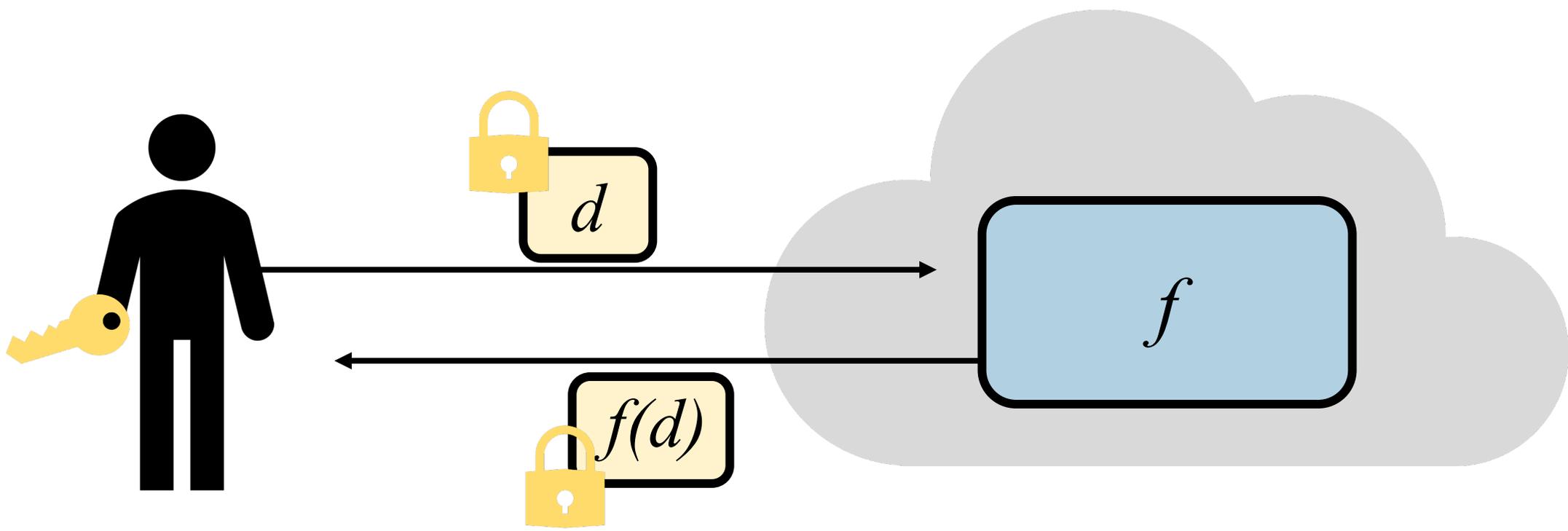
PARALLELIZATION OF FULLY HOMOMORPHIC DATA ENCODING

JESS WOODS

COMPUTER SCIENCE RESEARCH







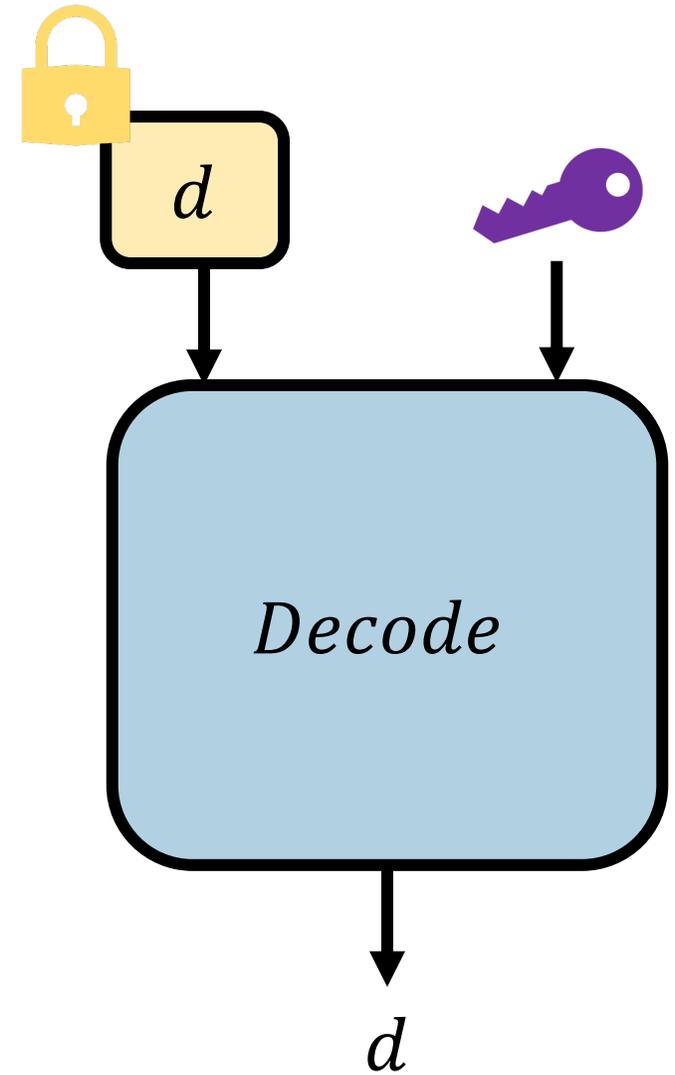
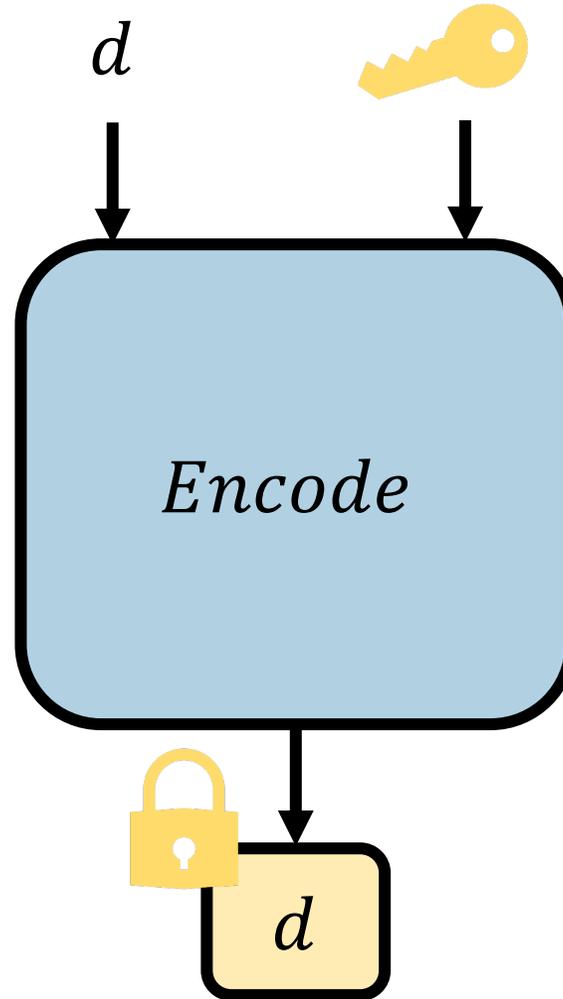
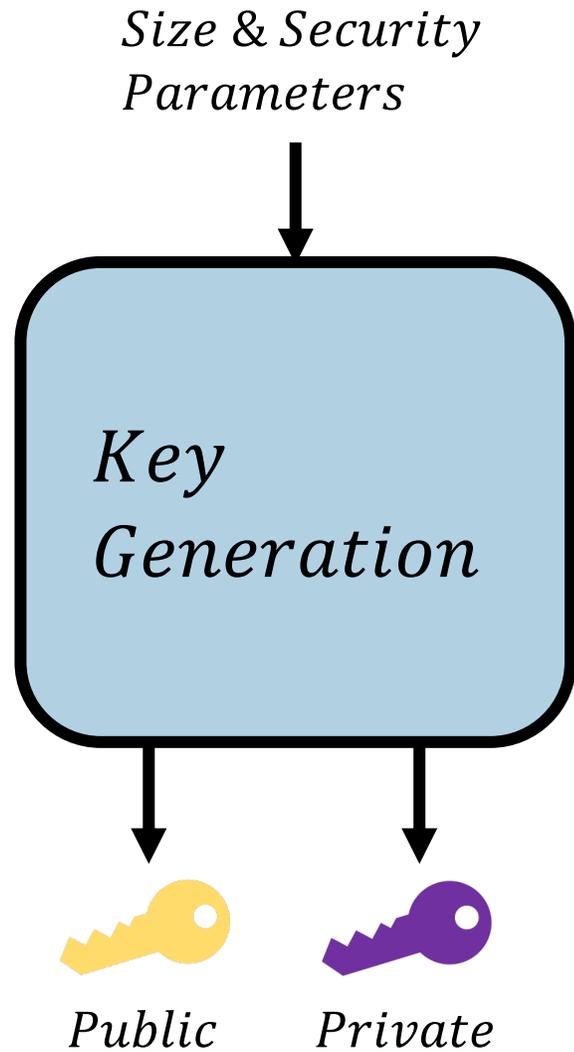
A diagram illustrating the addition of two locked variables. On the left, there are two yellow rounded rectangles, each with a yellow padlock icon on its top-left corner. The first rectangle contains the text d_1 and the second contains d_2 . A plus sign (+) is positioned between them. To the right of the plus sign is an equals sign (=). Further right is a single, larger yellow rounded rectangle with a yellow padlock icon on its top-left corner, containing the text $d_1 + d_2$.

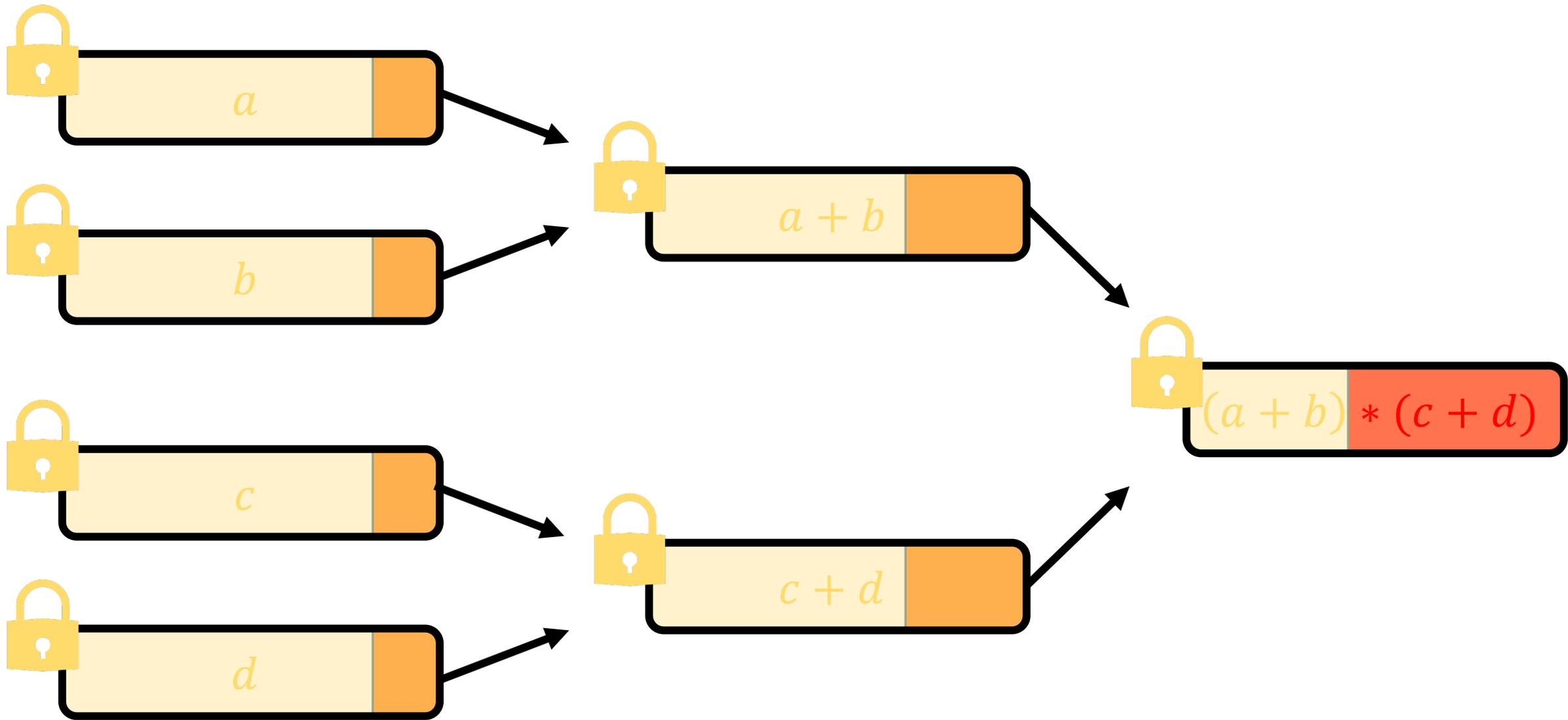
$$\text{locked } d_1 + \text{locked } d_2 = \text{locked } (d_1 + d_2)$$

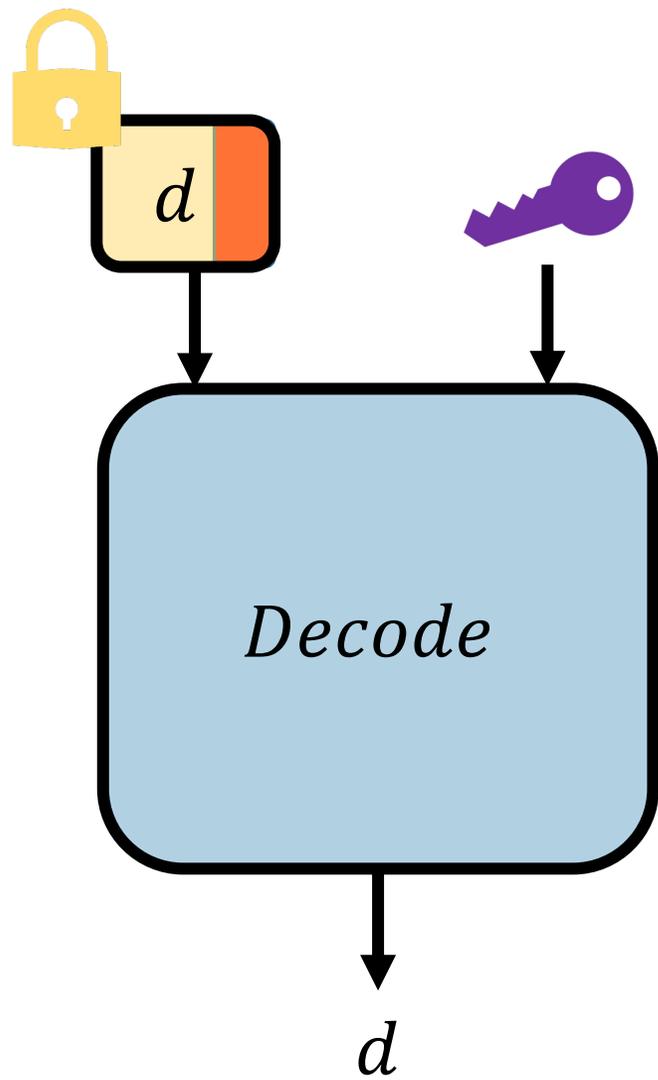
A diagram illustrating the multiplication of two locked variables. On the left, there are two yellow rounded rectangles, each with a yellow padlock icon on its top-left corner. The first rectangle contains the text d_1 and the second contains d_2 . A multiplication dot (\cdot) is positioned between them. To the right of the dot is an equals sign (=). Further right is a single, larger yellow rounded rectangle with a yellow padlock icon on its top-left corner, containing the text $d_1 \cdot d_2$.

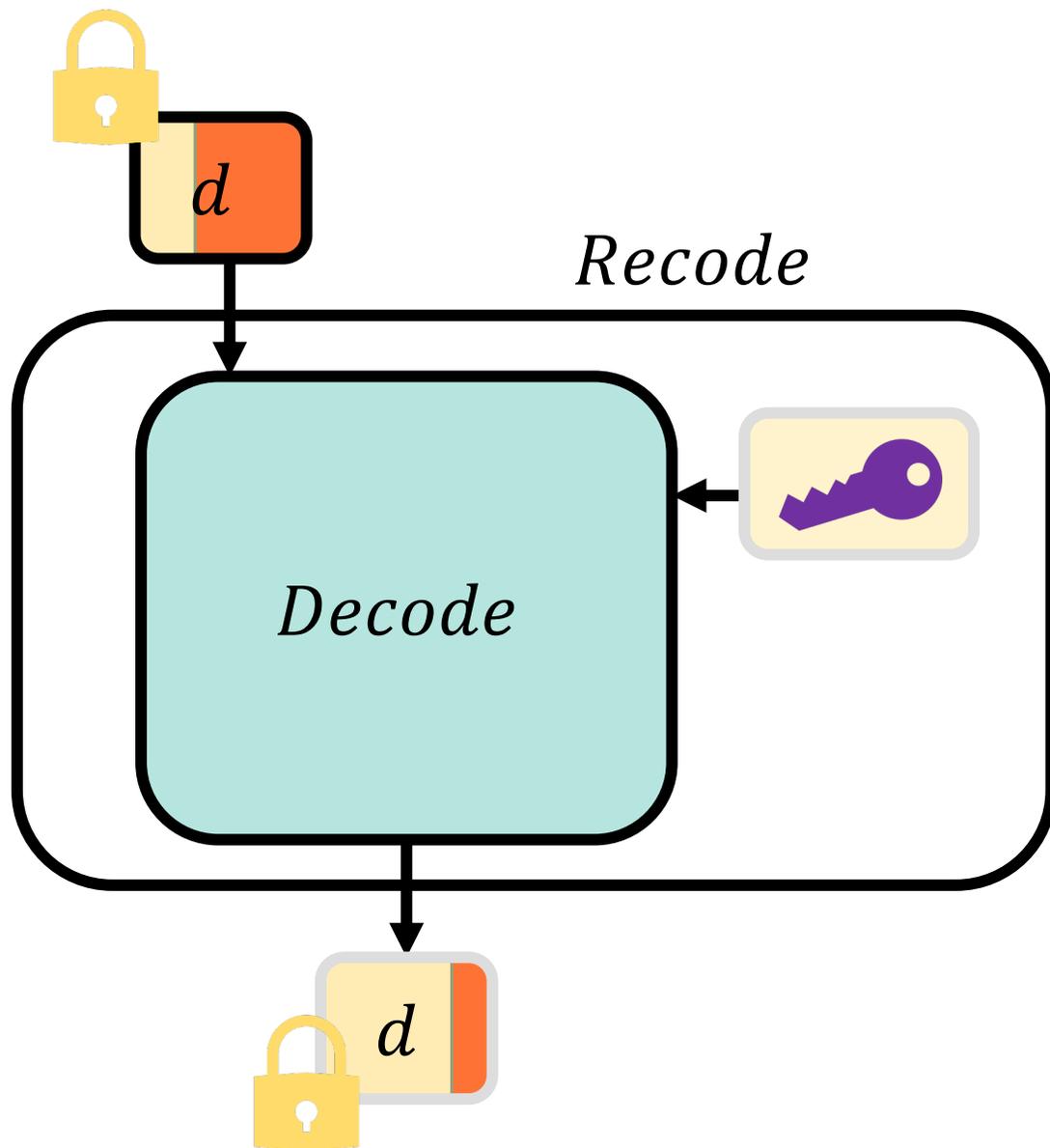
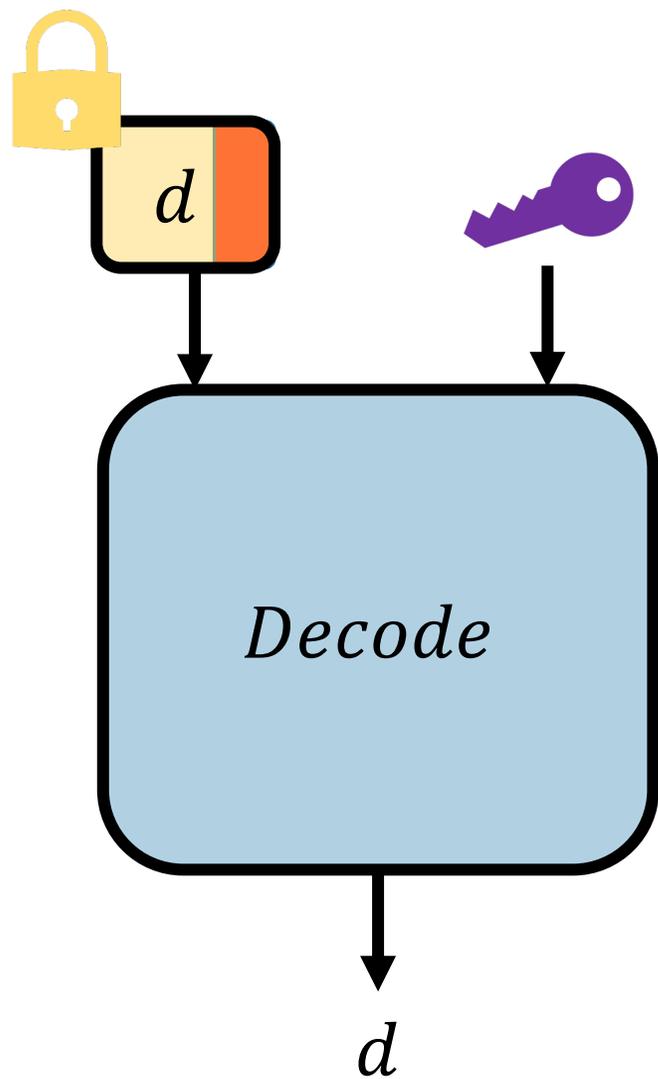
$$\text{locked } d_1 \cdot \text{locked } d_2 = \text{locked } (d_1 \cdot d_2)$$

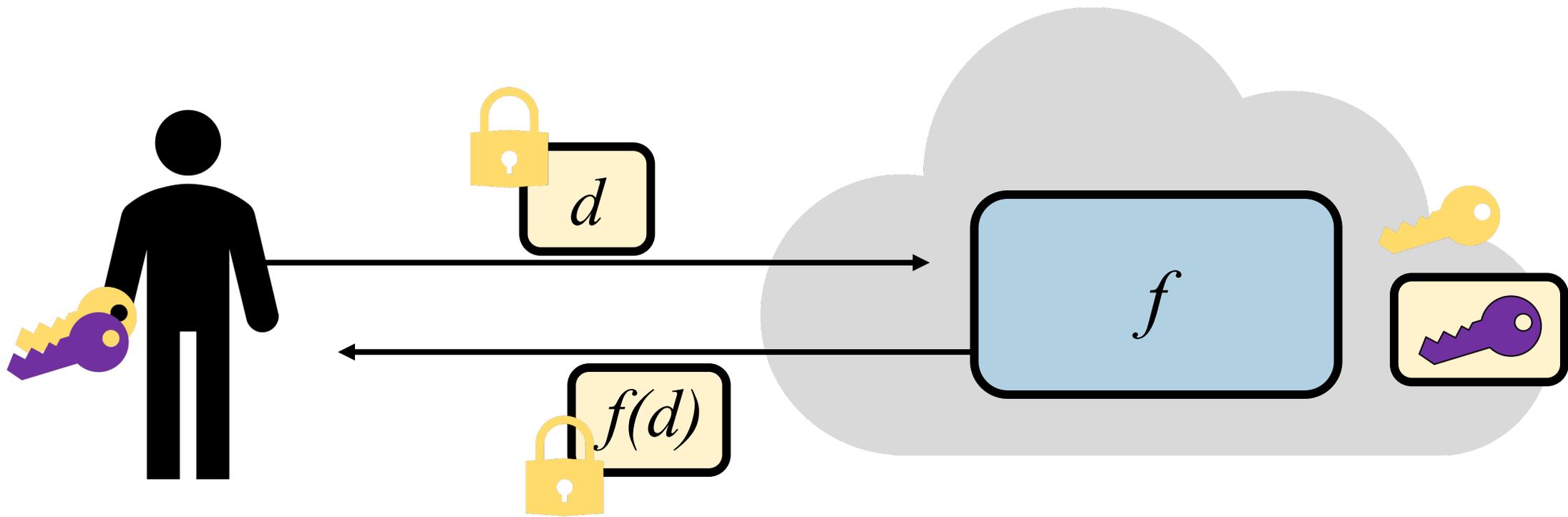
THE SCHEME

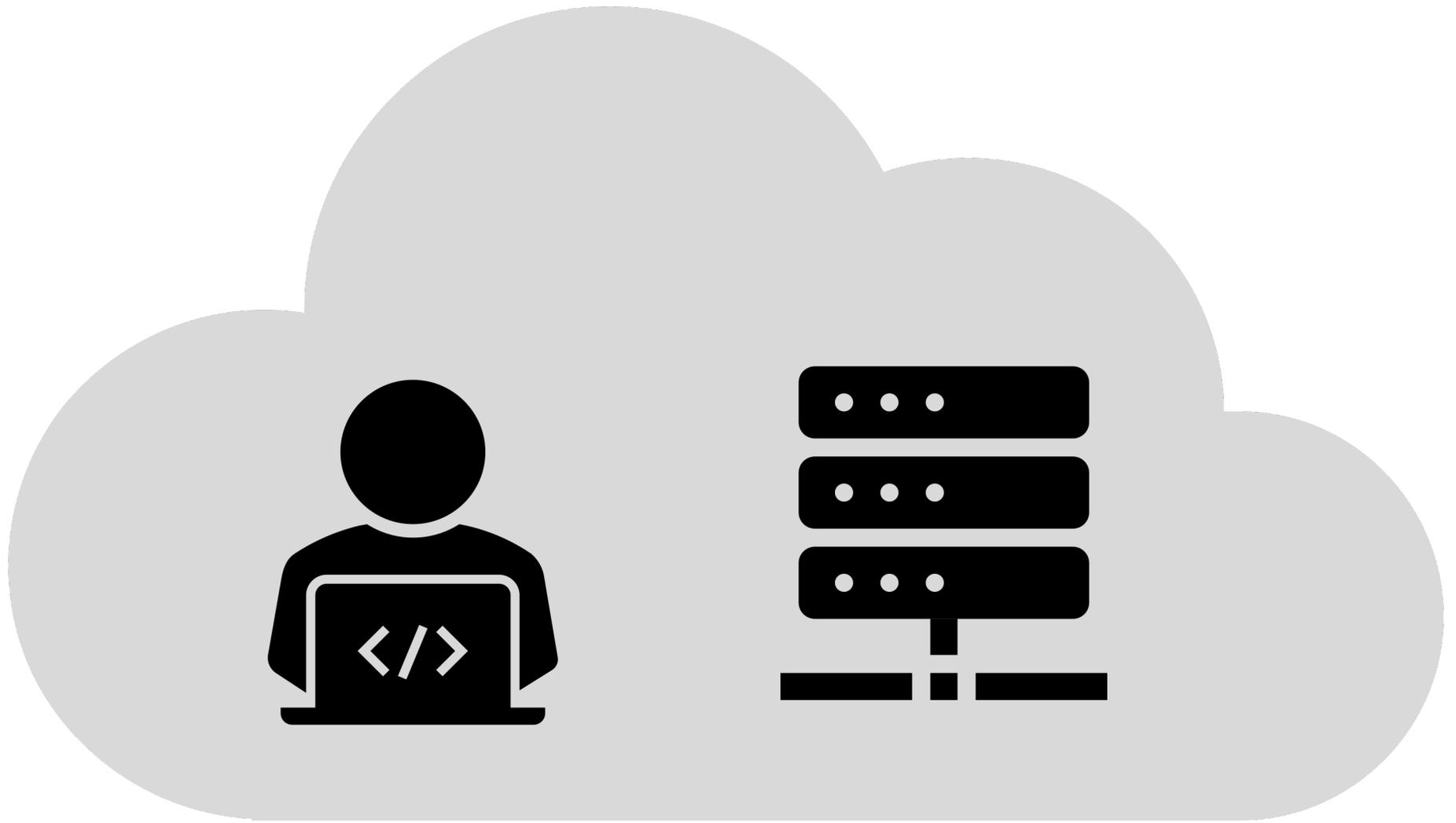




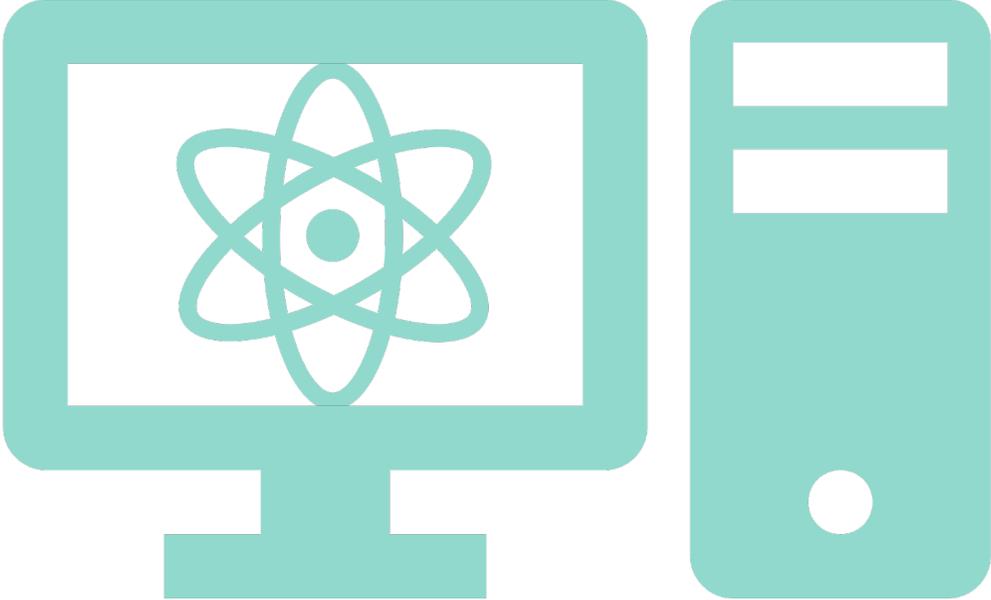




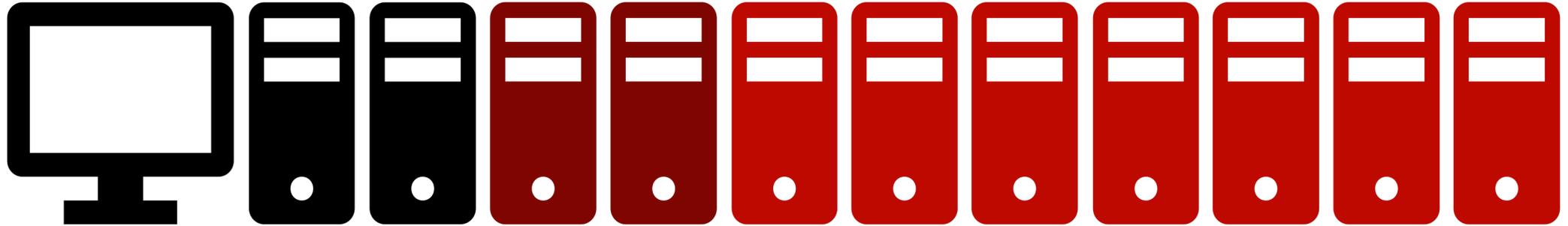








PROBLEMS



THEORY SOLUTION: BATCHING



× **+**

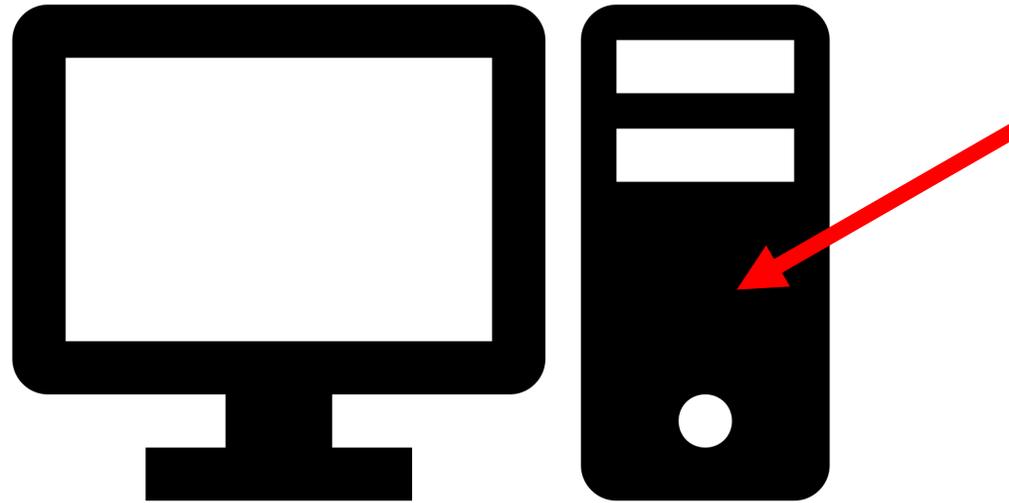
0 1 1 0 1 0 1 0

0 1 1 1 0 1 1 1

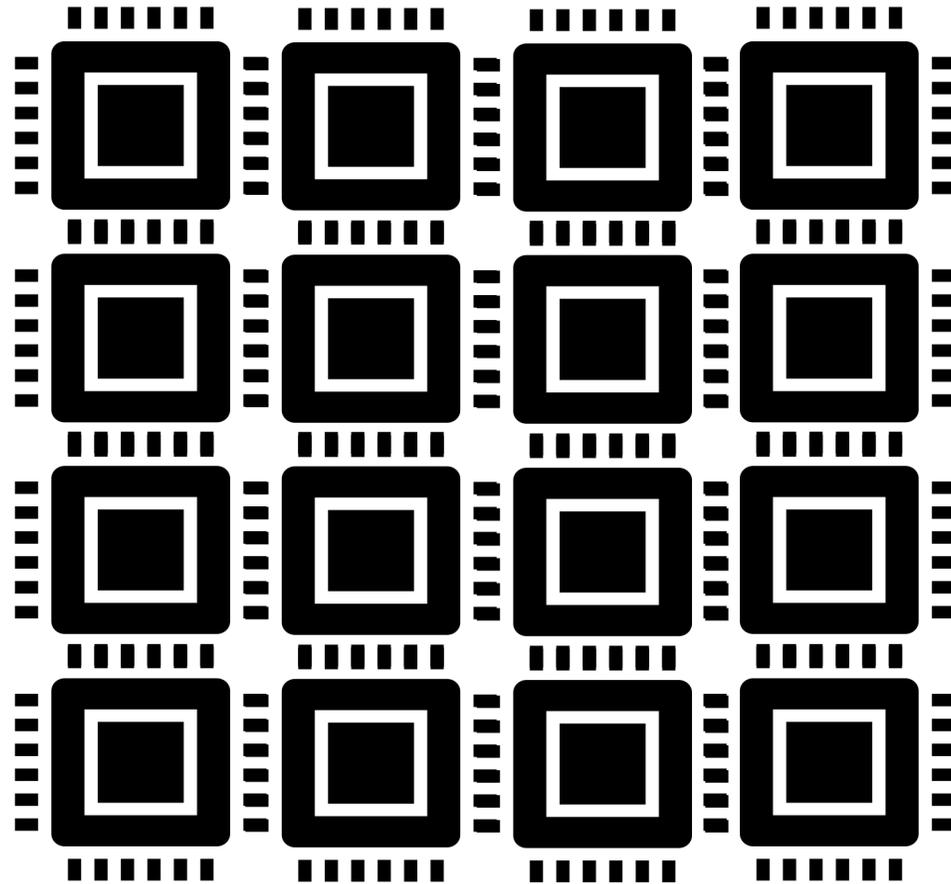


0 0 0 1 1 1 0 1

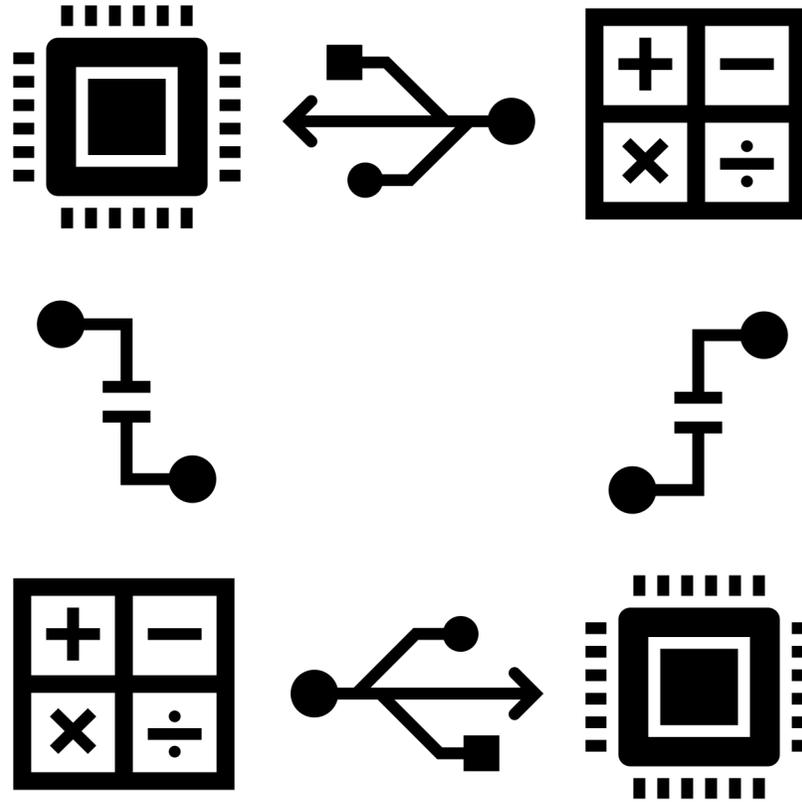
IMPLEMENTATION SOLUTION: CPU



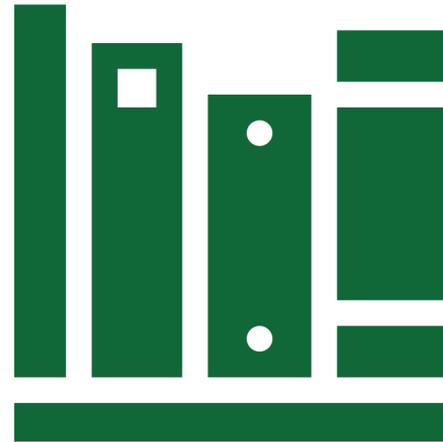
IMPLEMENTATION SOLUTION: GPU



IMPLEMENTATION SOLUTION: FPGA



MY RESEARCH



U.S. DEPARTMENT OF
ENERGY

Office of
Science