# DESIGN AND EVALUATION OF A NEW FAIR EXCHANGE PROTOCOL BASED ON AN ONLINE TTP

Abdullah AlOtaibi and Hamza Aldabbas

Software Technology Research Laboratory (STRL)
De Montfort University, Leicester, United Kingdom

Otaibi_as@hotmail.com, hamza@dmu.ac.uk

## *ABSTRACT*

*Security protocols in e-commerce are required to manage the transactions between buyers and sellers. In order to engage customers in e-commerce, these protocols should be well formulated and secured; they should protect both parties from fraudulent users and subsequently promote the growth of e-commerce. There are some protocols, known as fair exchange protocols, in e-commerce that are designed to guarantee fairness between the customer and the merchant so that neither party gains any advantage over the other. Therefore, in this paper, we introduce a new fair exchange protocol for trading products online between a buyer and a seller. The items to be exchanged in this protocol are a digital product and a payment. The following are the characteristics of this new protocol: (1) Dependency on a trusted third party is greatly reduced; further, the protocol also overcomes increased communication overheads and risks, hence leading to substantial improvement in the efficiency and practicality of the protocol. (2) The protocol ensures fairness for all parties and provides an internal dispute resolution mechanism, thereby guaranteeing that none of the parties involved in the transaction suffer unfairly in case one of the entities disappears before the transaction is formalized. (3) The protocol consists of three messages exchanged between the buyer (customer) and the seller (merchant).*

## *KEYWORDS:*

*E-commerce, Fair exchange protcocol, TTP (Trusted Third Party); protocols; security; fairness.*

## 1. INTRODUCTION

Over the past few years the Internet has become an essential business platform by aiding trading, distribution and sales between organisations, consumers, and even between consumers. This has brought ecommerce to an entirely new level[1]. Nowadays, without doubt, the development of information and communication technology is playing an enormous part in making individuals' lives easier than before. Due to the rapid growth of e-commerce in recent years, much business today is conducted online. In other words, more businesses than ever before are using the Internet to sell their commodities to people all over the world. The Internet provides them with a platform for selling their items to all kinds of people without the restrictions of geographical borders. Customer choice in buying goods and services has been greatly enhanced by this growth of e-commerce. For various reasons, many customers today opt to buy their items through the Internet; firstly, they have the convenience of making purchases from the comfort of their homes removing the need to go to shopping centres or

DOI : 10.5121/ijnsa.2012.4402

suffering the inconvenience of traffic jams and parking problems. Secondly, customers have the opportunity to quickly compare the prices of various traders. Thirdly, goods and services are delivered to the customer’s home. Lastly, customers are able to buy products at any time, from anywhere in the world.

In traditional commerce, customers do not have to worry that they will be given the product that they paid for. This is because the customer goes to a shop, selects a product, pays for it and takes it away. Customers also do not have to worry that their financial data will be revealed to a third party, as they make payment in cash. In addition to the above points, customers can also remain anonymous and avoid the merchants tracing their buying habits by making their payments in cash. However, in e-commerce, such factors can become a major concern for customers; for example, through online payment, personal data and financial information that is not encrypted might be revealed to fraudulent persons.

There must be trust between the buyer and the seller, but in e-commerce, customers are worried that dishonest dealers might send them the wrong or inferior product. There must be a system in place to ensure that the data being sent through any secure means are heavily protected. There is no doubt that e-commerce has made the exchange of goods and services easier but it also poses risks to both the customer and the merchant, in terms of security, safeguarding users’ privacy, trust and anonymity [2, 3].

## 2. FAIRNESS IN ELECTRONIC COMMERCE

According to Asokan [5], a fair system refers to a system “that does not discriminate against a correctly behaving player. As long as a player behaves correctly, a fair system must ensure that other players will not gain any advantage over the correctly behaving players.” In a fair exchange scenario, the transacting parties, for example X and Y, follow a fair exchange process. This process must not allow a situation where X can obtain Y’s items while Y cannot obtain X’s items. A process that involves a fair exchange protocol between X and Y must fulfil three conditions:

1. **Effectiveness:** If the protocol is executed correctly and the parties X and Y honourtheir commitment, then both parties will have each other’s items.

2. **Timeliness:** The protocol will be executed within an acceptable timeframe.

3. **Fairness:** There are two types of fairness:

    - *Strong fairness*: This means that at the end of the protocol, either eachparty obtains the expected item from the other, or no party obtains the expected item. This means that a party who behaves correctly does not suffer any disadvantage. For example, both parties shouldreceive the expected items, or neither do so.
    - *Weak fairness*: This means that at the end of the exchange, either strongfairness is achieved, or the correctly behaving party thatdoesnot receive the expected item can prove to a third partythat Y has received (or stillcanreceive) X’s item, without anymore involvement from X (regardless of whether Y behaves correctly or not), and vice versa. Although strong fairness isdesirable, sometimes it is very expensive or impossible to guarantee, that is why the two forms of fairness exist.

Weak fairness is important because it provides a platform for dispute resolution. The disadvantaged party can seek a dispute resolution outside the system. The party that suffered a disadvantage can achieve strong fairness by using an external dispute resolution system, such as a court of law, provided it can prove that it was treated unfairly. There are a number of fair exchange protocols that can ensure strong fairness by using a trusted third party. Most of these protocols, apart from Burk and Pfitzmann [6], refer to the fairness definition of Asokan [5].

Other protocols (such as those of Jakobsson, Pagnia and Jansen [7], and Sandholmand Lesser [8]) are difficult to juxtapose, as they do not precisely define the kind of fairness that has been attained. The Asokanas [9] definition of fairness will be used as a foundation for the formalization in the sections below, as other explanations of fairness (such as the notions of money atomicity and goods atomicity of Tygar [2]), have not been exactly defined.

# 3. TYPES OF FAIR EXCHANGE PROTOCOLS

Fair exchange protocols (whether they are for certified email, certified delivery, contract signing or fair purchase) may be classified into two main types, depending on the use of the TTP. Those protocols that do not involve the use of a TTP are the first type, while those protocols that involve the use of a TTP form the second type [4, 7, 10].

## 3.1.Protocols that involve a TTP

The protocols that involve the use of a TTP can be divided into three types, which are as follows [11]:

### 3.1.1. Protocols that are based on inline TTP.

Inline TTP-based protocols use the TTP for sending the traded commodities to the respective parties. This means that the TTP receives the items from each party, authenticates them and delivers them to the respective parties. For example, if there is a customer and a merchant in a transaction, then the two parties will exchange items such as a digital product (held by the merchant) and a payment (held by the customer). The protocol is then carried out in the following way. Both the customer and the merchant send their items to the TTP. The customer sends the payment while the merchant delivers the digital product. Then, the TTP authenticates the received items and, after approving them, it delivers the payment to the merchant and the digital product to the customer. Figure 1 illustrates a model of a fair exchange protocol that involvesan inline TTP.

We realize in this protocol that the TTP is actively involved in the exchange of items between the transacting parties. Engaging the TTP in this type of protocol guarantees that the parties involved in the transaction exchange their items fairly. Direct contact between the transacting parties is not normally necessary in inline TTP-based protocols.

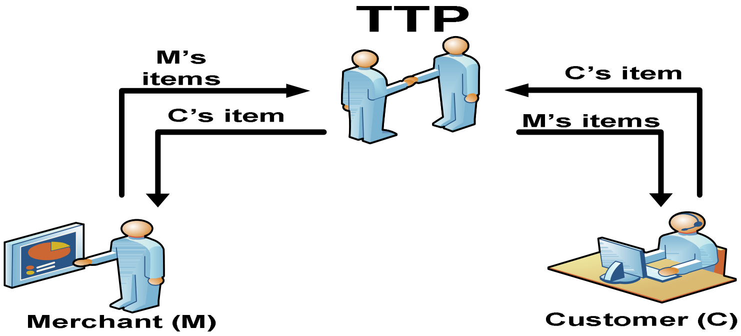

**Figure 1:** Inline TTP-based fair exchange model

The protocols that use an inline TTP to guarantee fairness for all parties involved in the transaction because the TTP will deliver the respective items to the parties;however, they also have some drawbacks. Firstly, it is expensive to run inline TTP protocols, asthey require the availability of the TTP during the execution of the protocol, which will lead to extra costs [12]. Secondly, in this type of protocol, the TTP may become the source of a communication bottleneck, hence leading to performance problems [5, 7, 13, 14] and[5, 5]. This is because the items to be exchanged must pass through the TTP. Thirdly, in the case of a crash at the TTP, the protocol will not be carried out and the parties will not be able to receive the items that they expect. Lastly, in the case of an attack, the TTP will be the main target [13].

Burk and Pfitzmann [6] suggestedan inline TTP-based fair exchange protocol that allows the transacting parties (where the parties are the customer and the merchant, and the items are the payment and the digital product) to reach an agreement on the items to be exchanged. Both parties then communicate with the TTP to confirm the contract that they have agreed upon. The payment is subsequently sent to the TTP by the customer.

Upon receiving the payment, the TTP confirms and verifies whether or not the payment is in accord with the agreement between the parties. After verifying that the payment is in accord with the agreement, the TTP sends a message to the merchant confirming that the correct payment from the customer has been received. After that, the digital product is sent to the TTP by the merchant. When the digital product is received by the TTP from the merchant, the TTP confirms and verifies whether or not the product certifies the agreement made by the two parties. If the digital product is in line with the description of the customer and fulfils the agreement between the two parties, the TTP then delivers the digital product and the payment to both the customer and the merchant, respectively.

### 3.1.2. Protocols that are based on online TTP

Protocols that make use of an online TTP involve less participation on the part of the TTP. In such a protocol, the TTP will not be used during the protocol run for delivering the parties' items, but rather, for verifying the items, and for generating and/or storing proof of exchange of the items [4]. The figure below illustrates the use of online TTP in fair exchange protocols. If the commodities to be traded between the transacting parties are a digital product and a payment, the customer starts the exchange, and when the payment is received by the merchant from the customer, the merchant verifies it with the TTP (a bank for example) before sending the digital product to the customer.

The TTP must therefore be online for the exchange process to be completed and should be contacted in case there is any dispute. Figure 2 illustrates a model of a fair exchange protocol that is based on an online TTP. There is minimal involvement on the part of the TTPin this type of protocol, but the TTP must be available during the exchange process. This can be viewed as a drawback because the TTP may become the source of a communication bottleneck. In addition, the TTP might be targeted by dishonest users.

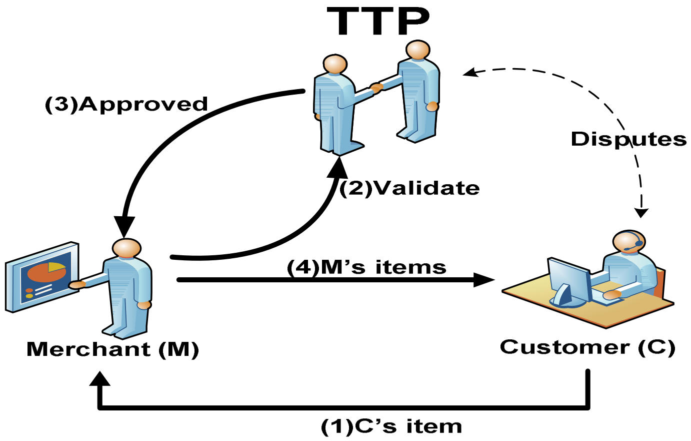

**Figure 2:** Online TTP-based fair exchange model

Zhang *et al.*[16] suggested a fair exchange protocol that uses an online TTP. This protocol is for the exchange of an item, such as a physical product, and a payment. The customer makes an online payment (i.e. via the protocol messages) to the merchant, where a delivery agent is used to deliver the product to the customer, which means that the product is not transmitted electronically. The protocol is based on the theory of cross validation [17]. In this protocol, the customer first begins the process by ordering a product from the merchant. The merchant then sends the invoice to the customer. Once the customer is happy with the invoice, they first send a coded payment to the merchant and secondly to the TTP (the bank). It is taken for granted that the merchant can download the coded payment (that was sent by the customer to the TTP) from the TTP (the bank). The merchant then makes a comparison of the two encrypted payments (i.e. the one received from the customer and the one downloaded from the TTP). If the merchant is satisfied that the encrypted messages compare, it means that the payment is valid. The merchant then delivers the product to the delivery agent after confirming the coded payment. The customer then takes the product from the delivery agent and, after confirming that the correct product has been sent, they send the decryption key to the merchant, who will then decode the coded payment.

### 3.1.3. Protocols that are based on offline TTP

In offline TTP protocols, the transacting parties exchange their commodities directly without the use of the TTP unless a problem occurs. Such type of protocols is also known in the literature as“Optimistic fair exchange protocols”. These protocols will thus be called optimistic fair exchange protocols. The example below illustrates how optimistic fair exchange protocols work if the commodities to be traded between the transacting parties are a payment and a digital product. The two parties directly trade their items, and in case of any problem, the TTP will be involved to mediate between the parties. Figure 3 illustrates a model of a fair exchange protocol that uses an offline TTP (optimistic fair exchange protocol).

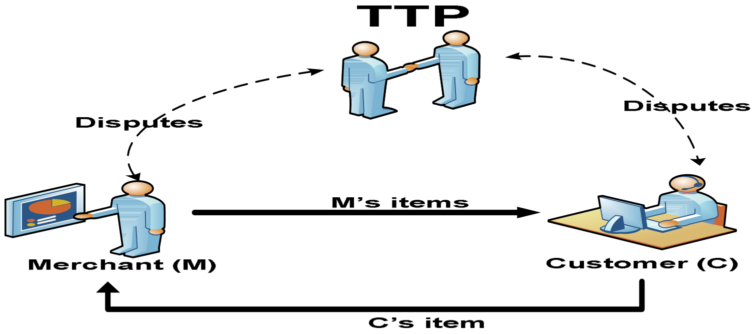

**Figure 3:** Offline TTP-based fair exchange model

In the optimistic fair exchange protocol, the role of the offline TTP is greatly reduced because the TTP is not involved in every exchange. As a result, the issue of the TTP being the source of a communication bottleneck, which is found in protocols that involve inline and online TTPs, is greatly reduced, as the parties exchange their items directly and rarely use the TTP.

The other advantage of these protocols is that the issue of having the TTP as the only source of failure is decreased, as the TTP will not be involved in the transaction unless there is a dispute. In addition to the above advantages, it will be less costly to run the TTP, as it will not be actively involved in the exchange process.

Zhang *et al.*[15] suggested an optimistic fair exchange protocol for trading two valuable documents (the two documents can be a payment and a digital product) between two parties; Party A and Party B (the two parties can be a customer and a merchant).The process of exchanging the items in Zhang's protocol consists of four messages to be exchanged between Party A and Party B. Party A begins the exchange process by transmitting the first message to Party B with the coded document of Party A,together with the coded key that decodes the decrypted document. After receiving the first message, Party B verifies its authenticity and, if satisfied, then transmits the second message to Party A,together with the coded document of Party B and the encrypted key that decodes it.

Upon receiving the second message, Party A verifies its validity and, if approved, then transmits the third message with the decoding key to Party B. After receiving the decoding key, Party B then uses it to decode the decrypted document that was obtained in the first message. After that, Party B transmits the fourth message with the decoding key to Party A. After receiving the decoding key, Party A then uses it to decode the coded document that was obtained in the second message. In case of any problem, the TTP will be involved.

## 3.2.Protocols that do not involve a TTP

In this type of protocol, the two parties involved in the transaction exchange their items without the involvement of a TTP.

### 3.2.1. Gradual Exchange Protocols

Gradual exchange protocols [18, 19] can be used when the commodities to be exchanged can be partitioned into a number of parts. The gradual exchange protocol is based on the principle of having several rounds to complete the process of exchanging items between the transacting parties. The parties exchange some items in every round and the number of rounds is equivalent to the number of parts into which the commodities are divided. The process of exchanging commodities continues until the transaction is completed and each party receives what s/he expects. In each round, both the customer and the merchant send part of their commodity and also receive part of the other party's commodity (see Figure 4). The number of parts delivered to each party is almost the same at any given time [14].

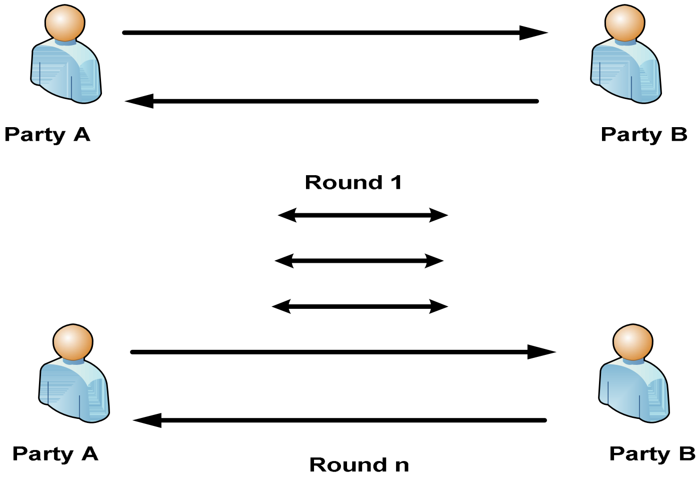

**Figure 4:** Gradual exchange protocols.

The major drawback of the gradual exchange protocol is that several rounds are needed to complete the exchange process. If there are many rounds to be made, a number of communication steps are required, which can heavily load the communication channel to be used between the two parties. Here, it is actually taken for granted that the items to be traded between the transacting parties are of the same size [11]. As a result, this type of protocol does not support items of different sizes. Gradual exchange protocol lacks the involvement of a TTP, which makes it problematic,as it is impossible to guarantee fairness for both parties without a TTP who can mediate and solve problems that may arise.

Jakobsson [20] suggested a new way of fair exchange for a digital product and a payment without the use of a TTP;in this instance, the protocol is based on the principle of dividing the payment into two parts. The two parts are then combined before the full payment can be realized, i.e. the first part of the payment cannot be used without the second part, and vice versa.

In the Jakobsson protocol [20], the first part of the payment is sent to the merchant by the customer. The merchant then submits the digital product to the customer after receiving the first initial payment. The customer then submits the second part of the payment to the merchant upon receiving the digital product. The merchant then combines the first and the second parts of the payment to construct the total payment. This protocol does not necessarily provide fairness for the two parties because the customer can vanish after receiving the digital product without sending the payment of the second part. Fairness is not guaranteed in this transaction, as the customer may receive the digital product, whilst the merchant may not receive the second part of the payment,i.e. the total payment could not be constructed

# 4. THEPROPOSED PROTOCOL

## 4.1.Notation

The notations used in the description are presented in Table 1:

Table 1: Notation

| Symbol | Interpretation |
|---|---|
| C, M, FSP | IDs for Customer, Merchant and Financial Service Provider |
| N | Invoice |
| D | Product |
| Di | Product information |
| Pi | Payment Information |
| A → B : X | A sends X to B |
| X → Y | Transmission from entity X to entity Y |
| PK | Public Key |
| SK | Secret Key (Private Key) |
| TSK | Temporary Session Key |
| X:PK | Public Key of Entity 'X' |
| X:SK | Secret Key of Entity 'X' |
| X:PKS[ ] | The data are signed using the Private Key of Entity 'X' |
| X:SKE[ ] | The data are encrypted using the Secret Key of Entity 'X'. |

## 4.2.Assumptions

- An area linked to the merchant's account, known as a public catalogue server, is controlled by the FSP. The merchant can access the server and download messages at any time without any restrictions.

- The protocol is well secured in the sense that any obtained enciphered messages cannot be decoded without the decryption keys.

- The customer opens an account with a FSP and the merchant registers with the FSP.

- The customer processes the payment through the FSP.

- The channel of transactions between the transacting parties is well secured during the exchange process.

- The pre-exchange phase occurs after the customer identifies the commodity that he or she wants to buy from the merchant. During this phase, it is assumed that both of the transacting parties have mutually agreed on the commodity and the price.

- All the entities involved in the transaction have trust and confidence in the FSP. The FSP is expected to be fair and objective.

## 4.3.Protocol description

This new protocol is intended to achieve fairness when exchanging a digital commodity D and a payment. The fundamental principle of this new protocol is to decrease the communication overheads by separating the transaction process into two phases. The protocol is also aimed at resolving the bottleneck issue through an online-based TTP.

### 4.3.1. Pre-exchange phase

Figure 1 below demonstrates the activities of the pre-exchange phase. The customer, (C), first selects the commodity, then the merchant (M) enciphers the commodity by using a temporary session key that C will use when decoding the commodity. During this phase, M creates the invoice for the commodity to be purchased. M subsequently submits the TSK with the invoice to the FSP. Both the TSK and the invoice are kept and maintained by the FSP. The FSP signs the invoice using its secret key and transmits it back to the merchant. The invoice contains the following information:

The product specifications, Di
The identity of the customer, C
The identity of the merchant, M.

*Pr-m1: Merchant → Financial Service Provider (FSP)*
*M: SK S [TSK, N].*
*Pre-m2: Financial Service Provider (FSP) → Merchant*
*FSP: SK S [N].*

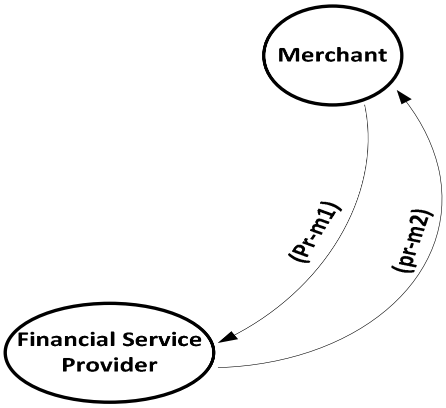

**Figure 1:** Pre-exchange phase

### 4.3.2. Exchange phase

During this phase, the transacting parties (C and M) and the FSP exchange three messages (Figure 2). These messages are as follows:

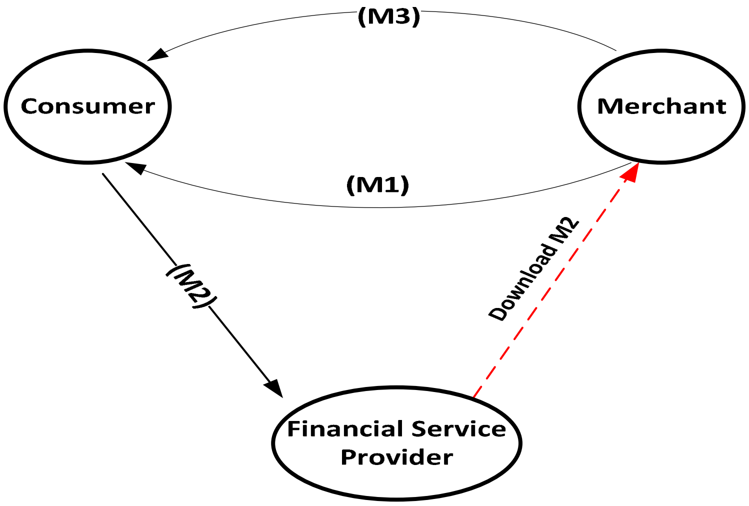

**Figure 2**: The exchange phase

*M1: Merchant → Consumer*
*M: SK S [ TSK E [D], N, FSP: PK, FSP: SK S [N] ].*
*N: [Di, Merchant ID, C].*

The merchant submits the invoice and the digital commodity to the customer. The digital commodity is enciphered using the session key, and the whole message is enciphered using the private key of the merchant. The message consists of the FSP public key. The public key contains the necessary information about the service provider that the consumer should send the payments to. Upon obtaining message M1 from M, C confirms the validity of D and N as well as FSP's signature on N. In order to verify the validity of D, C has to confirm two things: the digital commodity D itself and the enciphered D.

It is then the customer's wish to either complete or terminate the exchange process. Should he or she decide to complete the process, the customer then submits the following: Pi and N to the FSP. Should the customer decide to terminate the exchange process after obtaining Message 1 and before submitting Message 2 to the FSP, then both parties do not lose anything. On the other hand, if the customer sends Message 2 to the FSP, then the exchange process must be implemented, and the protocol will ensure that both parties exchange each other's item fairly.

*M2: Consumer → FSP*
*C: PK E [Payment Information, N].*

The payment information contains the following data:

The name of the financial institution of the customer
Personal information of the customer, C;
The account details of the customer.
The total amount of money the customer will pay for the digital commodity.

The customer submits the payment verification to the FSP. The message also contains the invoice. The merchant downloads Message 2 from the FSP server. Then, the merchant verifies the payment confirmation.

*M3: Merchant → Consumer*
*M: SK S [TSK].*

After downloading Message 2, the merchant confirms whether the payment is valid or not. If the payment is valid, the merchant submits the TSK to C. On the other hand, if the payment is not valid, M dismisses the transaction and terminates the exchange process. Hence, if the payment is invalid, M will not submit the TSK to C because it is the obligation of the customer to submit the correct payment in order to obtain the decoding key in Message 3.

### 4.3.3. After exchange (dispute resolution)

Disputes are normally associated with C; M will not lodge a complaint, as they obtain the payment first and then submit the TSK to C. Thus, the customer is the weakest link in this exchange process because they have to submit the correct payment in order to obtain the decoding key for the enciphered commodity that they obtained in Message 1.
The diagram below shows the messages that are sent in the case of the customer making a complaint (Figure 3)

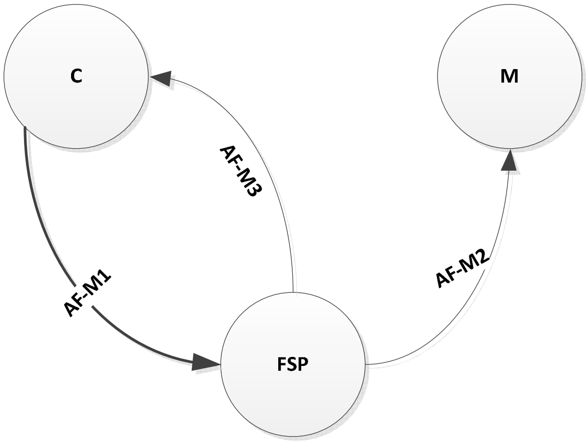

**Figure 3:** Dispute resolution

*Af-M1: Customer → FSP*
*SK S [Payment Confirmation, Invoice]*

*Af-M2: FSP → Merchant*
*FSP sends a warning message to the Merchant.*
*SKS [Payment Confirmation, Invoice]*

*Af-M3: FSP→ C: SKS [TSK]*
*Or*
*FSP→C: abort*

Upon obtaining message Af-M1 above, the FSP will counter-check the payment against the cost of the commodity. If the payment is correct, then the FSP delivers it to M. The aim of forwarding the payment to M is because C might not send any payment to M during the exchange phase or might submit an incorrect payment. On the other hand, if the FSP confirms that the payment is incorrect, it submits a termination message to C.

The customer will not gain an unfair advantage whether C sends an incorrect payment to M or whether no payment is sent at all. This is because the FSP will confirm the payment against the price of the product. If the correct payment has been sent, the FSP will submit the decoding key to C and will also forward the payment to M in order to guarantee fairness for all parties. Hence, all parties involved in the transaction will achieve fairness. However, if the payment is invalid, then the FSP will decline the customer's request for dispute resolution.

## 4.4.The Protocol Analysis

The following cases are considered:

- C claims to the FSP that he has received an incorrect digital product, but he should not have submitted the payment to M; it is the mistake of the customer to submit the payment to M if he had any doubt about the digital product. If the customer submits the payment to M, it implies that he is happy with the digital commodity D. Hence, such a claim will not occur, as C is aware of the rules of the protocol that allow C to confirm the commodity before submitting the payment to M. Therefore, C has to consider his own interest by avoiding risks.
- C claims to the FSP that he has not obtained the decoding key from M. This scenario has three possibilities:

1. C claims to the FSP that he has not obtained the decoding key from M, in spite of having already submitted the correct payment to M. C has the right to lodge a complaint about this to the FSP, and the FSP will resolve the dispute as indicated previously.

2. C claims to the FSP that he has not obtained the decoding key from M and that he submitted an incorrect payment to M. In order to lodge a complaint to the FSP, C submits Message 3 to the FSP, i.e. the message he obtained from M, in addition to the correct payment for the product. In the case of C submitting the correct payment to the FSP, then M will have obtained two payments (the incorrect payment from C, and the correct payment from FSP), and this is the consequence that C has to suffer for being fraudulent.

3. C complains to the FSP that he has not obtained the decoding key from M, and hence has not submitted the payment to M, i.e. C has obtained Message 1 from M but has not submitted Message 2 to M. In order for C to obtain the decoding key, C has to submit to the FSP the correct payment, together with Message 1 that was obtained from M. Therefore, in a scenario where C has not submitted Message 2 to M, then the FSP will submit it (which is the correct payment), and the FSP will also submit the decoding key to C. Therefore, fairness is ensured for both parties.

Of course, M will not lodge a complaint, as M has the decoding key for the payment. We need to consider the following scenario:

1. M complains to have obtained an incorrect payment from C. This is highly unlikely to occur because C is aware that if he submits an incorrect payment, he cannot obtain the

decoding key and the FSP will dismiss the process. However, if it is C's mistake and M wants to negotiate with C, then there is no problem but the FSP will not order M to submit the decoding key, as M has not obtained the correct payment. Hence, if M has obtained an incorrect payment, he will not submit the decoding key.

## 5. COMPARISONS

In this section, the proposed protocol presented in this paper will be compared to Zhang *et al.* [16], Devane et al.[8], Q. Zhang *et al.* and Zhou *et al.*[21].

Zhang *et al.* [16] suggested a fair exchange protocol that uses online TTP. This protocol is for the exchange of an item, such as a physical product and a payment. In this instance, we have observed a limitation in the fairness of the protocol. If the merchant claims that he has received an incorrect decryption key for the payment token, or did not receive one at all, the third party (bank) will provide the K1-1 after checking that the customer is satisfied. The third party (bank) will also provide the K1-1 if the customer is not traceable. However, if the customer is not intentionally untraceable and also does not have the required product, then by having the K1-1 from the third party, the merchant is certainly at an advantage.

Devane *et al.* [8] suggested a fair exchange protocol that can be used for buying items online.
We have observed a limitation in the fairness of the protocol; the merchant will receive the payment only after the customer has confirmed receipt of the items, however, there is no guarantee that the customer will make the payment after acquiring the items. In this instance, the customer is certainly in an advantaged position.

Q. Zhang *et al.* created a protocol [16] that gives users a centric online m-payment solution. We have observed that this protocol has a weakness in terms of fairness. This issue of fairness can arise when the merchant falsely claims that he does not consent to the terms and conditions after the transaction. On the other hand, the customer can falsely claim that the merchant has not posted the product; the third party then requests the merchant to produce the delivery cabinet history and submit proof. There are certain limitations in the fairness of this protocol. For example, if the merchant makes an allegation that he or she received an incorrect decoding key for the payment token, or indeed never received it, then according to the extended protocol, the third party (TP) would issue the Kf' after obtaining the customer's consent. If the customer were untraceable, the third party (TP) would also issue the Kf'. Consider a scenario where the customer is not traceable due to unforeseen circumstances, and has not received the requested item, then by acquiring Kf' from the third party, the merchant would definitely be in aposition of unfair advantage.

Zhou and Gollmann proposed a non-repudiation protocol that uses an online TTP [21]. According to the definition of fairness, the protocol is not fair. This is because, if B gives up after B finishes the first step, B does not know the subject matter of the message, but he receives the Non-Repudiation of Delivery Token. Besides, the protocol is designed to transport more messages when running and it includes C in the evidence, which increases the amount of data transport.

**Table2:** Comparison of fair exchange protocols

| Protocol | Items tobeexchanged | Fairness | Weaknesses | Load onTTP | Efficiency | # Messages (exchange phase) | Type of fairness |
|---|---|---|---|---|---|---|---|
| Zhang et al | Payment and a Product (digital or physical) | Yes | 1 | High | Medium | 7 +physical Deliveryand collection | Strong |
| Devane et al | Payment and digital product | Yes | 1 | High | Medium | 7 | Strong |
| Zhou et al | Provide the originator and the intended recipient with evidence after an execution | Yes | 3 | High | Medium | 5 | Fairness is not ensured |
| Q. Zhang et al | Payment and digital product | Yes | 1 | High | Medium | 12 | Strong |
| **Proposed protocol** | **Payment and digital product** | **Yes** | **0** | **Low** | **High** | **3** | **Strong** |

**Table 3:** Protocol Comparisons

|  | Ray et al [23] | Devane et al [8] | Ray et al[7] | Zhang et al[15] | Alaraj et al[2] | Proposed protocol |
|---|---|---|---|---|---|---|
| **# of messages in the exchange phase** | 6 | 7 | 4 | 4 | 3 | **3** |
| **# of messages in dispute resolution phase** | Not specified | Not specified | 3 to 5 | 3 | 3 | **3** |
| **TTP type** | Inline | Online | Offline | Offline | Offline | **Online** |
| **TTP hold item** | Yes | No | Yes | No | No | **No** |
| **Both parties are involved indispute resolution** | Not specified | Not specified | Yes | No | No | **No** |
| **# of modular exponentiations in the exchange phase** | 20 | 28 | 27 | 20 | 11 | **19** |
| **# of modularexponentiations in the dispute resolution phase** | Not specified | Not specified | 5 to 6 | 6 | 7 | **7** |

**Table 4:**The timing of executing of the proposed protocol for product size = 128 KB

| ID | Action | Source | Destination | Time (ns) | Transferred Bytes |
|---|---|---|---|---|---|
| **Pr-M1** | Generate Temporary Session Key | Merchant | Merchant | 123996 | 8 (Not Transferred) |
| **Pr-M1** | Encrypting Temporary Session Key | Merchant | Merchant | 166949 | 24 (Not Transferred) |
| **Pr-M1** | Sending Encrypted Temporary Session Key | Merchant | FSP | 23791019 | 24 |
| **Pr-M1** | Sending Invoice Details | Merchant | FSP | 76782686 | 77 |
| **Pr-M2** | Generating message digest for signing invoice | FSP | FSP | 19450 | 16 (Not Transferred) |
| **M1** | Encrypting product using session key | Merchant | Merchant | 871214 | 1160 (Not Transferred) |
| **M1** | Encrypting the product and invoice and FSP PK | Merchant | Merchant | 1168236 | 1732 (Not Transferred) |
| **M1** | Sending the product and invoice and FSP PK to the customer | Merchant | Customer | 1732021596 | 1732 |

| | | | | | |
|---|---|---|---|---|---|
| **M1** | Decrypt Merchant Message | Customer | Customer | 1370844 | 1259 (Not Transferred) |
| **M2** | Validate invoice received from customer | FSP | FSP | 27555 | 16 (Not Transferred) |
| **M3** | Sending Session Key to Customer | Merchant | Customer | 11918201 | 8 |

# 6. CONCLUSION

We have introduced in this paper, a new fair exchange protocol for trading a digital commodity and a payment in the B2C domain. The new protocol consists of three messages, to be exchanged between the transacting parties and the FSP, which (to the best of our knowledge) is the minimum number of messages to be exchanged between three parties in fair exchange protocols in the literature. The only way in which M might act unfairly is after obtaining the payment from C and then refusing to send the decoding key or submitting an incorrect decoding key. In this case, the FSP can be used to resolve such a dispute. The protocol can ensure fairness for both transacting parties.

## References

[1] M. Alshehri, H. Aldabbas, J. Sawle and M. A. Baqar. "Adopting E-commerce to user's needs". *International Journal of Computer Science & Engineering Survey (IJCSES), vol 3, no.1,* February 2012.

[2] A. Alaraj and M. Munro, "An efficient e-commerce fair exchange protocol that encourages customer and merchant to be honest," *Computer Safety, Reliability, and Security,* pp. 193-206, 2008.

[3] H. Aldabbas, T. Alwada'n, H. Janicke and A. Al-Bayatti, "Data Confidentiality in Mobile Ad hoc Networks", *International Journal of Wireless & Mobile Networks (IJWMN),* vol. 4, no. 1, February 2012.

[4] A. Nenadic, *A Security Solution for Fair Exchange and Non-Repudiation in e-Commerce,* 2005.

[5] N. Asokan, M. Schunter and M. Waidner, "Optimistic protocols for fair exchange," in *Proceedings of the 4th ACM Conference on Computer and Communications Security,* pp. 7-17, 1997.

[6] H. Bürk and A. Pfitzmann, "Value exchange systems enabling security and unobservability," *Comput. Secur.,* vol. 9, pp. 715-721, 1990.

[7] I. Ray, I. Ray and N. Natarajan, "An anonymous and failure resilient fair-exchange e-commerce protocol," *Decis. Support Syst.,* vol. 39, pp. 267-292, 2005.

[8] S. Devane, M. Chatterjee and D. Phatak, "Secure e-commerce protocol for purchase of e-goods-using smart card," in *Information Assurance and Security, 2007. IAS 2007. Third International Symposium on,* pp. 9-14, 2007.

[9] G. Ateniese, B. de Medeiros and M. T. Goodrich, "TRICERT: A distributed certified e-mail scheme," in *ISOC 2001 Network and Distributed System Security Symposium (NDSS'01),* 2001.

[10] M.Schunter :*Optimistic fair exchange*. PhD Thesis, University of Saarland, Germany, 2000.

[11] S. Kremer, O. Markowitch and J. Zhou, "An intensive survey of fair non-repudiation protocols," *Comput. Commun.,* vol. 25, pp. 1606-1621, 2002.

[12] S. Micali, "Simple and fast optimistic protocols for fair electronic exchange," in *Proceedings of the Twenty-Second Annual Symposium on Principles of Distributed Computing,* pp. 12-19, 2003.

[13] P. Liu, P. Ning and S. Jajodia, "Avoiding loss of fairness owing to process crashes in fair data exchange protocols," in *Dependable Systems and Networks, 2000. DSN 2000. Proceedings International Conference,* pp. 631-640, 2000.

[14] V. Shmatikov and J. C. Mitchell, "Analysis of a fair exchange protocol," in *Proceedings of the Seventh Annual Symposium on Network and Distributed System Security (NDSS 2000),* 2000.

[15] N. Zhang, Q. Shi, M. Merabti and R. Askwith, "Practical and efficient fair document exchange over networks," *Journal of Network and Computer Applications,* vol. 29, pp. 46-61, 2006.

[16] Q. Zhang, K. Markantonakis and K. Mayes, "A practical fair-exchange e-payment protocol for anonymous purchase and physical delivery," in *Computer Systems and Applications. IEEE International Conference*, pp. 851-858, 2006.

[17] I. Ray and H. Zhang, "Experiences in developing a fair-exchange e-commerce protocol using common off-the-shelf components," *Electronic Commerce Research and Applications,* vol. 7, pp. 247-259, 2008.

[18] M. Blum, "How to exchange (secret) keys," *ACM Transactions on Computer Systems (TOCS),* vol. 1, pp. 175-193, 1983.

[19] S. Even, O. Goldreich and A. Lempel, "A randomized protocol for signing contracts," *Commun ACM,* vol. 28, pp. 637-647, 1985.

[20] M. Jakobsson, "Ripping coins for a fair exchange," in *Advances in Cryptology—EUROCRYPT'95,* pp. 220-230, 1995.

[21] J. Zhou and D. Gollman, "A fair non-repudiation protocol," in *Security and Privacy, 1996. Proceedings, 1996 IEEE Symposium*, pp. 55-61, 1996.

[22] A. Alaraj,*Enforcing Honesty in E Commerce Fair Exchange Protocols*. PhD Thesis, University of Durham, UK, 2008.

[23] I. Ray, I. Ray, and N. Narasimhamurthy: A Fair-Exchange E-Commerce Protocol with Automated Dispute Resolution. In proceedings of the 14th Annual IFIP WG 11.3 Working Conference on Database Security, The Netherlands, pp. 27-38, 2000