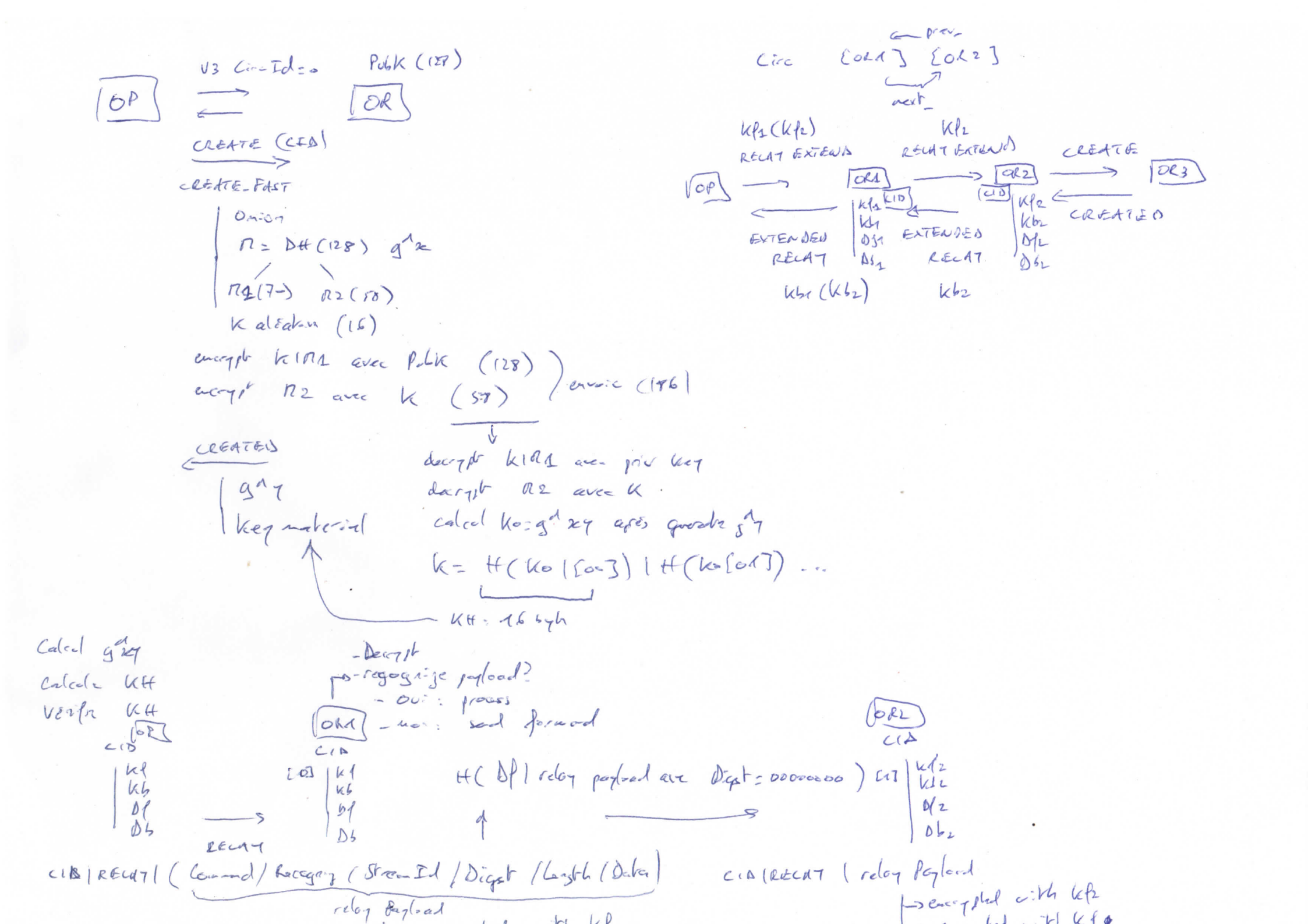
OP
OR
V3 Circ-Id = 0
PubK (128)
CREATE (CEA)
CREATE_FAST
Omega
n = DH (128) g^x
n1 (72) n2 (58)
K aleatoire (16)
encrypt K|n1 avec PubK (128)
encrypt n2 avec K (58)
envoie (186)
CREATED
g^y
key material
decrypt K|n1 avec priv key
decrypt n2 avec K
calcul K0 = g^xy après generate y
K = H(K0|[00]) | H(K0|[01]) ...
KH : 16 byte
Circ
[OR1]
[OR2]
prev
next
Kf1 (Kf2)
RELAY EXTENDED
Kf2
RELAY EXTENDED
CREATE
OR1
OR2
OR3
CID
KID
Kf1
Kb1
Df1
Db1
Kf2
Kb2
Df2
Db2
EXTENDED RELAY
EXTENDED RELAY
CREATED
Kb1 (Kb2)
Kb2
Calcul g^xy
Calcule KH
Verifie KH
OR2
CID
Kf
Kb
Df
Db
RELAY
-Decrypt
-regarde si je payload?
- oui : process
- non : send forward
OR1
CID
[01]
Kf1
Kb1
Df1
Db1
H(Df | relay payload avec Digest = 00000000) [17]
OR2
CID
Kf2
Kb2
Df2
Db2
CID | RELAY | (Command | Recognized | StreamId | Digest | Length | Data)
relay payload
CID | RELAY | relay Payload
→ encrypted with Kf2