1, Request

Bob

TTP

Alice

2,L

3,doc, EOO, L

4, L, EOO

5, L, EOR

6, L, doc

7 ,L, EOR

8, L

8,L

Explain of Coffry\_Saidha fair exchange protocol:

Notations:

L: Unique label to link all message of a given protocol run

EOO: SigA(H(doc))

EOR: SigB(sigA(H(doc)))

Sstep0: Alice and Bob register;

--Alice and Bob get userId(A), userId(B), publicKey(A),publicKey(B) from registerUser;

Step1: Alice sends a request to TTP that she wants a fair exchange with Bob;

--TTP calls getUserKey(Alice) to check that Alice exists and that she is using the correct key

--TTP calls getUserKey(Bob) to check that Bobs exists and that he is using the correct key

-- if all userKey is right , TDS getLabel() to get a unique label and sends the message to DB to use the StoreMessage(label, sender: Alice, receiver: TTP, step:1, message: request, protocol: Coffry\_Saidha) in the message\_log\_table, the same message also need store in the exchange\_state\_table.

Return  success/failure

(It means that this fair exchange is effective)

Step2: TTP sends a unique label to Alice;

--Alice stores the label in the client;

--TDS send the message to DB, for the message\_log\_table, StoreMessage(label, sender:TTP, receiver: Alice, step:2, message: label, protocol: Coffry\_Saidha)

For the exchange\_state\_table, just change the step in to 2 and message according the storeMessage.

Return  success/failure

Step3: After Alice receives the label, she will send the document which she wants to give Bob and EOO(SigA(H(doc))) and label to TTP, After TTP receives the message from Alice, it stores the document;

--Alice sends her privateKey with h(doc) and label to TTP;

--TTP stores the document into S3

--S3 get the objectID and send it to DB.

--DB stores the objectID in the exchange\_state\_table,

--TTP send the message to DB, DB storemessage (label, sender:Alice, receiver: TTP, step:3, message: SigA(H(doc)) , protocol: Coffry\_Saidha))

-- For the exchange\_state\_table, just change the step in to 3 and message according the storeMessage.

Return success/failure

Step4: TTP sends the EOO(SigA(H(doc))) and the label to Bob;

--TTP get EOO from DB and label to Bob;

--Bob stores SigA(H(doc)) and label;

--TTP sends message to DB, and DB will store the StoreMessage(label, sender:TTP, receiver: BOb, step:4, message: SigA(H(doc) , protocol: Coffry\_Saidha)) in the message\_log\_table.

-- For the exchange\_state\_table, just change the step in to 4 and message according the storeMessage.

Return success/failure

Step5: Bob sends the EOR(SigB(sigA(H(doc)))) and label to TTP after he receives EOO;

--Bob send his privateKey with SigA(H(doc)) and label to TTP;

-- TTP sends message to DB, and DB will store the StoreMessage(label, sender:Bob, receiver:TTP, step:5, message: SigB(sigA(H(doc)) , protocol: Coffry\_Saidha)) in the message\_log\_table.

-- For the exchange\_state\_table, just change the step in to 5 and message according the storeMessage.

Return success/failure

Step6: After receiving EOR from Bob, TTP would send the document and label to B which it store before;

--TTP get the document from S3, and send document to B, B store the document.

-- TTP sends message to DB, and DB will store the StoreMessage(label, sender:TTP, receiver:BOb, step:6, message: doc, , protocol: Coffry\_Saidha)in the message\_log\_table.

-- For the exchange\_state\_table, just change the step in to 6 and message according the storeMessage.

Return success/failure

Step7: TTP sends EOR and label to Alice which means Bob will receive the document which she wants to give.

--Alice store EOR;

-- TTP sends message to DB, and DB will store the StoreMessage(label, sender:TTP, receiver:Alice, step:7, message: doc, , protocol: Coffry\_Saidha)in the message\_log\_table.

-- For the exchange\_state\_table, just change the step in to 7 and message according the storeMessage.

Return success/failure

Step8: Alice and Bob send the label to TTP which means this fair exchange finished.

--Alice and Bob delete the label after sending.

-- TTP sends message to DB, and DB will store the StoreMessage(label, sender:Alice, receiver:TTP, step:8, message:label, in the message\_log\_table.

StoreMessage(label, sender:Bob, receiver:TTP, step:8, message:label, , protocol: Coffry\_Saidha)in the message\_log\_table.

-- For the exchange\_state\_table, just change the step in to 8 and message according the storeMessage.

Return success/failure

Abort protocol

Step1: Alice sends SigA(abort, Mxa)

- TTP sends message to DB, and DB will store the StoreMessage(label, sender:Alice, receiver:TTP, step:abort\_1, message:abort, in the message\_log\_table.

-- For the exchange\_state\_table, just change the step in to abort\_1 and message according the storeMessage.

Return success/failure

Step2:TTP sends Alice: resolved? If true: send resolved\_contract; if false, send abort\_token; set aborted=true;

Reference: Distributed Algorithms lecture notes.