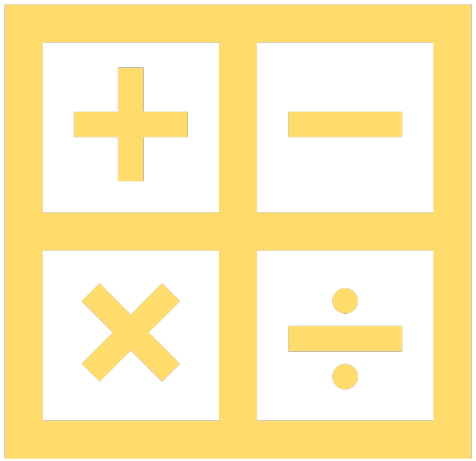
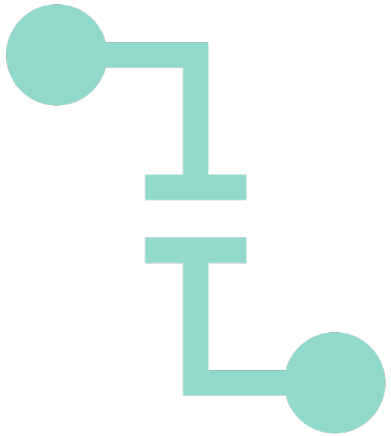
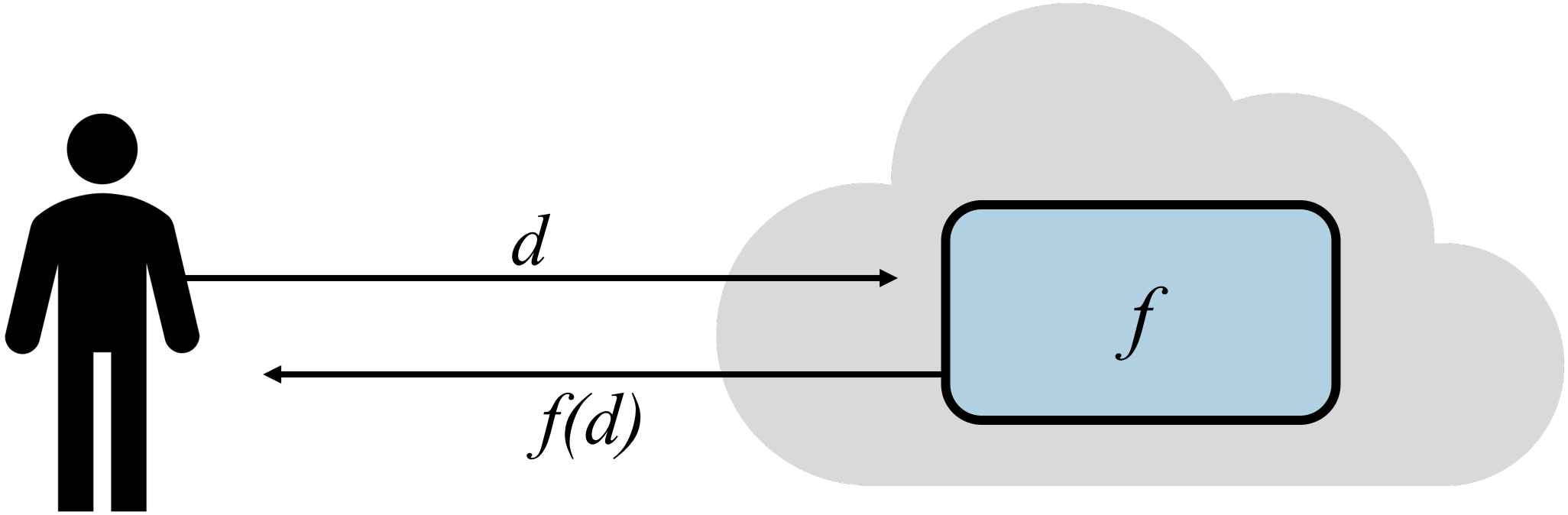
PARALLELIZATION OF FULLY HOMOMORPHIC DATA ENCODING

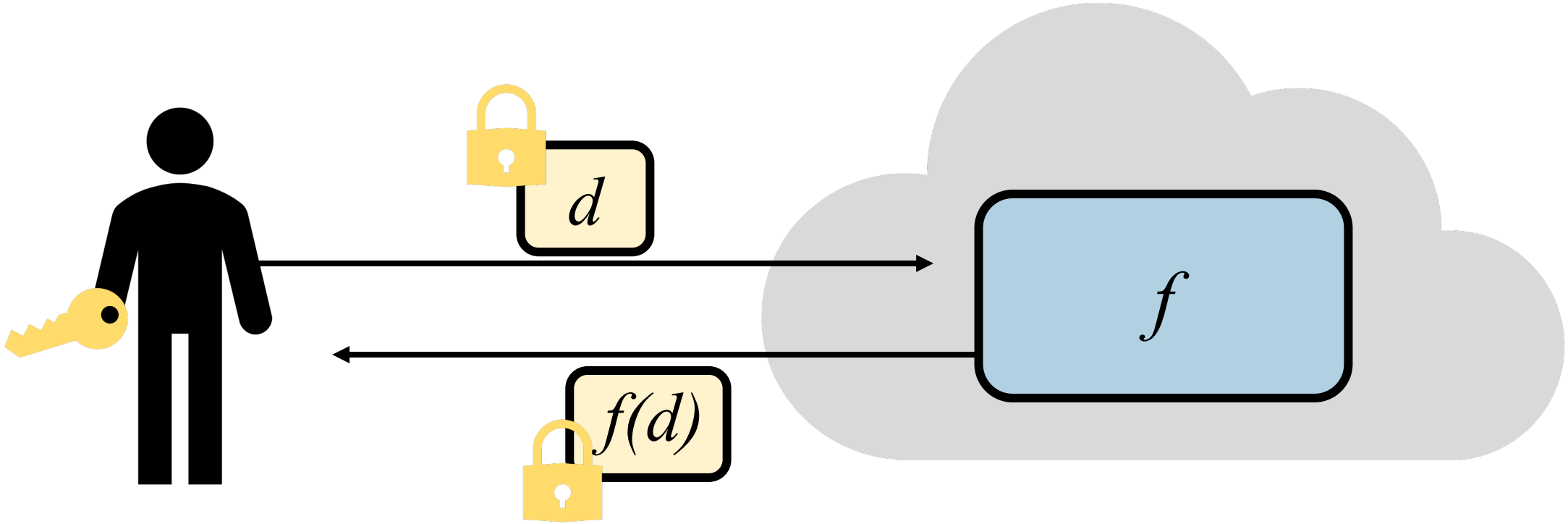
JESS WOODS

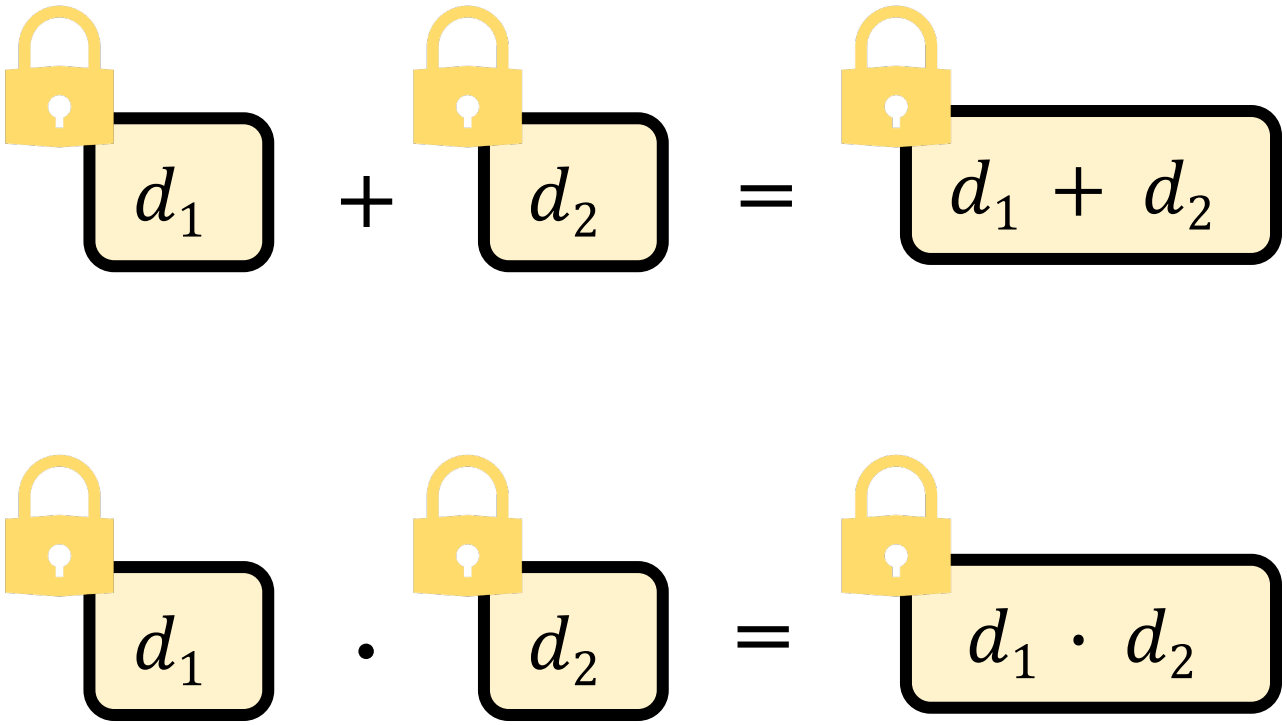
COMPUTER SCIENCE RESEARCH



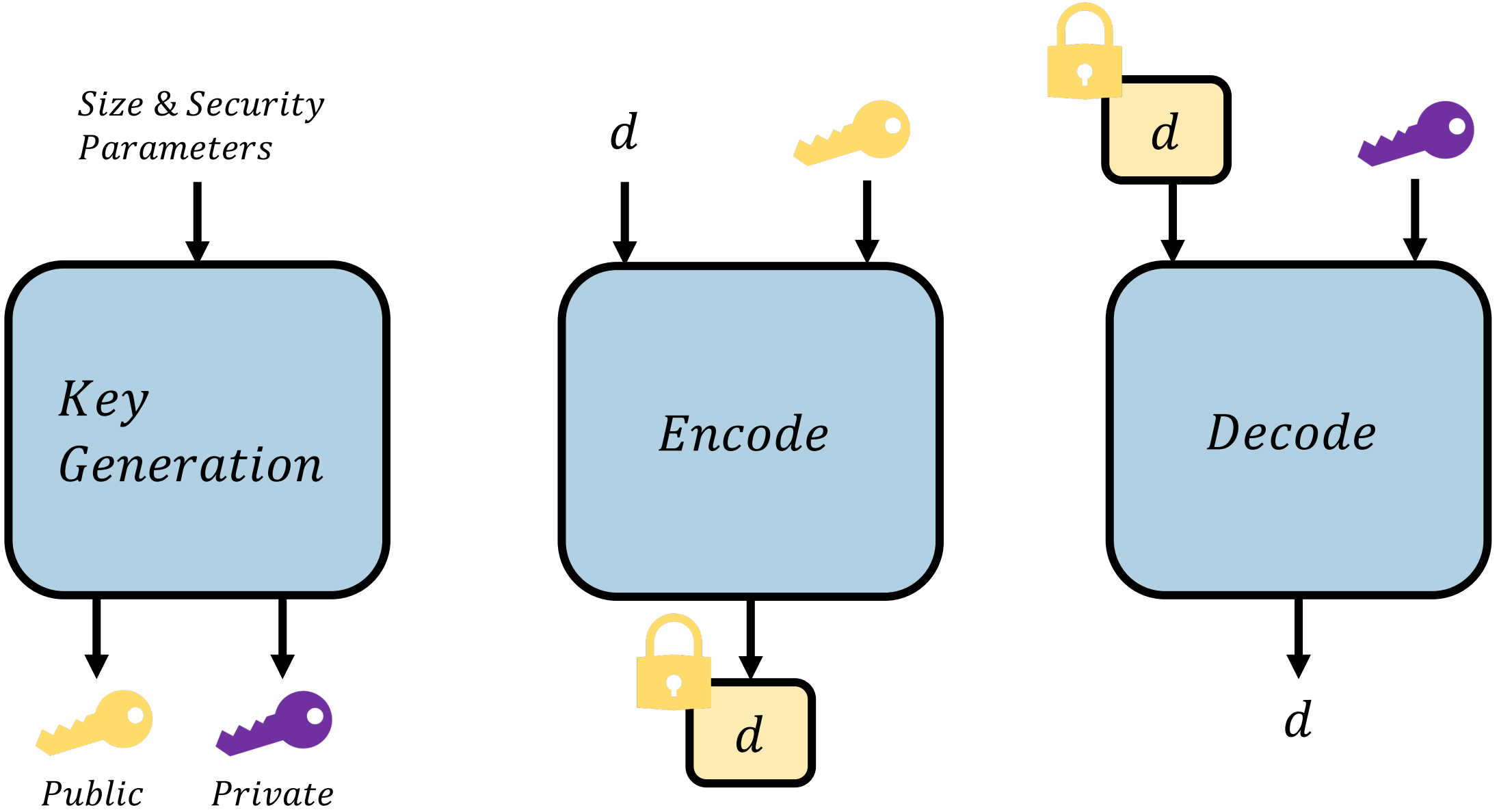


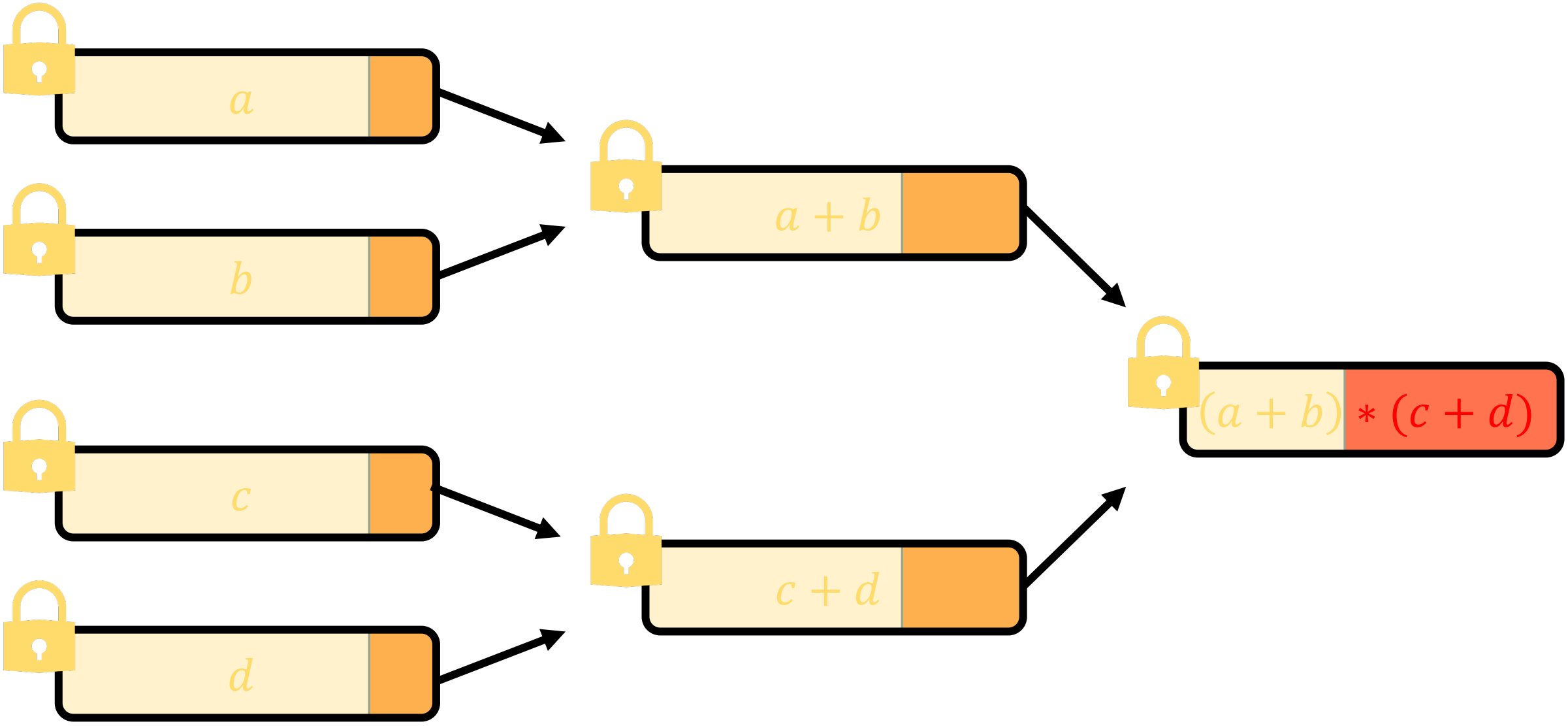

d
f
f(d)

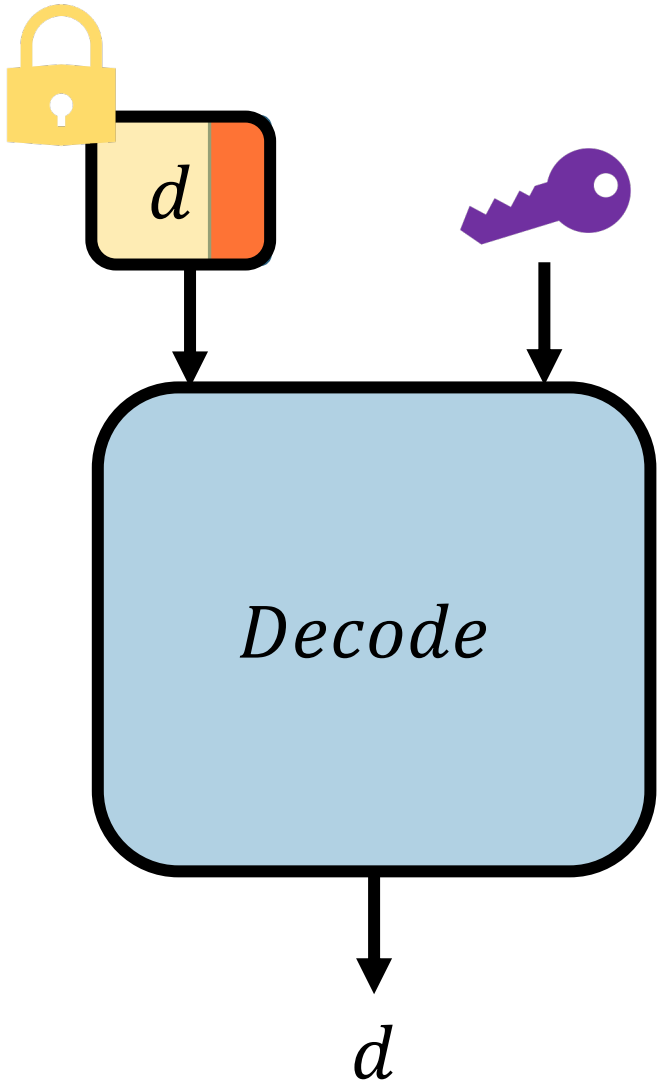

d
f
f(d)

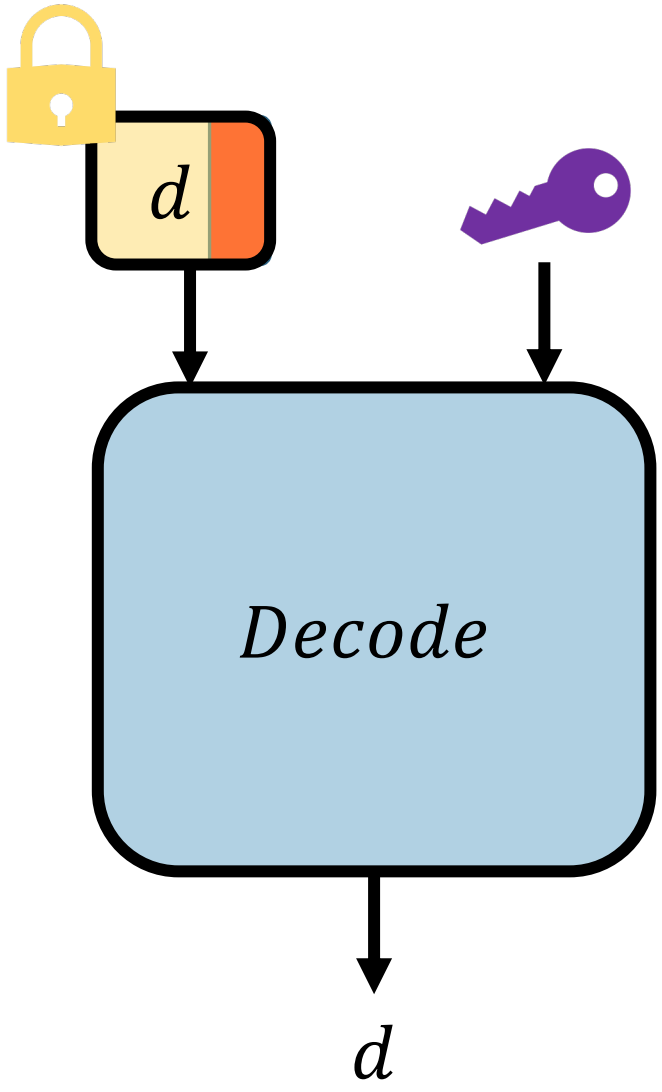

d_1
+
d_2
=
$d_1 + d_2$
d_1
·
d_2
=
$d_1 \cdot d_2$

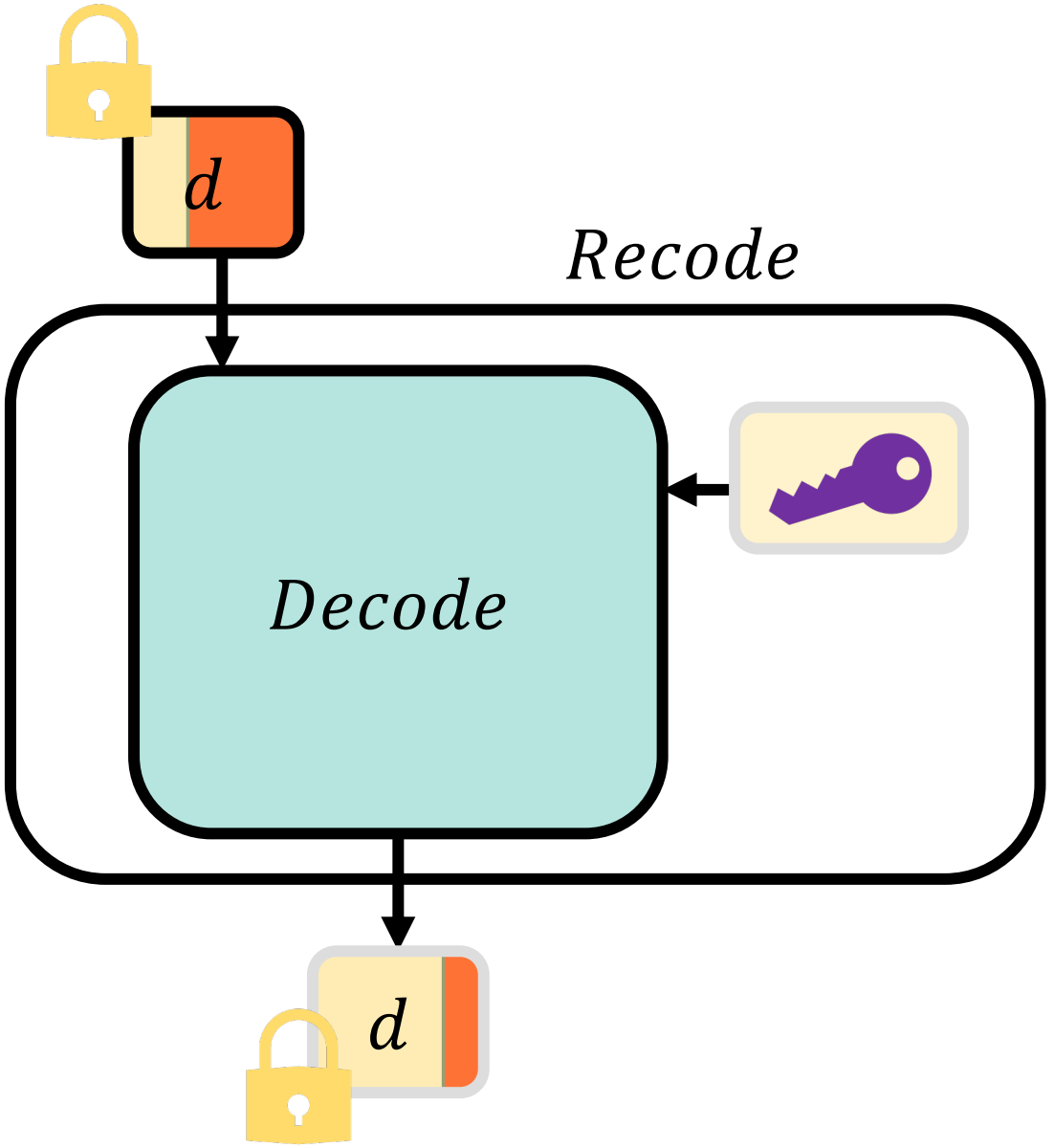
THE SCHEME

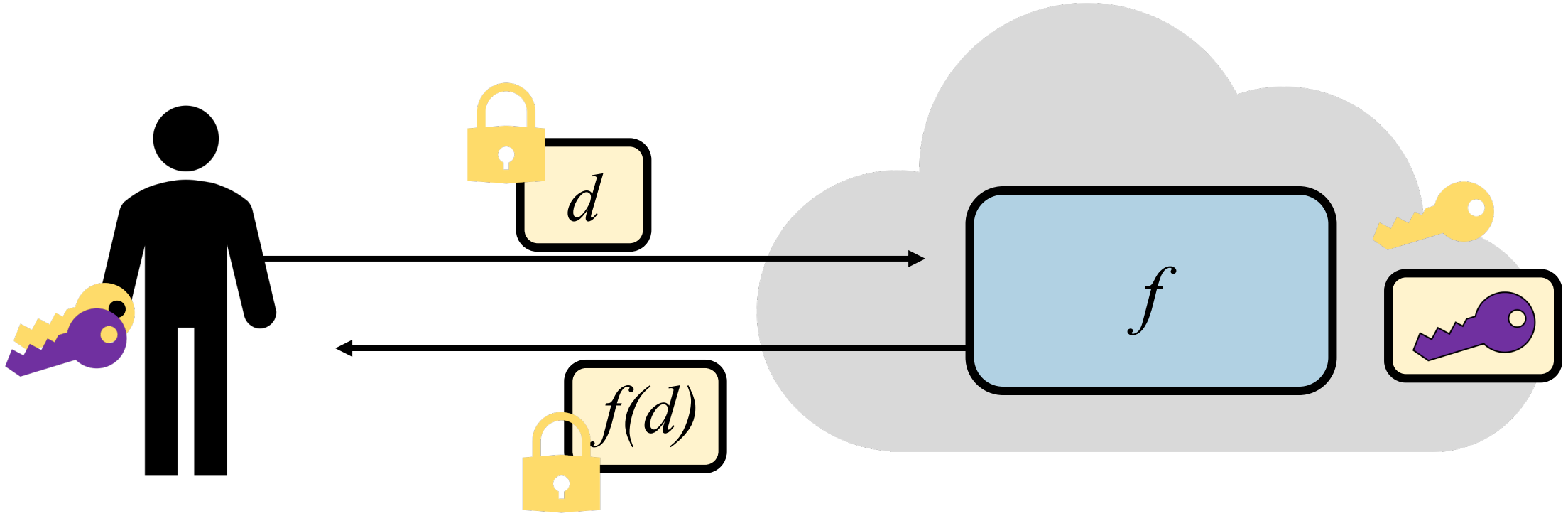

Size & Security Parameters
Key Generation
Public
Private
d
Encode
d
d
Decode
d

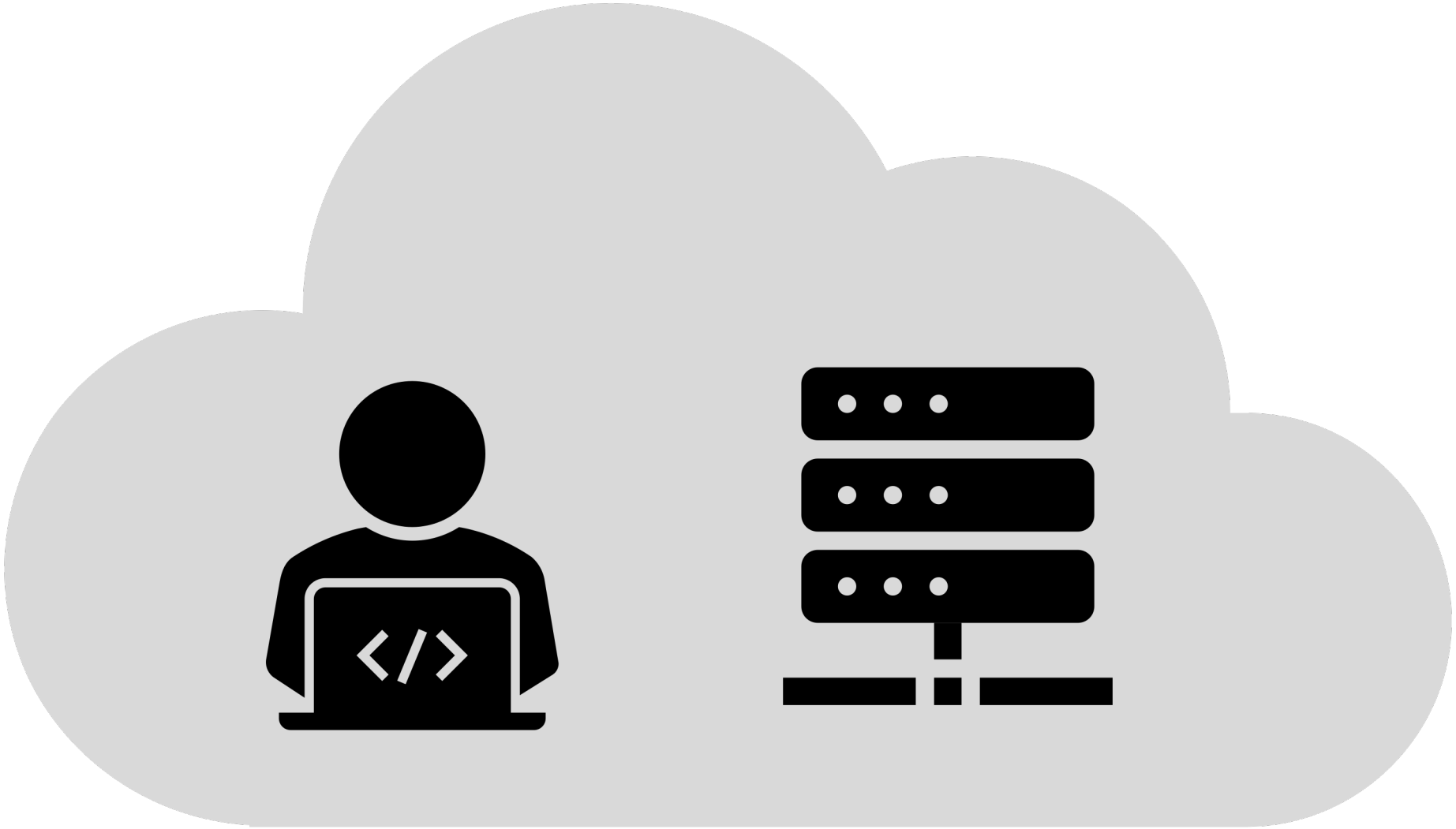

a
b
c
d
a + b
c + d
(a + b) * (c + d)

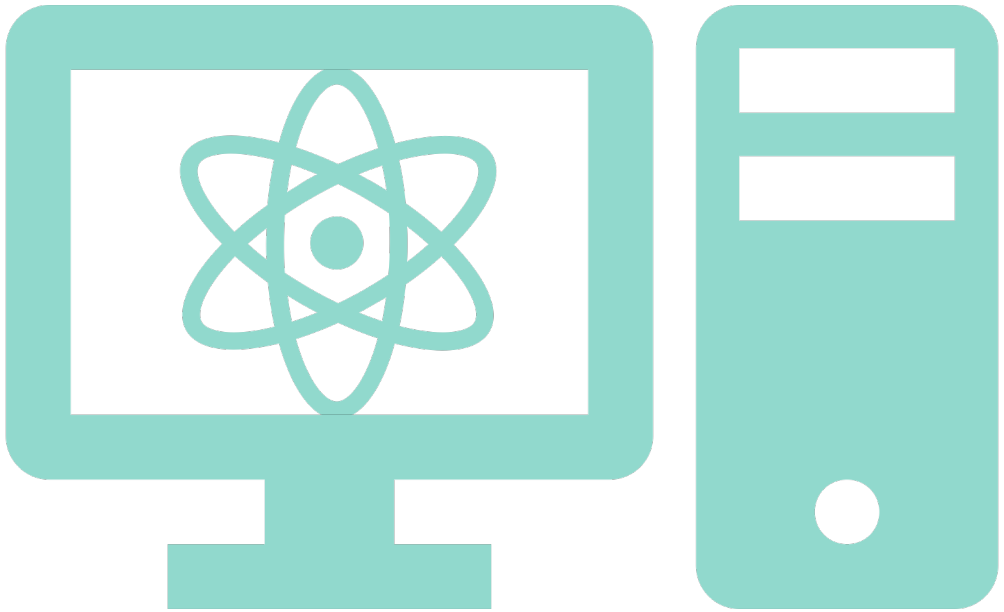

d
Decode
d


d
Decode
d

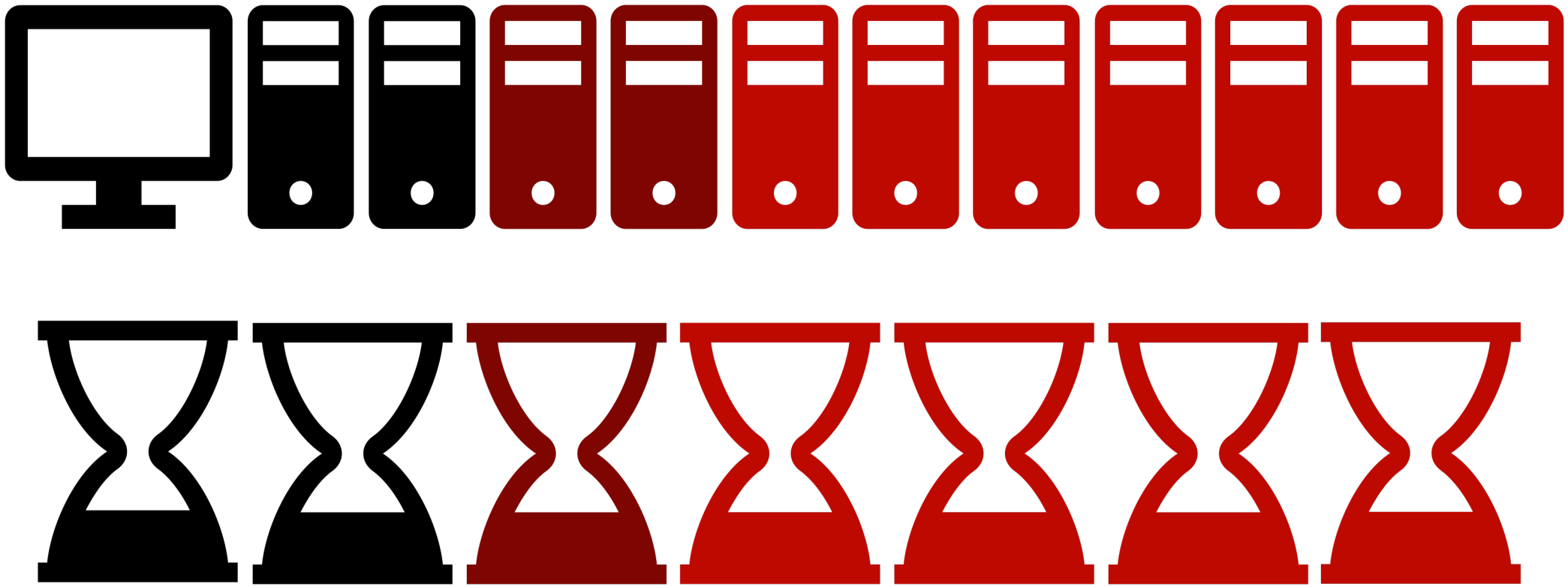

d
Recode
Decode
d


d
f
f(d)

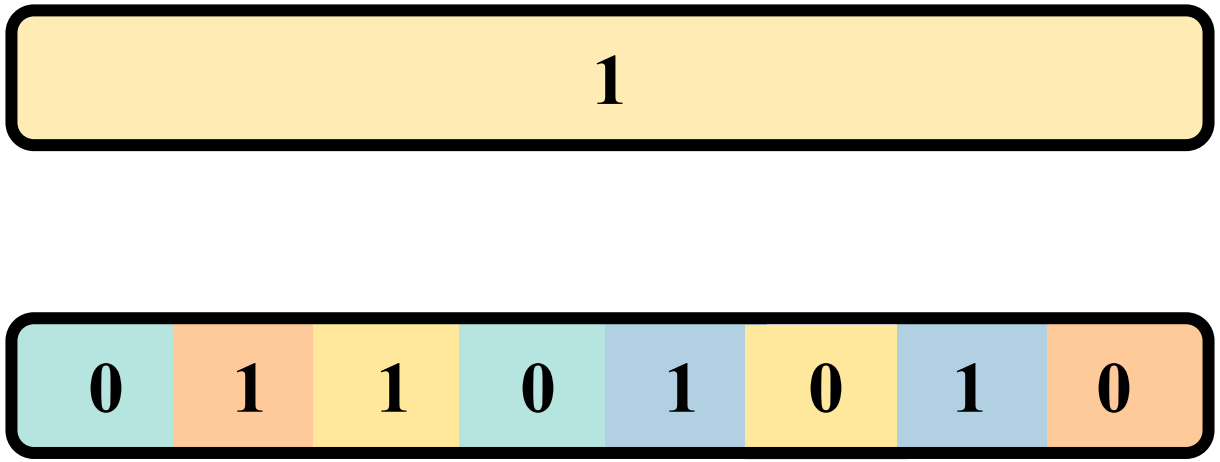


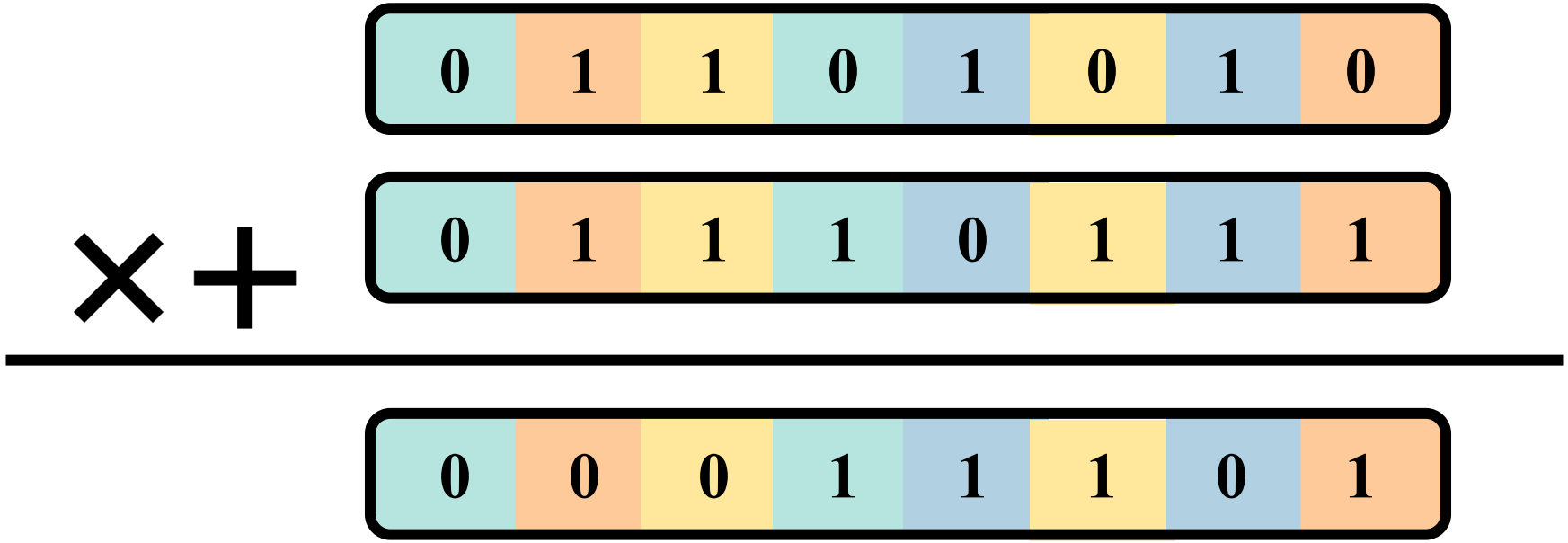


PROBLEMS

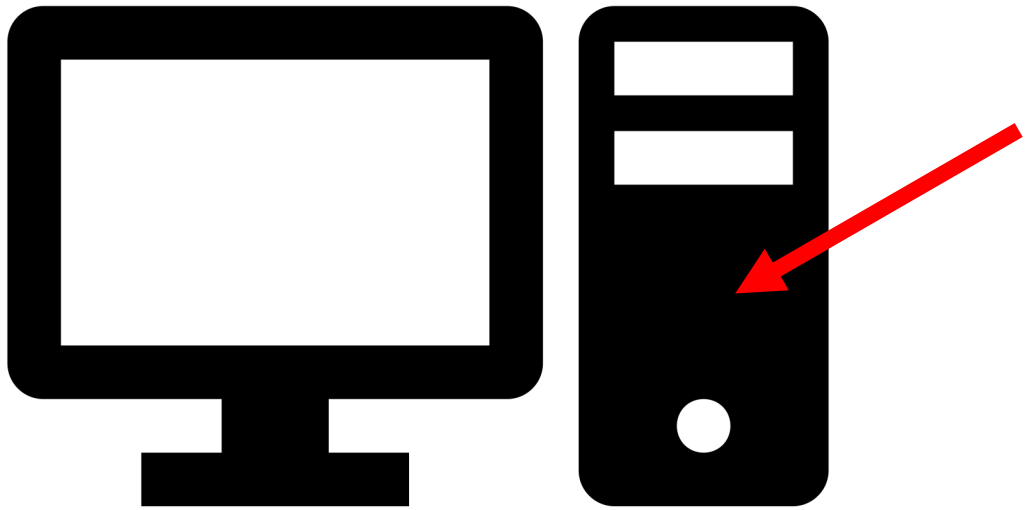


THEORY SOLUTION: BATCHING

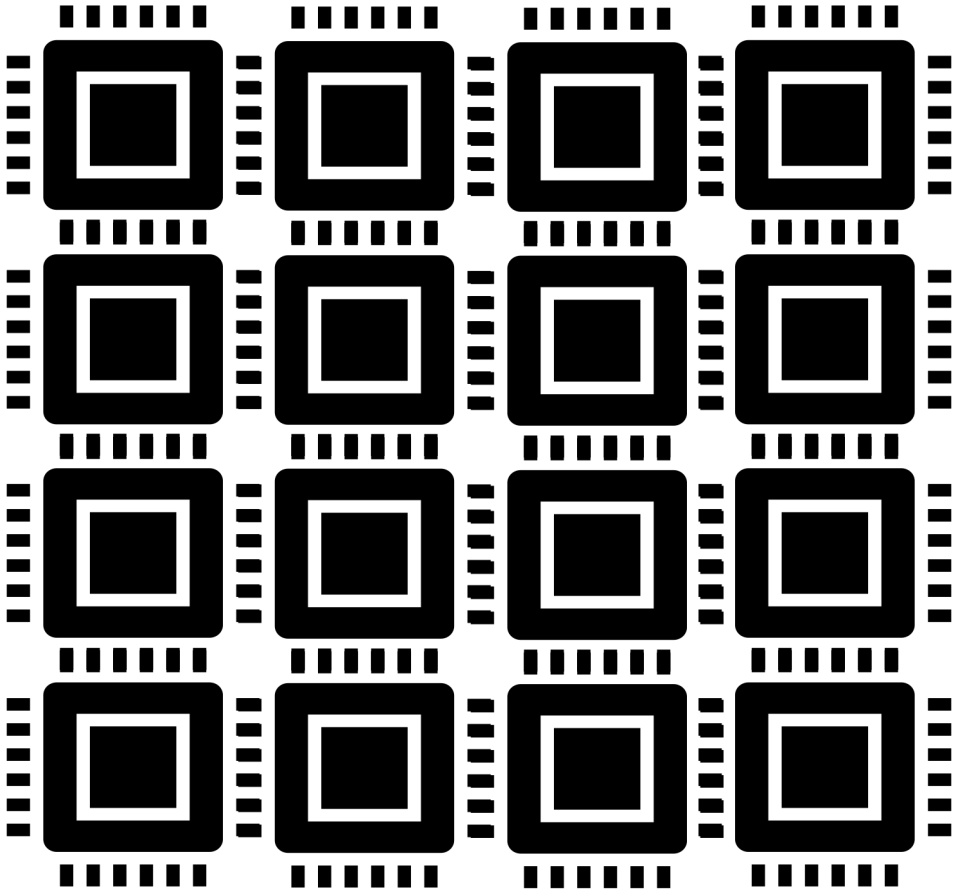



0 1 1 0 1 0 1 0
0 1 1 1 0 1 1 1
× +
0 0 0 1 1 1 0 1

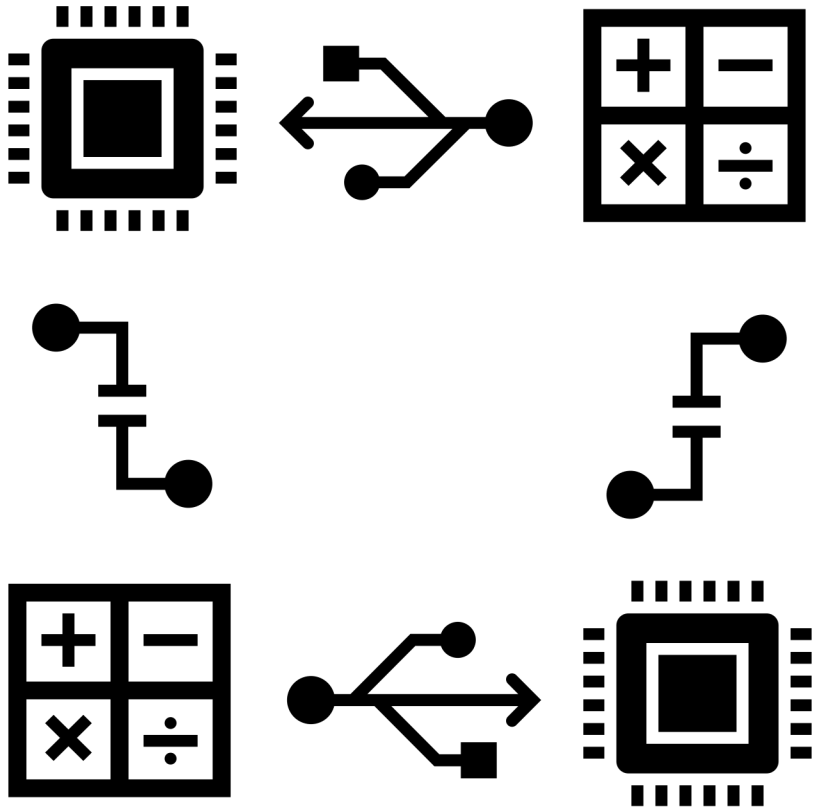
IMPLEMENTATION SOLUTION: CPU



IMPLEMENTATION SOLUTION: GPU



IMPLEMENTATION SOLUTION: FPGA



MY RESEARCH

U.S. DEPARTMENT OF ENERGY | Office of Science