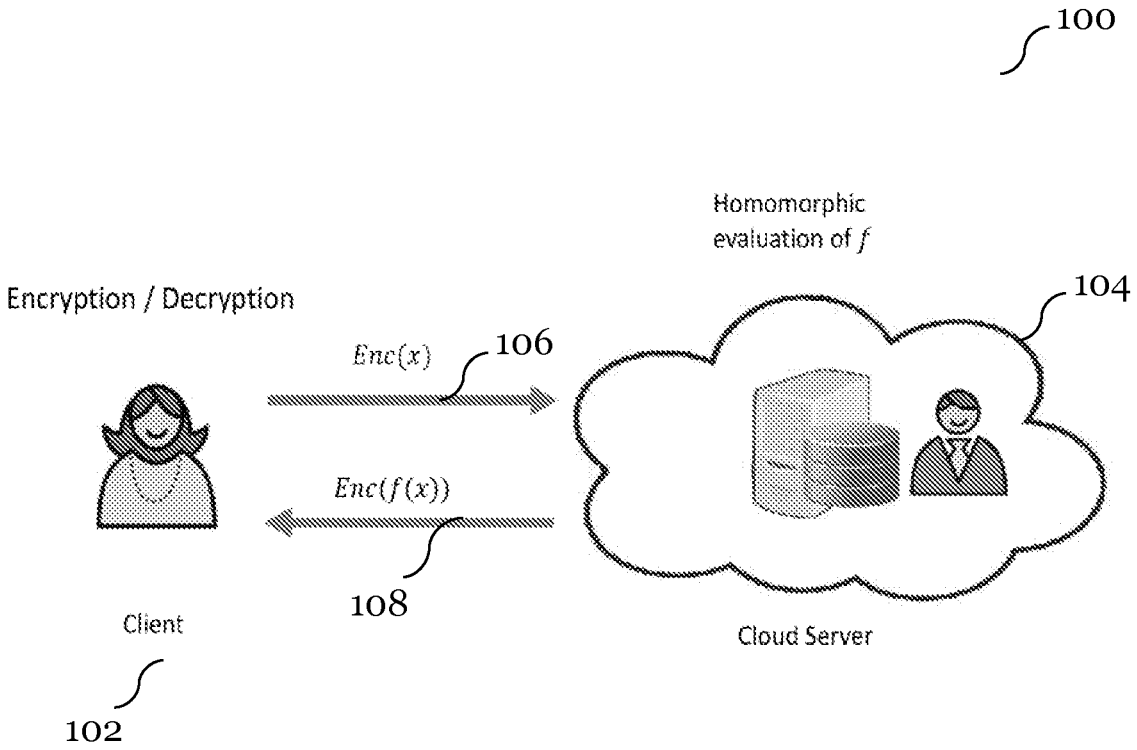

100
Homomorphic
evaluation of f
Encryption / Decryption
104
Enc(x)
106
Enc(f(x))
108
Client
102
Cloud Server

Figure 1

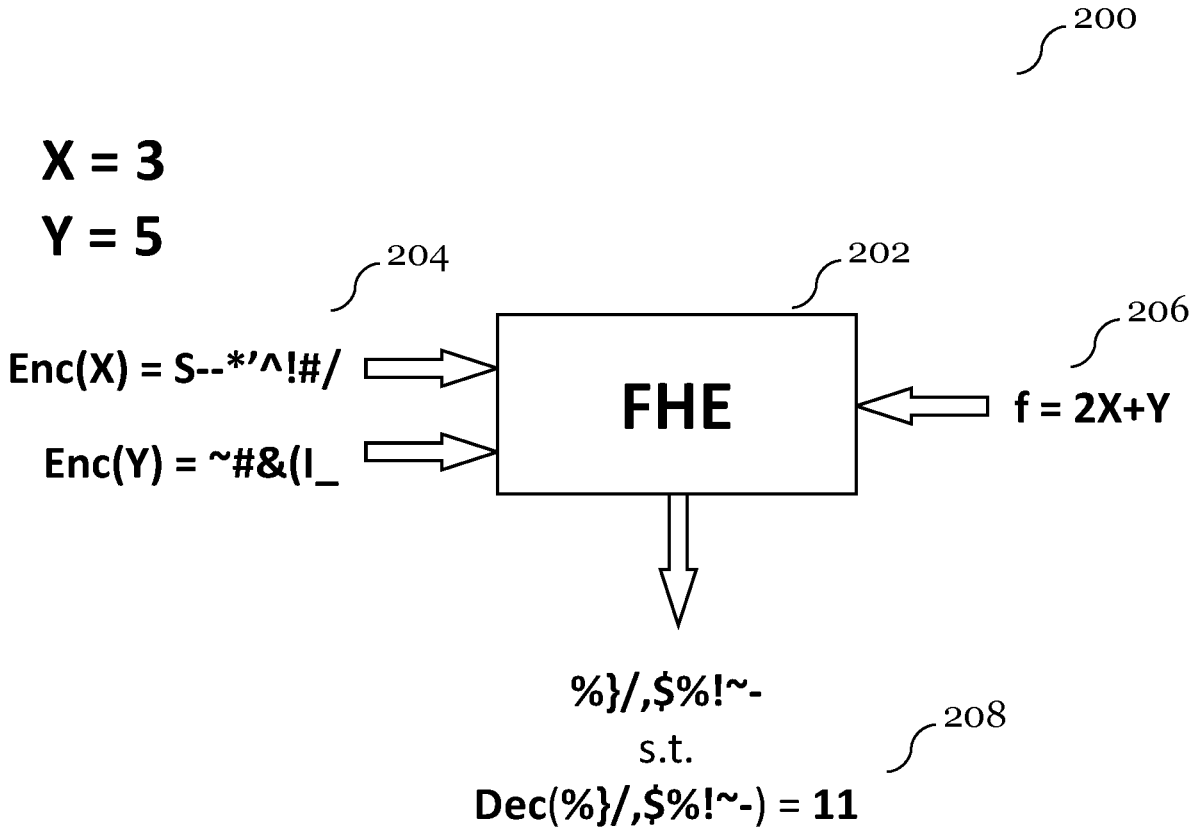


Figure 2

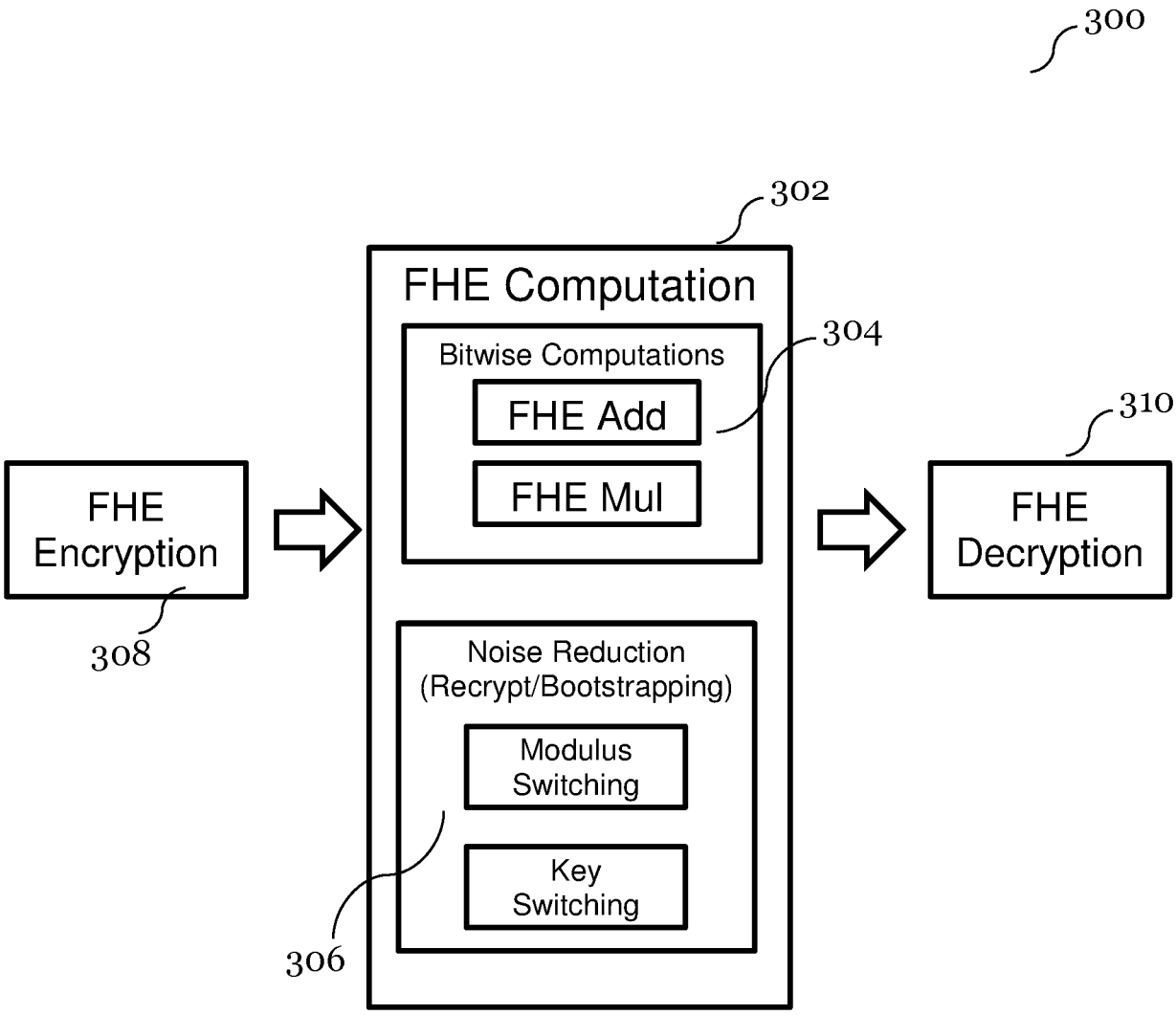

300
302
FHE Computation
Bitwise Computations
304
FHE Add
FHE Mul
310
FHE Encryption
FHE Decryption
308
Noise Reduction
(Recrypt/Bootstrapping)
Modulus Switching
Key Switching
306

Figure 3

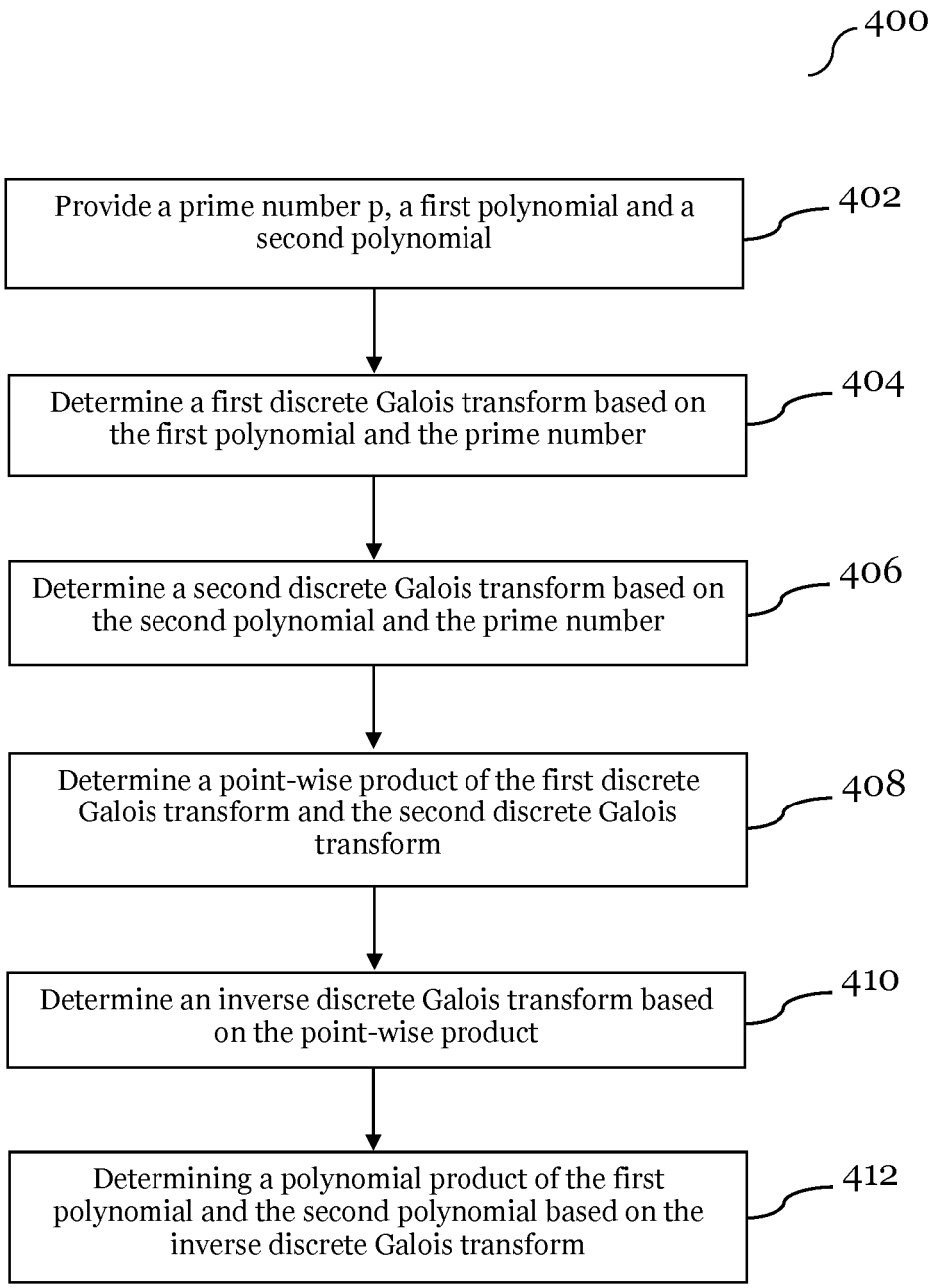

400
Provide a prime number p, a first polynomial and a second polynomial
402
Determine a first discrete Galois transform based on the first polynomial and the prime number
404
Determine a second discrete Galois transform based on the second polynomial and the prime number
406
Determine a point-wise product of the first discrete Galois transform and the second discrete Galois transform
408
Determine an inverse discrete Galois transform based on the point-wise product
410
Determining a polynomial product of the first polynomial and the second polynomial based on the inverse discrete Galois transform
412

Figure 4

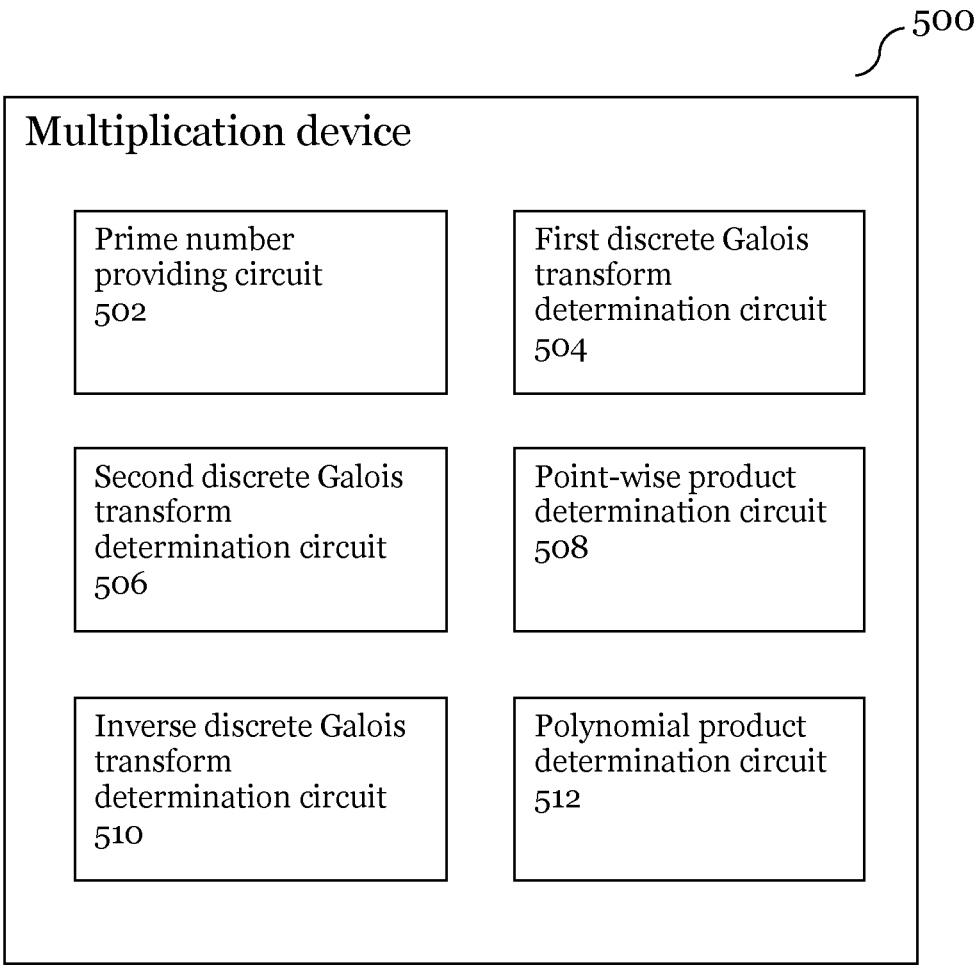

500
Multiplication device
Prime number providing circuit 502
First discrete Galois transform determination circuit 504
Second discrete Galois transform determination circuit 506
Point-wise product determination circuit 508
Inverse discrete Galois transform determination circuit 510
Polynomial product determination circuit 512

Figure 5