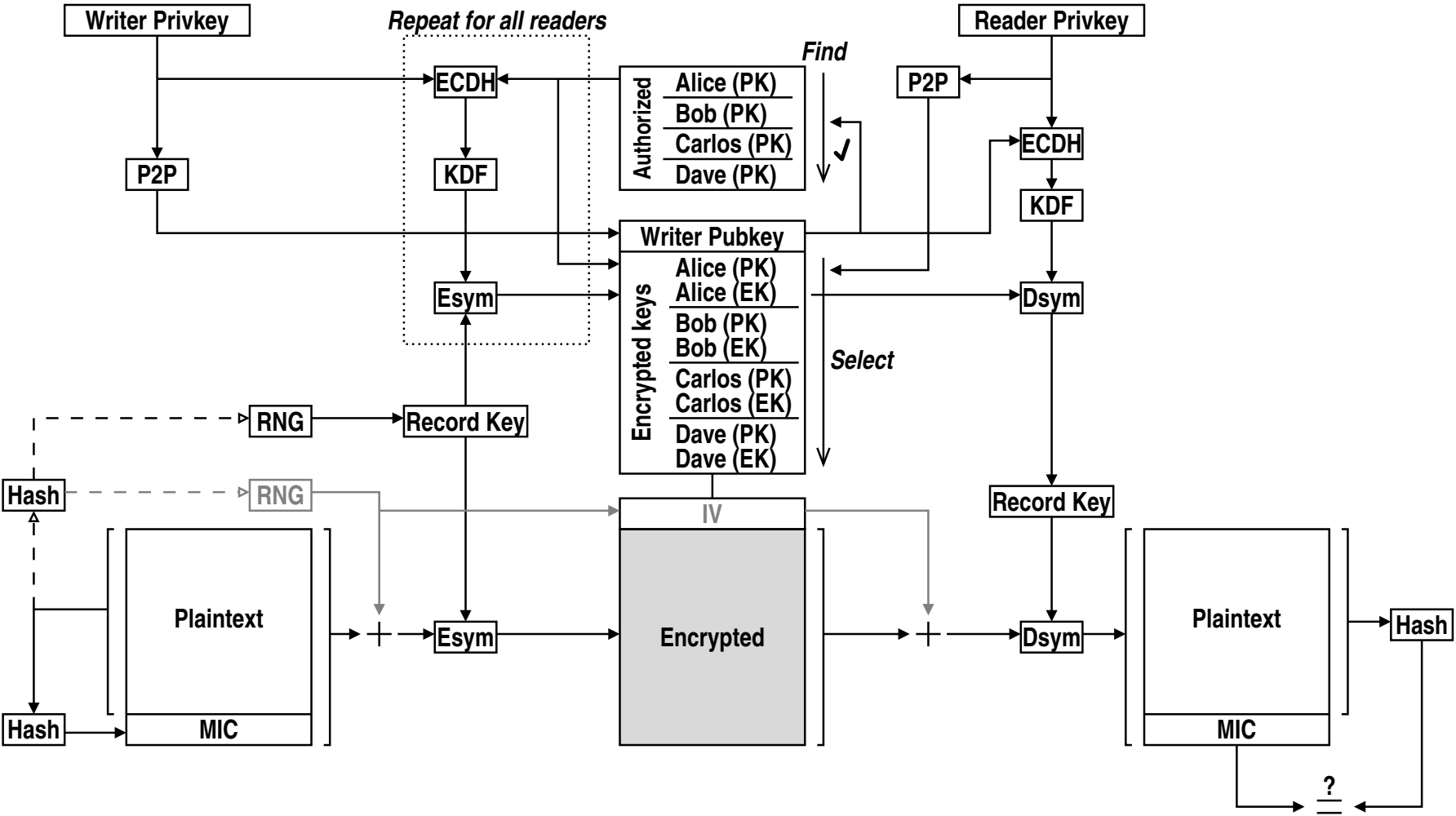
Writer Privkey
Repeat for all readers
Reader Privkey
Find
ECDH
Authorized
Alice (PK)
Bob (PK)
Carlos (PK)
Dave (PK)
P2P
P2P
KDF
ECDH
KDF
Writer Pubkey
Encrypted keys
Alice (PK)
Alice (EK)
Bob (PK)
Bob (EK)
Carlos (PK)
Carlos (EK)
Dave (PK)
Dave (EK)
Esym
Dsym
Select
RNG
Record Key
Hash
RNG
IV
Record Key
Plaintext
Esym
Encrypted
Dsym
Plaintext
Hash
Hash
MIC
MIC
?