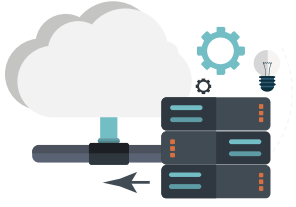
User : x, $Enc(\ )$, $Dec(\ )$, $f(\ )$

Server : Eval, $f(\ )$

② User encrypts his message x, $Enc(x)$

③ User sends $Enc(x)$ to store

⑥ Server returns $Enc(f(x))$

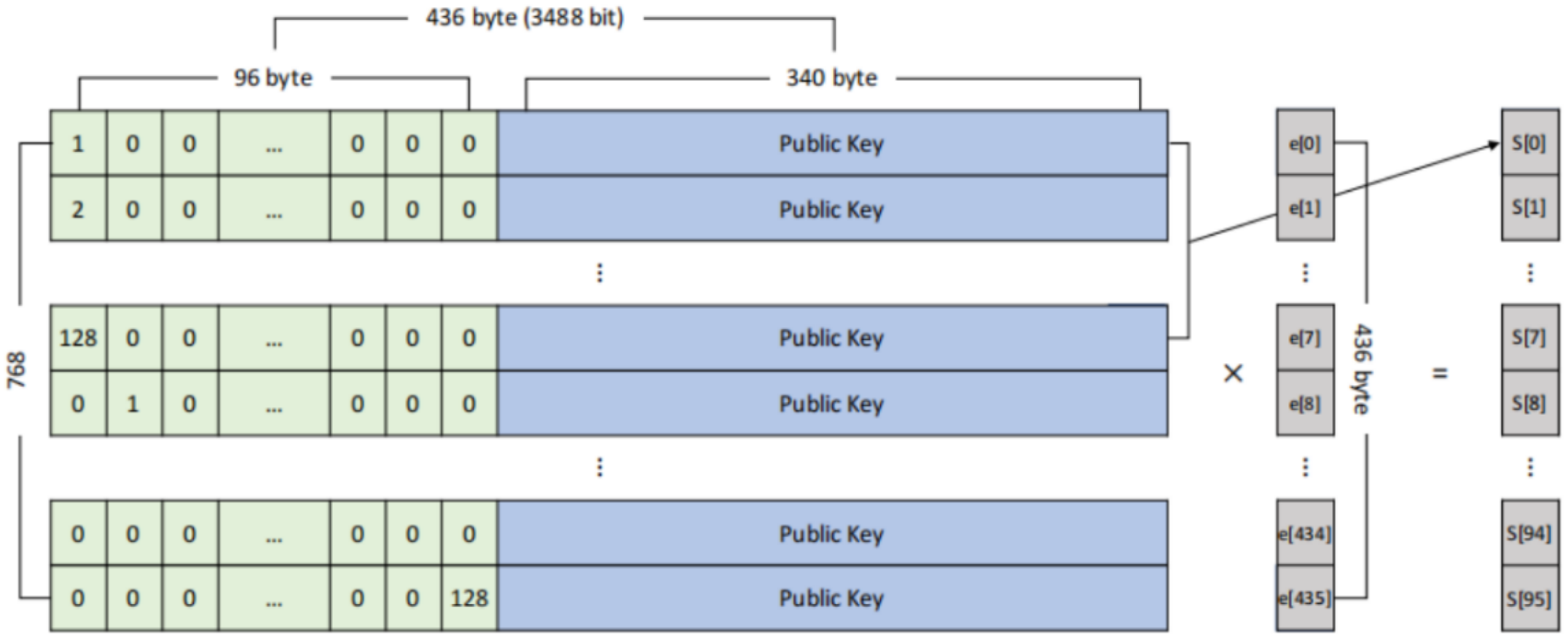


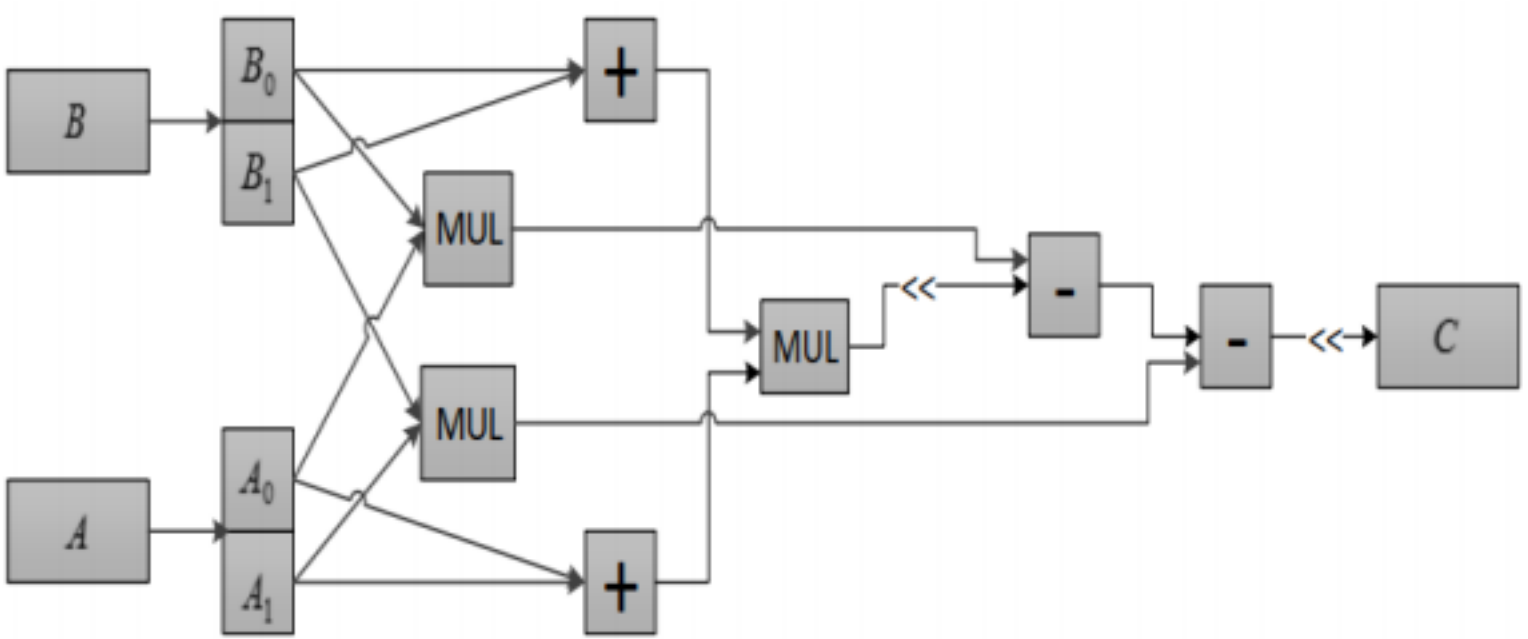
④ Server received the request $f(\ )$

① User : input x , Need $f(x)$

⑤ Server evalutes $f(\ )$ homomophically

⑦ User computes $Dec(Enc(f(x))) = f(x)$, and gets $f(x)$


436 byte (3488 bit)
96 byte
340 byte
768
1 0 0 ... 0 0 0
Public Key
2 0 0 ... 0 0 0
Public Key
128 0 0 ... 0 0 0
Public Key
0 1 0 ... 0 0 0
Public Key
0 0 0 ... 0 0 0
Public Key
0 0 0 ... 0 0 128
Public Key
e[0]
e[1]
e[7]
e[8]
e[434]
e[435]
436 byte
S[0]
S[1]
S[7]
S[8]
S[94]
S[95]


B
A
B_0
B_1
A_0
A_1
+
+
MUL
MUL
MUL
-
-
<<
<<
C