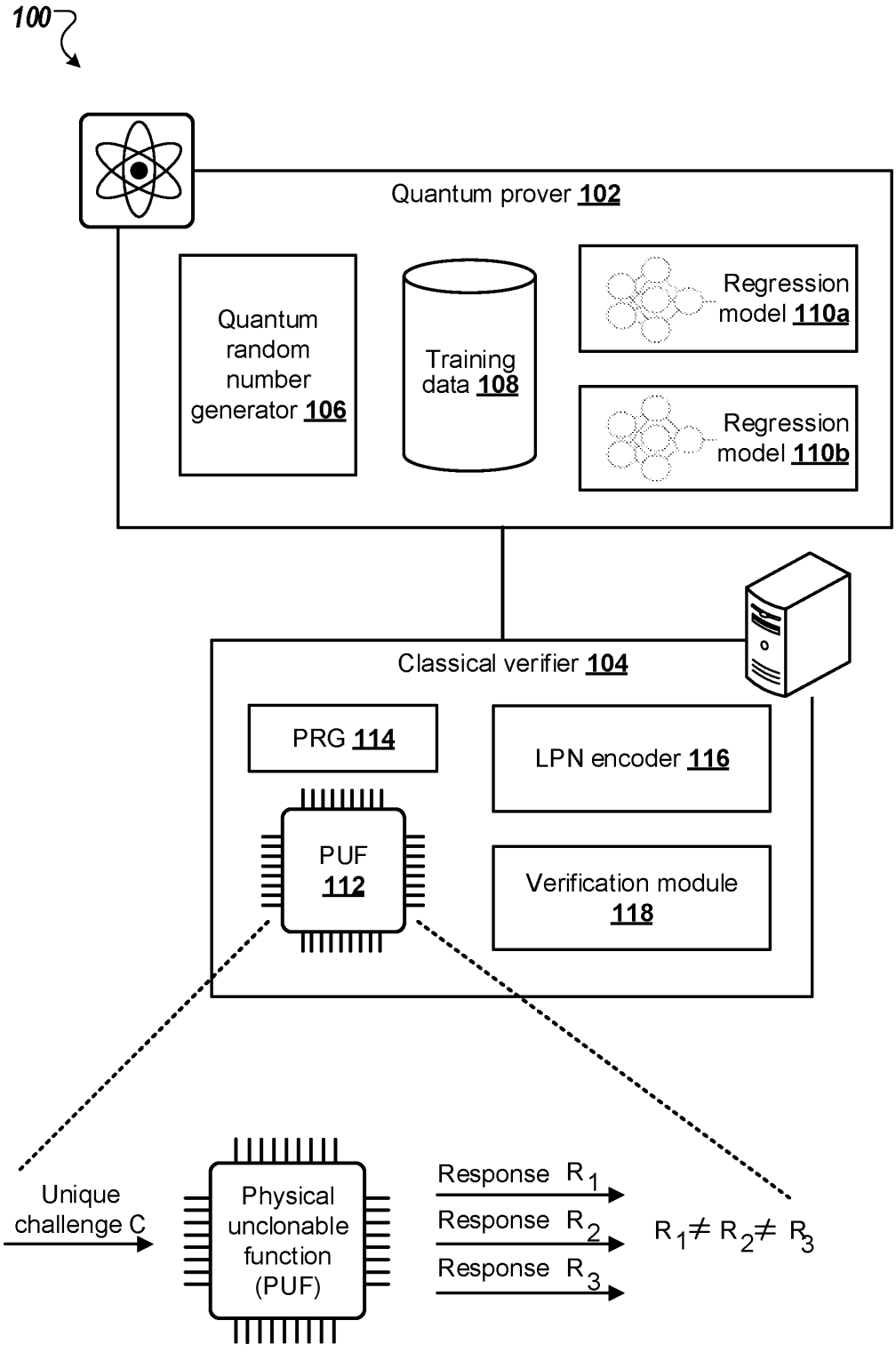
100
Quantum prover 102
Quantum random number generator 106
Training data 108
Regression model 110a
Regression model 110b
Classical verifier 104
PRG 114
LPN encoder 116
PUF 112
Verification module 118
Unique challenge C
Physical unclonable function (PUF)
Response R1
Response R2
Response R3
R1≠ R2≠ R3

FIG. 1

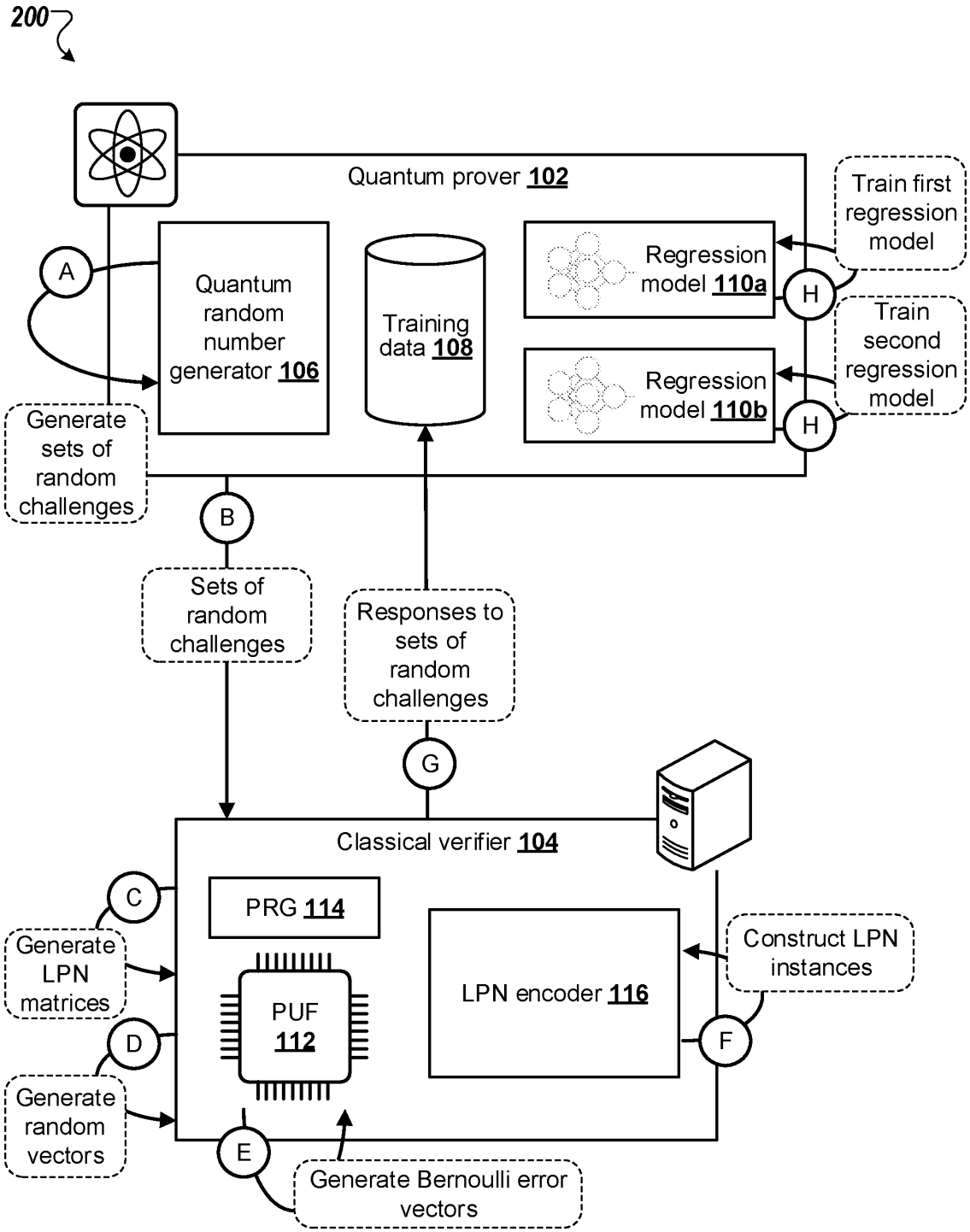
200
Quantum prover 102
Train first regression model
Quantum random number generator 106
Training data 108
Regression model 110a
Train second regression model
Regression model 110b
A
H
H
Generate sets of random challenges
B
Sets of random challenges
Responses to sets of random challenges
G
Classical verifier 104
C
PRG 114
Generate LPN matrices
PUF 112
LPN encoder 116
Construct LPN instances
D
F
Generate random vectors
E
Generate Bernoulli error vectors

FIG. 2

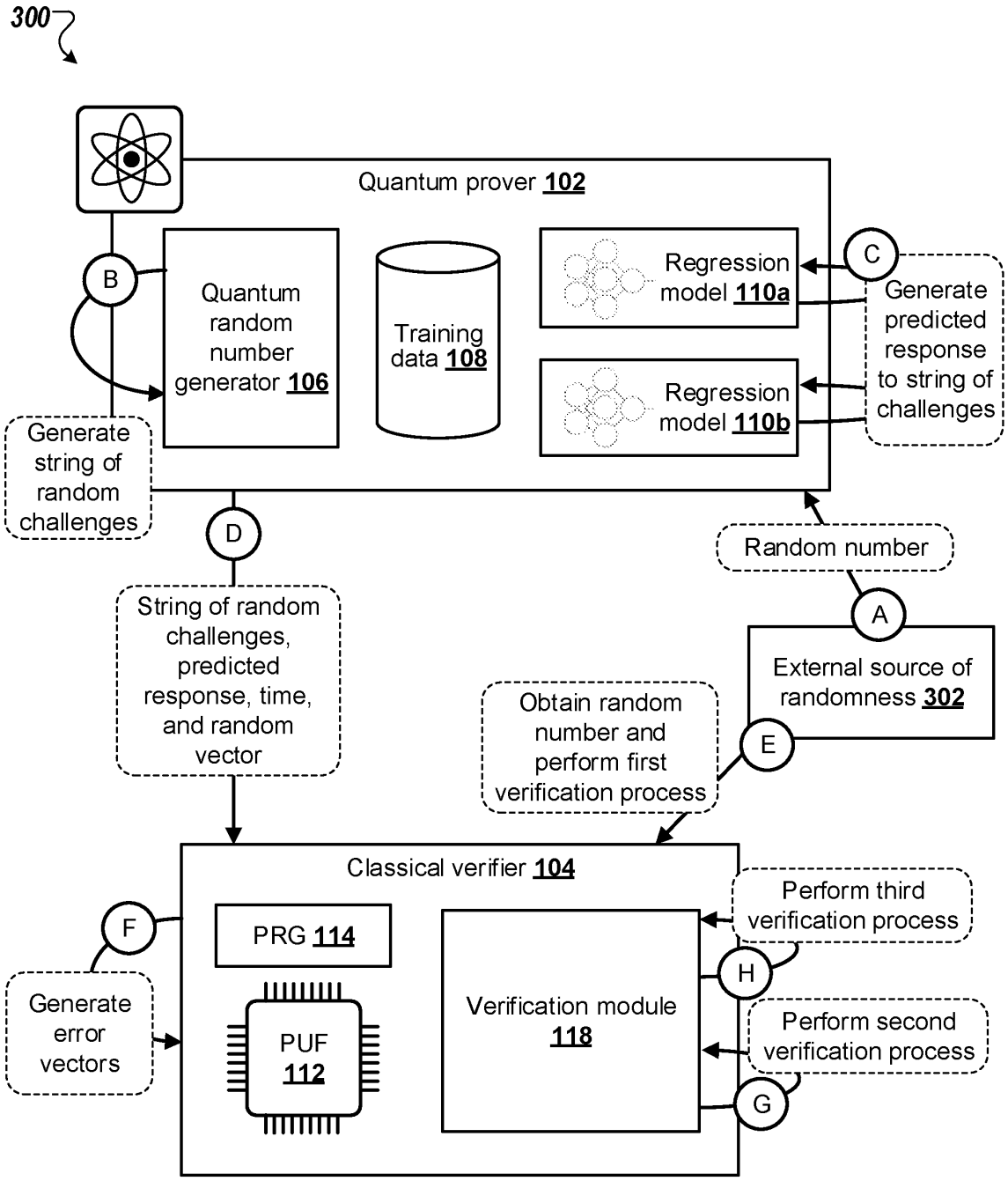
300
Quantum prover 102
Quantum random number generator 106
Training data 108
Regression model 110a
Regression model 110b
Generate predicted response to string of challenges
Generate string of random challenges
Random number
External source of randomness 302
String of random challenges, predicted response, time, and random vector
Obtain random number and perform first verification process
Classical verifier 104
PRG 114
PUF 112
Verification module 118
Perform third verification process
Perform second verification process
Generate error vectors
A
B
C
D
E
F
G
H

FIG. 3

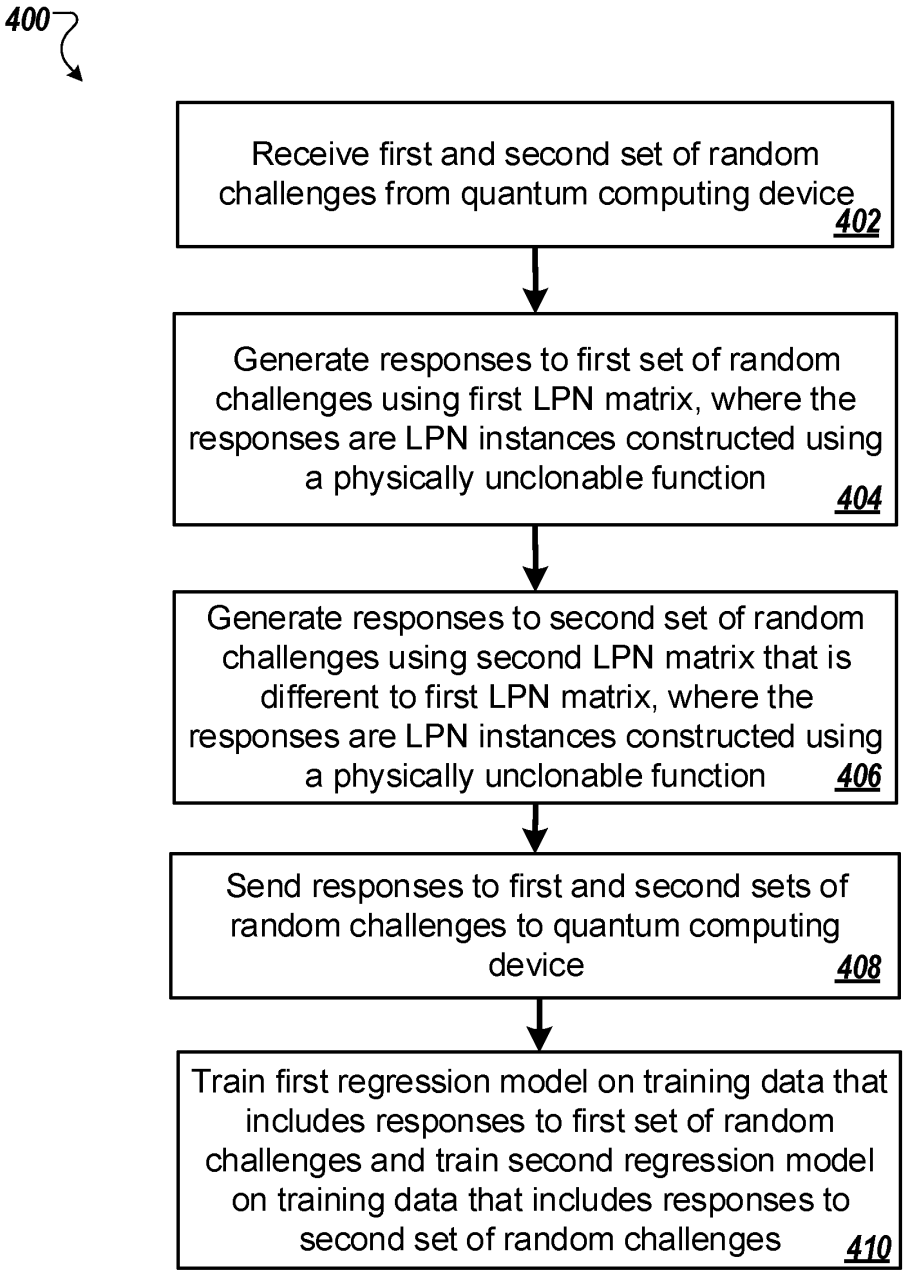
400
Receive first and second set of random challenges from quantum computing device
402
Generate responses to first set of random challenges using first LPN matrix, where the responses are LPN instances constructed using a physically unclonable function
404
Generate responses to second set of random challenges using second LPN matrix that is different to first LPN matrix, where the responses are LPN instances constructed using a physically unclonable function
406
Send responses to first and second sets of random challenges to quantum computing device
408
Train first regression model on training data that includes responses to first set of random challenges and train second regression model on training data that includes responses to second set of random challenges
410

FIG. 4

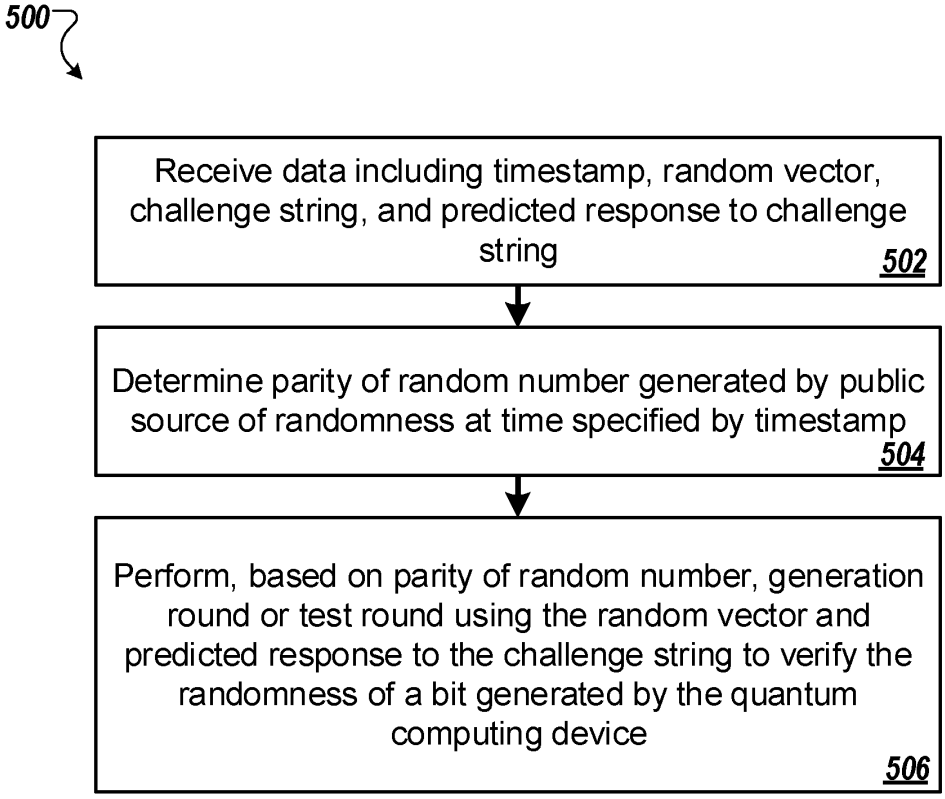
500
Receive data including timestamp, random vector, challenge string, and predicted response to challenge string
502
Determine parity of random number generated by public source of randomness at time specified by timestamp
504
Perform, based on parity of random number, generation round or test round using the random vector and predicted response to the challenge string to verify the randomness of a bit generated by the quantum computing device
506

FIG. 5