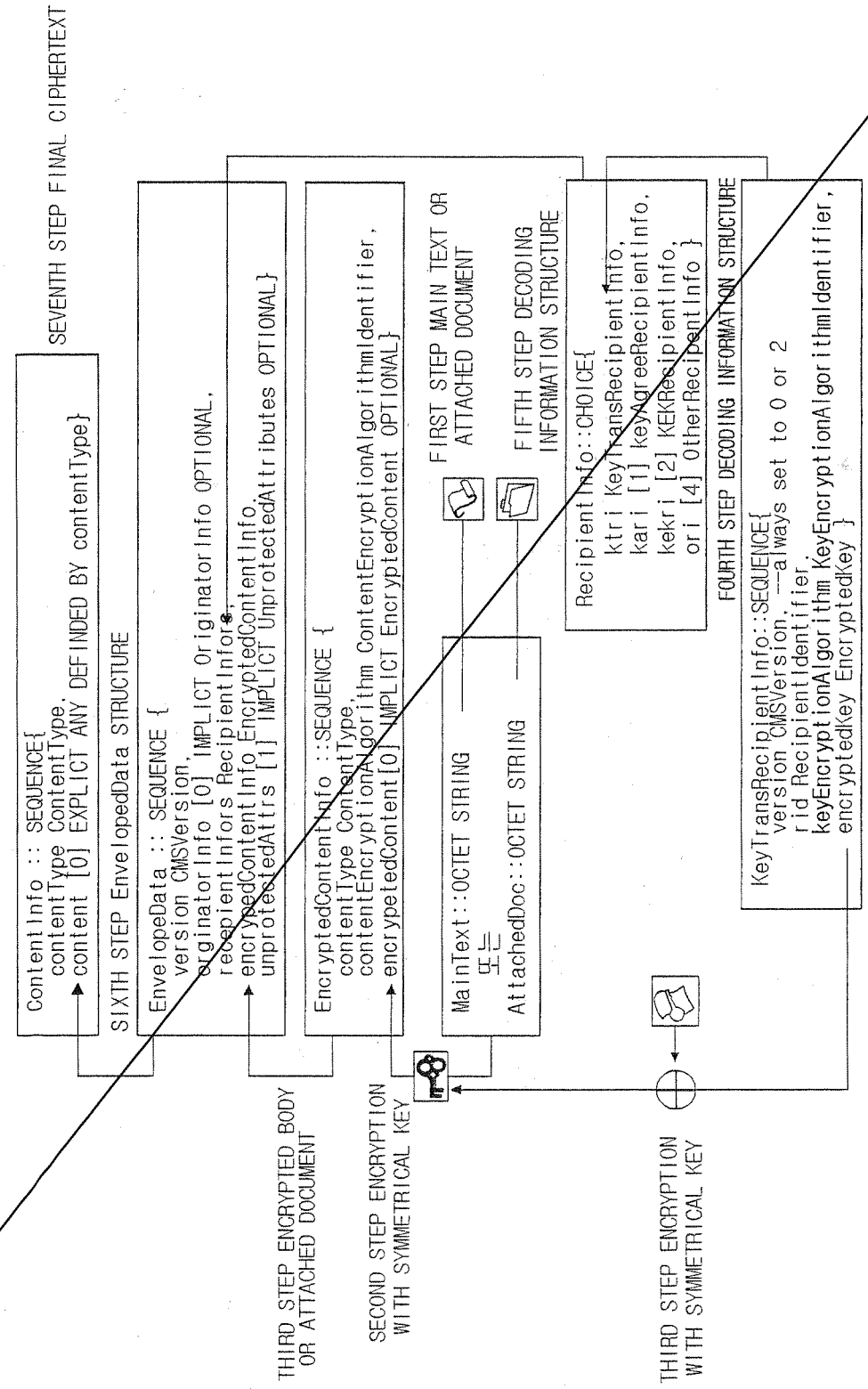
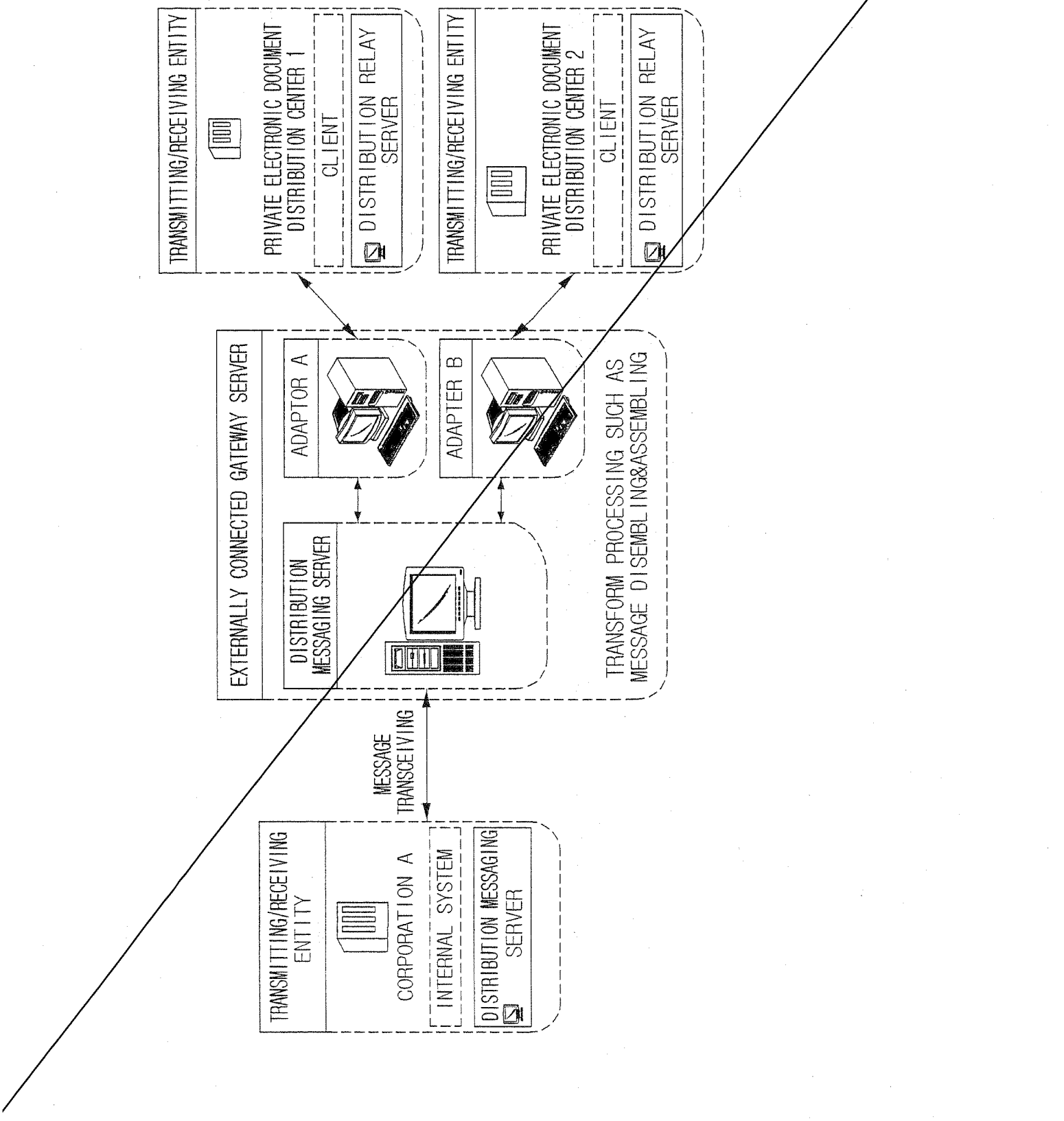
[FIG. 12]


SEVENTH STEP FINAL CIPHERTEXT
ContentInfo :: SEQUENCE{
contentType ContentType,
content [0] EXPLICT ANY DEFINDED BY contentType}
SIXTH STEP EnvelopedData STRUCTURE
EnvelopeData :: SEQUENCE {
version CMSVersion,
orginatorInfo [0] IMPLICT OriginatorInfo OPTIONAL,
recipientInfors RecipientInfors,
encryptedContentInfo EncryptedContentInfo,
unprotectedAttrs [1] IMPLICT UnprotectedAttributes OPTIONAL}
EncryptedContentInfo ::SEQUENCE {
contentType ContentType,
contentEncryptionAlgorithm ContentEncryptionAlgorithmIdentifier,
encrypetedContent[0] IMPLICT EncryptedContent OPTIONAL}
MainText::OCTET STRING
또는
AttachedDoc::OCTET STRING
FIRST STEP MAIN TEXT OR
ATTACHED DOCUMENT
FIFTH STEP DECODING
INFORMATION STRUCTURE
RecipientInfo::CHOICE{
ktri KeyTransRecipientInfo,
kari [1] keyAgreeRecipientInfo,
kekri [2] KEKRecipientInfo,
ori [4] OtherRecipientInfo }
FOURTH STEP DECODING INFORMATION STRUCTURE
KeyTransRecipientInfo::SEQUENCE{
version CMSVersion, --always set to 0 or 2
rid RecipientIdentifier,
keyEncryptionAlgorithm KeyEncryptionAlgorithmIdentifier,
encryptedkey EncryptedKey }
THIRD STEP ENCRYPTED BODY
OR ATTACHED DOCUMENT
SECOND STEP ENCRYPTION
WITH SYMMETRICAL KEY
THIRD STEP ENCRYPTION
WITH SYMMETRICAL KEY

[FIG. 32]


TRANSMITTING/RECEIVING ENTITY
PRIVATE ELECTRONIC DOCUMENT DISTRIBUTION CENTER 1
CLIENT
DISTRIBUTION RELAY SERVER
TRANSMITTING/RECEIVING ENTITY
PRIVATE ELECTRONIC DOCUMENT DISTRIBUTION CENTER 2
CLIENT
DISTRIBUTION RELAY SERVER
EXTERNALLY CONNECTED GATEWAY SERVER
ADAPTOR A
ADAPTER B
DISTRIBUTION MESSAGING SERVER
TRANSFORM PROCESSING SUCH AS MESSAGE DISEMBLING&ASSEMBLING
MESSAGE TRANSCEIVING
TRANSMITTING/RECEIVING ENTITY
CORPORATION A
INTERNAL SYSTEM
DISTRIBUTION MESSAGING SERVER