energies

MDPI

Article

Design of a Logistics System with Privacy and Lightweight Verification

Chin-Ling Chen [1,2,3], Dong-Peng Lin [4], Hsing-Chung Chen [5,6,7,*], Yong-Yuan Deng [3,*] and Chin-Feng Lee [4,*]

1 School of Computer and Information Engineering, Xiamen University of Technology, Xiamen 361024, China
2 School of Information Engineering, Changchun Sci-Tech University, Changchun 130600, China
3 Department of Computer Science and Information Engineering, Chaoyang University of Technology, Taichung 41349, Taiwan
4 Department of Information Management, Chaoyang University of Technology, Taichung 41349, Taiwan
5 Department of Computer Science and Information Engineering, Asia University, Taichung 41354, Taiwan
6 Department of Medical Research, China Medical University Hospital, China Medical University, Taichung 40402, Taiwan
7 Department of Bioinformatics and Medical Engineering, Asia University, Taichung 41354, Taiwan
* Correspondence: shin8409@ms6.hinet.net or cdma2000@asia.edu.tw (H.-C.C.); allen.nubi@gmail.com (Y.-Y.D.); lcf@cyut.edu.tw (C.-F.L.)

Received: 29 April 2019; Accepted: 27 June 2019; Published: 8 August 2019

Abstract: Presently, E-commerce has developed rapidly as a result of many services and applications integrating e-commerce technologies offered online. Buyers can buy goods online and sellers can then deliver the goods to them. Logistics therefore plays an important role in online e-commerce applications, with a focus on rapid delivery, the integrity of goods, and the privacy of personal information. Previous studies have proposed secure mechanisms for the transfer of electronic cash and digital content, in which only the sender and the receiver know the secret information hidden in the signature. However, they did not consider requirements such as the anonymous and lightweight verification in the logistics architecture. Therefore, this study designs a secure logistics system, with anonymous and lightweight verification, in order to meet the following requirements: Mutual authentication, non-repudiation, anonymity, integrity and a low overhead for the logistics environment. A buyer could check the goods and know if the parcel has been exchanged by a malicious person. Moreover, the proposed scheme not only presents a solution to meet the logistics system's requirements, but also to reduce both computational and communication costs.

Keywords: mutual authentication; privacy; logistics system; ECC; ban logic

1. Introduction

Background

In recent years, with the rapid development of e-commerce, online shopping has become a current trend and many shopping and financial transactions can now be completed via online shopping. These activities include online orders and online payments [1]. As buyers and sellers interact online, the purchase of goods is divided into digital and physical products. If a product is physical, the seller will entrust their logistics to deliver the goods to the buyer. As these logistics requirements grow, greater focus is required, not only on rapid delivery, but also on ensuring the integrity of goods and the privacy of personal information [2–7].

Unfortunately, the current process of goods delivery and online shopping does not entail an immediate physical exchange of goods. There is therefore a risk of counterfeiting and fraud, in addition

to a risk that goods may be lost due to human error, and this may be compounded by information errors, which could mean that it cannot be determined where the goods were lost. In 2016, Liu and Wang [6] noted that the means of preventing the loss of goods has become a very important issue in this field.

However, during the goods transportation process, the logistics provider will copy both the buyer and seller's personal information on an order detail and paste the order detail on the packages. That is, the goods can only be accurately delivered to the buyer, but this process includes the risk of private personal information being leaked, which may result in improper use or theft of that personal information. The delivery verification can also include the risks of identity impersonation, parcel exchange, and the loss of packages. Since there is no reliable mechanism for the buyer and seller to identify each other, it is impossible to know who has the goods or when goods are lost.

In 2006, Aijaz et al. [1] classified various attacker behaviors as active and passive attackers, internal and external personnel, and malicious and rational attackers. Active attackers tamper with shopping information, while passive attackers do not actively participate in tampering with information, but rather eavesdrop on shopping information. The stolen information may then be forwarded to other attackers. Internal attackers are very dangerous in the transmission process. As a consequence of their good understanding of items and personal information, internal personnel can cause various kinds of complex attacks. External personnel are not members of the transaction process, so they are much less harmful than internal personnel. The main goal of malicious attackers is to steal or tamper with information and cause the loss of property.

This paper proposes a logistics method using the public key crypto system to protect the personal privacy and the shopping information of buyers, sellers, and logistics companies during the transmission process to prevent information from being stolen. In addition, lightweight encryption technology is used to protect personal tag information to prevent personal information from being leaked during the delivery process.

In 2016, Liu and Wang [6] published papers on an NFC-based security-enhanced express delivery systems, in which the individuals' personal information was hidden in tags and only authorized people could get permission to access that information, thus protecting personal information from being stolen and achieving fast identity authentication. Digital signatures are then used by buyers, sellers, and logistics companies to achieve non-repudiation. The proposed system thus achieves mutual authentication, lightweight and fast verification, cost savings, the anonymity of personal information, non-repudiation in the transaction, and the completeness of the product.

The remainder of this paper is arranged as follows. Section 2 presents the system architecture. Section 3 presents the proposed secure package logistics system, based on protecting personal information anonymously by tag. Section 4 presents a security analysis and then illustrates the computation cost, communication cost, and performance analysis of the proposed scheme. Section 5 offers conclusions.

2. Related Works and Requirement

2.1. Related Works

In 2016, Liu and Wang noted that digital tags may not be able to perform complex encryption and decryption operations due to computation limitations [6]. In general, current logistics schemes lack face to face package checking procedures and rely on buyers to ensure that packages are intact upon receipt. In addition, the security issues of RFID systems are not completely suitable for the scheme proposed in this study [8]. Instead, this study uses ECC (elliptic curve cryptography) to generate session keys that are used to secure data transmissions and the BAN logic model [9] to prove the correctness of the proposed scheme with mutual authentication. Recently, many authentication schemes have applied BAN logic to prove the correctness of authentication and key establishment. The following is the notation of BAN logic.

$P\|\equiv X$	P believes X, or P would be entitled to believe X.
$P \lhd X$	P sees X. Someone has sent a message containing X to P, who can read and repeat X.
$P\| \sim X$	P once said X. P at some time sent a message including X.
$P\\|\Rightarrow X$	P has jurisdiction over X. P is an authority on X and should be trusted on this matter.
$< X >_Y$	This represents X combined with Y.
$\#(X)$	The formula X is fresh, that is, X has not been sent in a message at any time before the current run of the protocol.
$P \overset{K}{\leftrightarrow} Q$	P and Q may use the shared key K to communicate.
$P \overset{S}{\Leftrightarrow} Q$	The formula S is a secret known only to P and Q and possibly to principals trusted by them.

2.2. Requirements

In order to achieve a good logistics system, the following security requirements must be met and known attacks must be prevented:

(1) Mutual authentication: The basic requirement for good system communication is the identity authentication during the transmission process. The message must guarantee the validity of a sender and receiver [10,11].
(2) Non-repudiation: In the information transmission process, if each identity is not authenticated, the sender and the receiver are vulnerable to being sent false information by an impersonation attack. Therefore, the non-repudiation of information is crucial to effectively prevent impersonation [4,12].
(3) Anonymity: It is easy for buyer and seller to disclose information in the goods delivery process. Therefore, the contents should not disclose any information about the buyer and seller [13].
(4) Integrity: In an unencrypted environment, information is easily tampered with in the transmission process, resulting in the receiver being vulnerable to the information received not being that sent by the original sender's information. Therefore, the integrity of the information must be ensured during transmission [14].
(5) Low overhead: Identity verification in the information transmission process must ensure information integrity and maintain transmission speed, so reduced computation is necessary for a faster system [15,16].

There are several common malicious attack patterns that can target package logistic systems [15,17–19], as follows:

(1) Modification attack: The attacker intercepts the information of the transmitting party and the receiving party, and modifies the contents of the shopping information, resulting in the loss of the transmitting party and the receiving party. Therefore, the transmitted information must be secure against modification in order to prevent such attacks.
(2) Impersonation attack: The attacker uses a fake identity to disguise themselves as a sender and sends a fake message to the receiver, causing the receiver to receive a false message.
(3) Man-in-the-middle-attack: The attacker establishes independent contact with both ends of the communication and exchanges the information so that both sender and receiver of the communication think that they are talking directly with each other through a private connection. In fact, the entire conversation is completely controlled by the attacker. In a man-in-the-middle attack, an attacker can intercept calls from both parties and insert new content.
(4) Clone attack: An attacker steals items by copying a label and impersonating a deliverer to deliver a non-original item.

3. The Proposed Scheme

3.1. System Architecture

The system consists of the following parties: Seller (S), logistics (L), buyer (B), and deliverer (D). The architecture and information flow are shown in Figure 1. The four parties in the scheme, in detail, are the following:

(1) Seller: An online shopping store. People can shop there and the seller sends the goods to the buyer, who will sign for the delivered package.
(2) Logistics: A company entrusted to deliver the packages to the buyer.
(3) Deliverer: The logistics employee. They assist the logistics company to deliver the package to the buyer.
(4) Buyer: Someone who buys something from the seller and who signs for the delivered package.

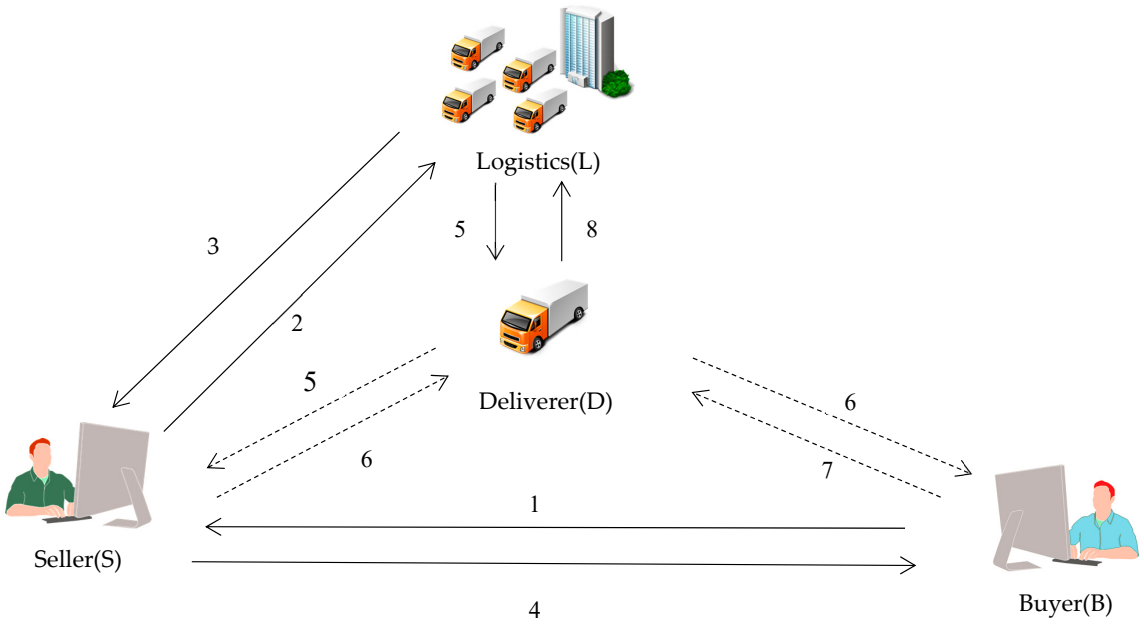


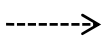
Figure 1. Logistics system architecture.

The eight steps in the scheme, in detail are as follows:

(1) The buyer requests a product from the seller.
(2) The seller provides the buyer and seller's information to the logistics.
(3) The logistics generates the transaction number and sends the buyer's tag to the seller.
(4) The seller sends the transaction number and the buyer's tag to the buyer.
(5) The logistics gives the tag of the seller's information to the deliverer. The deliverer goes to the seller's home and sends his/her identity to the seller.
(6) The seller verifies the deliverer's identity. The seller then transmits their signature and gives the goods and the buyer's tag to the deliverer. The deliverer goes to the buyer's house and sends his/her identity to the buyer.
(7) The buyer transmits their signature to the deliverer.
(8) The deliverer brings the buyer and the seller's signature back to the logistics to verify the signature and complete the transaction.

3.2. Notations

The notations used in this paper are listed below:

ID_X	Identification of X
M_X	X's address and telephone information
$M_{Product}$	Product information
TID	Transaction number
$Tag_{X,Y}$	The tag used for X to Y
P_{ukX},P_{rkX}	The public key and private key of X, respectively
$Sig_{X,Y}$	The signature for X to Y
C_i	The ith ciphertext
P	Base point
SK_{XY}	Session key between X and Y
$E_{SK_{XY}}(M)$	Encrypt message M with session key SK_{XY}
$D_{prkX}(M)$	Decrypt message M with session key SK_{XY}
$S_{prkX}(M)$	Sign message M with X's private key prk_X
$V_{pukX}(M)$	Verify message M with X's public key puk_X
$E_{pukX}(M)$	Encrypt message M with X's public key puk_X
$D_{prkX}(M)$	Decrypt message M with X's private key prk_X
$h(M)$	The message M calculated by one-way hash function
$\oplus$	Exclusive-or operation for any two operands with same binary size
$\|\|$	Concatenation operator
$A \overset{?}{=} B$	Determine if A is equal to B
	A secure channel
	An insecure channel

3.3. Initialization Phase

During the initialization phase, the Certificate Authority (CA) issues the public key and private key, and selects a large prime, P, and elliptic curve, E, over a finite field for each party.

3.4. Session Key Generation Phase and Order Request Phase

In the session key generation phase and order request phase, the buyer provides shopping information to the seller. The seller sends the buyer and the seller's information to the logistics and asks for the goods to be delivered. The logistics generates the transaction number and the tag for the seller and sends the transaction numbers to the buyer. Figure 2 presents the session key generation and order request phase of the proposed scheme.

Step 1: The buyer selects a random r_B and computes R_B as follows:

$$R_B = r_B{*}P, \tag{1}$$

The buyer signs the (R_B,ID_B) with the private key Prk_B, as follows:

$$Sig_{BS} = S_{prkB}(R_B,ID_B), \tag{2}$$

The buyer then sends (R_B,ID_B,Sig_{BS}) to the seller.

Step 2: The seller selects a random number r_S and then computes R_S and signs the (R_S,ID_S) with the private key Prk_S, as follows:

$$R_S = r_S{*}P, \tag{3}$$

$$Sig_{SL} = S_{prkS}(R_S, ID_S). \tag{4}$$

The seller then sends (R_S,ID_S,Sig_{SL}) to logistics. The seller then verifies the Sig_{BS} with the public key Puk_B to determine whether the signagture is legal or not, as follows:

$$V_{pukB}(Sig_{BS}) \stackrel{?}{=} (R_B, ID_B). \tag{5}$$

If it passes the verification, the seller computes session key SK_{BS}, as follows:

$$SK_{BS} = h((r_s{*}R_B)||ID_B||ID_S), \tag{6}$$

uses the SK_{BS} to encrypt (R_B, ID_B) with SK_{BS}, as follows:

$$C_1 = E_{SK_{BS}}(R_B, ID_B), \tag{7}$$

and signs the (R_S,ID_S) with the private key Prk_S, as follows:

$$Sig_{SB} = S_{prkS}(R_S, ID_S), \tag{8}$$

The seller then sends (R_S, ID_S,C_1,Sig_{SB}) to the buyer.

Step 3: The logistics selects a random number r_L, and computes R_L, as follows:

$$R_L = r_L{*}P. \tag{9}$$

Logistics then verifies the Sig_{SL} with the public key Puk_S to determine whether the signagture is legal or not, as follows:

$$V_{pukS}(Sig_{SL}) \stackrel{?}{=} (R_S, ID_S), \tag{10}$$

If it holds, logistics computes session key SK_{SL}, as follows:

$$SK_{SL} = h((r_L{*}R_S)||ID_S||ID_L). \tag{11}$$

Then the logistics encrypts (R_S,ID_S) with SK_{SL}, as follows:

$$C_3 = E_{SK_{SL}}(R_S, ID_S). \tag{12}$$

Next, logistics signs the (R_L,ID_L) with the private key Prk_L, as follows:

$$Sig_{LS} = S_{prkL}(R_L,ID_L), \tag{13}$$

and sends (R_L,ID_L,C_3,Sig_{LS}) to the seller.

Step 4: The buyer verifies the Sig_{SB} with the public key Puk_S to determine whether the signagture is legal or not, as follows:

$$V_{pukS}(Sig_{SB}) \stackrel{?}{=} (R_S, ID_S). \tag{14}$$

The buyer then computes session key SK_{BS}, as follows:

$$SK_{BS} = h((r_B{*}R_S)||ID_B||ID_S), \tag{15}$$

and uses the SK_{BS} to decrypt C_1, as follows:

$$(R_B{*}, ID_B{*}) = D_{SK_{BS}}(C_1), \tag{16}$$

and determines whether (R_B,ID_B) is equal or not, as follows:

$$(R_B, ID_B) \stackrel{?}{=} (R_B, ID_B){*}. \tag{17}$$

The seller then encrypts $(R_S,ID_S,ID_B,M_B,M_{product})$ with SK_{BS}, as follows:

$$C_2 = E_{SK_{BS}}\left(R_S, ID_S, ID_B, M_B, M_{product}\right), \tag{18}$$

Then buyer then sends (ID_B,C_2) to the seller.

Step 5: The seller decrypts C_2 with SK_{BS}, as follows:

$$\left(R_S{*}, ID_S{*}, ID_B, M_B, M_{product}\right) = D_{SK_{BS}}(C_2), \tag{19}$$

and then gets $(R_S{*},ID_S{*})$, and determines whether (R_S,ID_S) is equal or not, as follows:

$$(R_S, ID_S) \stackrel{?}{=} (R_S{*}, ID_S{*}). \tag{20}$$

The seller verifies the Sig_{LS} with the public key Puk_L to determine whether the signagture is legal or not, as follows

$$V_{pukL}(Sig_{LS}) \stackrel{?}{=} (R_L, ID_L). \tag{21}$$

If it passes the verification, the seller computes SK_{SL}, as follows:

$$SK_{SL} = h((r_S{*}R_L)||ID_S||ID_L), \tag{22}$$

and decrypts C_3 with SK_{SL}, as follows:

$$(R_S{*}, ID_S) = D_{SK_{SL}}(C_3). \tag{23}$$

The seller gets $(R_S{*},ID_S{*})$, determines whether (R_S,ID_S) is equal or not, as follows:

$$(R_S, ID_S) \stackrel{?}{=} (R_S{*}, ID_S{*}), \tag{24}$$

If it holds, the seller encrypts $(R_L,ID_L,ID_S,M_S,ID_B,M_B)$ with SK_{SL}, as follows:

$$C_4 = E_{SK_{SL}}(R_L, ID_L, ID_S, M_S, ID_B, M_B), \tag{25}$$

and then sends (ID_S,C_4) to logistics.

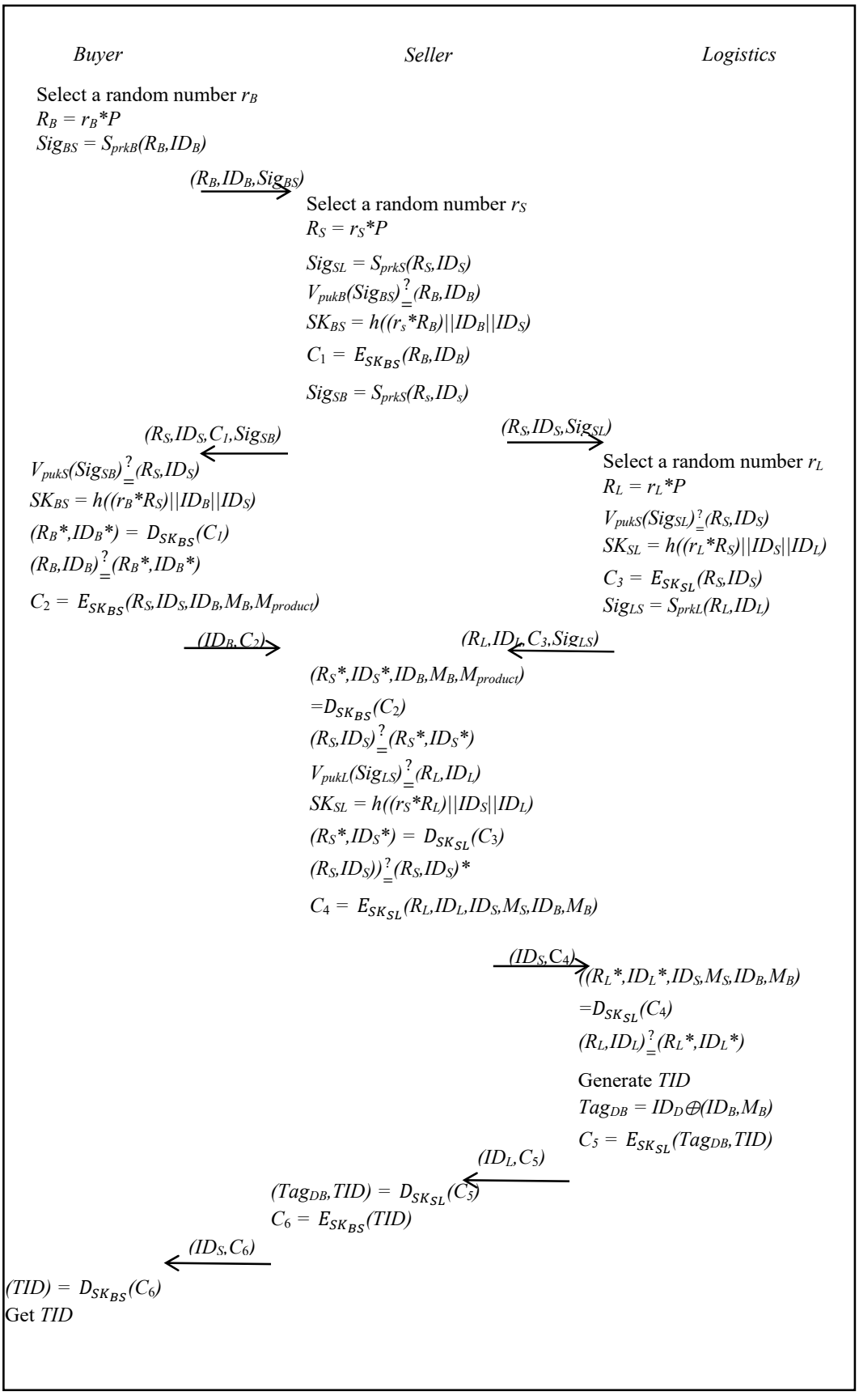


Figure 2. Session key generation and order request phase.

Step 6: The logistics decrypts C_4 with SK_{SL}, as follows:

$$(R_L*, ID_L*, ID_S, M_S, ID_B, M_B) = D_{SK_{SL}}(C_4), \tag{26}$$

and then gets (R_L*, ID_L*) and determines whether (R_L, ID_L) is equal or not, as follows:

$$(R_L, ID_L) \stackrel{?}{=} (R_L*, ID_L*), \tag{27}$$

Logistics generates *TID* and $Tag_{DB,}$ and computes the following:

$$Tag_{DB} = ID_D \oplus (ID_B, M_B). \tag{28}$$

and then uses the SK_{SL} to encrypt (Tag_{DB}, TID), as follows:

$$C_5 = E_{SK_{SL}}(Tag_{DB}, TID), \tag{29}$$

then sends (ID_L, C_5) to the seller.

Step 7: The seller decrypts C_5 with SK_{SL}, as follows:

$$(Tag_{DB}, TID) = D_{SK_{SL}}(C_5). \tag{30}$$

The seller encrypts *(TID)* with SK_{BS}, as follows:

$$C_6 = E_{SK_{BS}}(TID), \tag{31}$$

then sends (IDS,C6) to the buyer.

Step 8: The buyer decrypts C6 with SKBS, as follows:

$$TID = D_{SK_{BS}}(C_6), \tag{32}$$

and then gets *TID*.

3.5. Package Collection Phase

The logistics sends the tag containing the seller information to the deliverer. The deliverer decrypts the tag and goes to the seller's house. After verifying the delivery identity, the seller transmits their signature to give the goods and the buyer's tag to the deliverer. The package collection phase is illustrated in Figure 3.

Step 1: The logistics signs (ID_D, ID_L, TID) with private key Prk_L, as follows:

$$Sig_{LS} = S_{prkL}(ID_D, ID_L, TID), \tag{33}$$

The logistics uses SK_{SL} to encrypt (ID_D, ID_L, TID), as follows:

$$C_7 = E_{SK_{SL}}(ID_D, ID_L, TID), \tag{34}$$

then generates Tag_{DS}, as follows:

$$Tag_{DS} = ID_D \oplus (ID_S, M_S), \tag{35}$$

and sends $(ID_L, Tag_{DS}, C_7, Sig_{LS})$ to the deliverer.

Step 2: The deliverer computes the following formula:

$$(ID_S, M_S) = Tag_{DS} \oplus ID_D, \tag{36}$$

and the deliverer can then get (ID_S, M_S).

Step 3: The deliverer sends *(IDD,IDL,TagDS,C7,SigLS)* to the seller for verification and the seller computes *IDD** as follows:

$$ID_D^* = Tag_{DS} \oplus (ID_S, M_S), \tag{37}$$

and verifies whether ID_D is equal or not, as follows:

$$ID_D \stackrel{?}{=} ID_D. \tag{38}$$

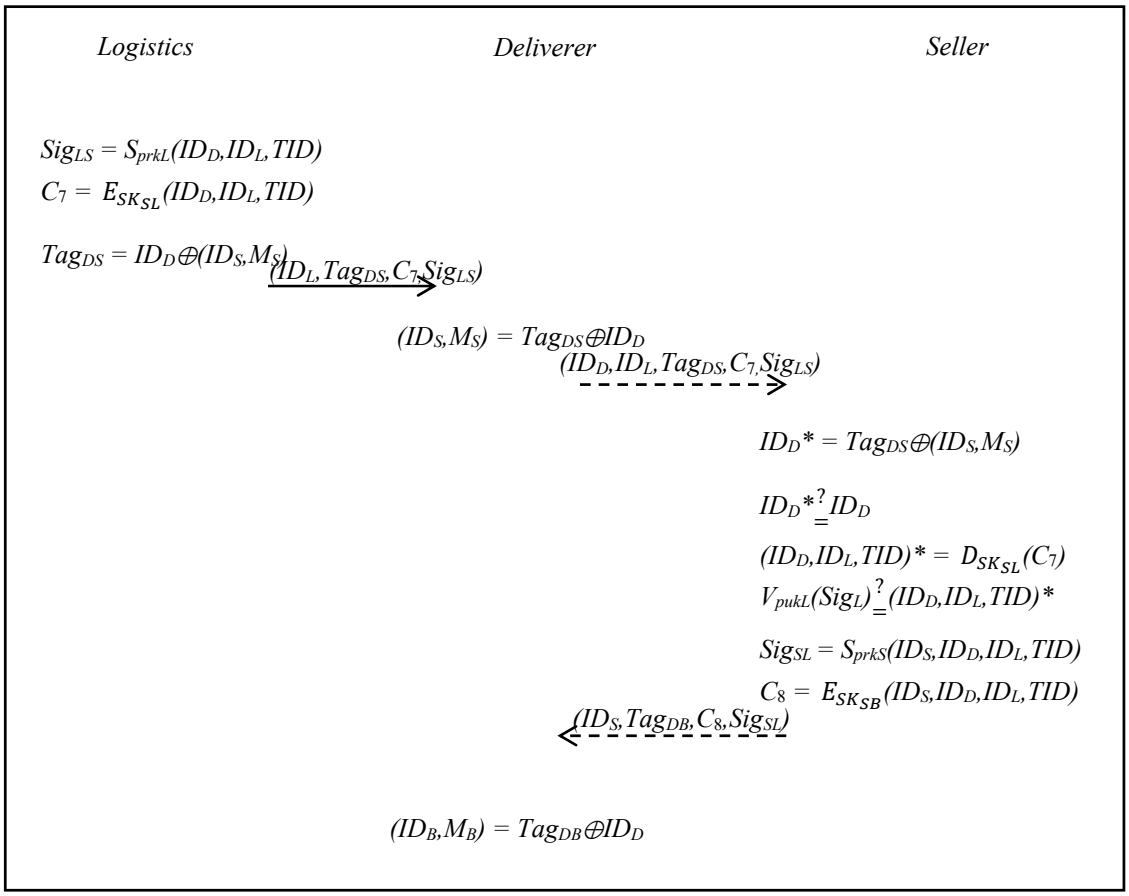


Figure 3. Package collection phase of the proposed scheme.

The seller decrypts C_7 with SK_{SL}, as follows:

$$(ID_D, ID_L TID)* = D_{SK_{SL}}(C_7). \tag{39}$$

The seller verifies the Sig_{LS} with the public key Puk_L to determine whether the signagture is legal or not, as follows:

$$V_{pukL}(Sig_{LS}) \stackrel{?}{=} (ID_D, ID_L, TID)*. \tag{40}$$

If it passes the verification, the seller signs the (ID_S,ID_D,ID_L,TID) with the private key Prk_S, as follows:

$$Sig_{SL} = S_{prkS}\ (ID_S, ID_D,ID_L,TID), \tag{41}$$

and uses SK_{SB} to encrypt (ID_S, D_D, ID_L,TID), as follows:

$$C_8 = E_{SK_{SB}}(ID_S, ID_D, ID_L, TID). \tag{42}$$

The seller then gives the goods and $(ID_S,Tag_{DB},C_8,Sig_{SL})$ to the deliverer.

Step 4: The deliverer computes as following formula:

$$(ID_B,M_B) = Tag_{DB} \oplus ID_D, \tag{43}$$

and gets (ID_B,M_B).

3.6. Product Transfer Phase

The deliverer decrypts the tag and sends the goods to the buyer's address. After verifying the deliverer's identity, the buyer obtains the goods and sends a signature to the deliverer. The deliverer takes the signatures of the buyer and the seller. The deliverer then returns to the logistics for confirmation and completes the transaction. The product transfer phase is illustrated in Figure 4.

Step 1: The deliverer sends the goods and (ID_D, Tag_{DB}, C_8) to the buyer to verify the identity, using the following formula:

$$ID_D{}^* = Tag_{DB} \oplus (ID_B,M_B), \tag{44}$$

Once the deliverer has $ID_D{}^*$, they determine whether the ID_D is equal or not, as follows:

$$ID_D{}^* \overset{?}{=} ID_D. \tag{45}$$

The buyer decrypts C_8 with SK_{SB}, as follows:

$$(ID_S, ID_D, ID_L, TID) = D_{SK_{SB}}(C_8), \tag{46}$$

and then gets TID^* and determines whether the TID, which is stored in the session key generation and order request phase, is equal or not, as follows:

$$TID^* \overset{?}{=} TID. \tag{47}$$

The deliverer uses Prk_B to sign $(ID_B,ID_S,ID_D,ID_L,TID)$, as follows:

$$Sig_{BL} = S_{prkB}(ID_B,ID_S,ID_D,ID_L,TID), \tag{48}$$

The buyer sends (Sig_{BL}, ID_B) to the deliverer.

Step 2: The deliverer returns to the logistics. Logistics verifies Sig_S with public key Puk_S, as follows:

$$V_{pukS}(Sig_{SL}) \overset{?}{=} (ID_S, ID_D, ID_L, TID), \tag{49}$$

and then determines whether the signagture is legal or not. Logistics verifies Sig_B with public key Puk_B, as follows:

$$V_{pukB}(Sig_{BL}) \overset{?}{=} (ID_B, ID_S, ID_D, ID_L, TID), \tag{50}$$

and determines whether the signagture is legal or not.

If it passes the verification, the transaction is completed.

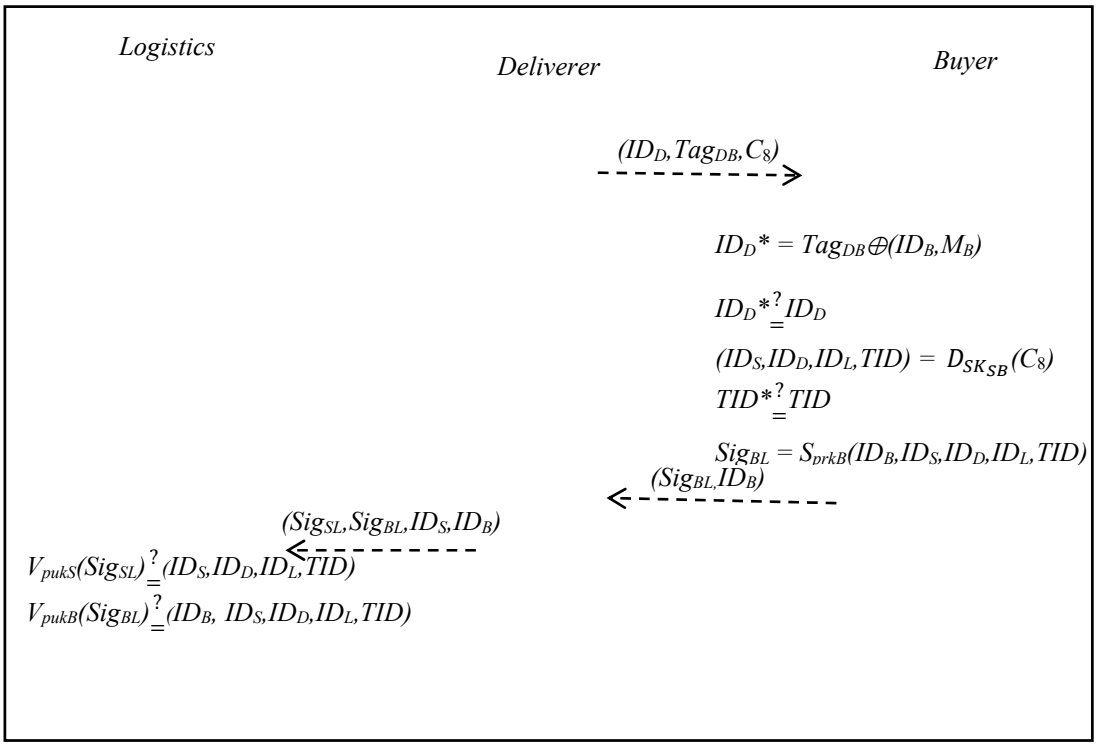


Figure 4. Product transfer phase of the proposed scheme.

4. Security Analysis and Discussion

4.1. Mutual Authentication Issue

This study uses BAN logic to prove that the proposed scheme achieves mutual authentication in each phase. In the session key generation and order request phases of the proposed scheme, the main goal is to determine whether the data has been modified between the buyer and seller, or the seller and the logistics provider.

The notation of BAN logic is described below:

$P \mid \equiv X$	*P believes X, or P would be entitled to believe X.*
$P \lhd X$	*P sees X, someone has sent a message containing X to P, who can read and repeat X.*
$P \mid \sim X$	*P once said X. P at some time sent a message including X.*
$P \mid \stackrel{K}{\rightarrow} X$	*P has X as a public key.*
$P \stackrel{k}{\leftrightarrow} X$	*P and X may use the session key K to communicate*
$P \mid \Rightarrow X$	*P has jurisdiction over x.*
$\#(X)$	*The formula X is fresh.*
$\{X\}_K$	*The formula X encrypted by K.*

The main goals of the scheme must be achieved in order to verify that the transmitted data has not been modified between buyer and seller, or between the seller and the logistics provider. These goals are listed below:

$G1$ $S|\equiv S \overset{SK_{BS}}{\leftrightarrow} B$
$G2$ $S|\equiv B|\equiv S \overset{SK_{BS}}{\leftrightarrow} B$
$G3$ $B|\equiv S \overset{SK_{BS}}{\leftrightarrow} B$
$G4$ $B|\equiv B|\equiv S \overset{SK_{BS}}{\leftrightarrow} B$
$G5$ $S|\equiv S \overset{SK_{SL}}{\leftrightarrow} L$
$G6$ $S|\equiv L|\equiv S \overset{SK_{SL}}{\leftrightarrow} L$
$G7$ $L|\equiv S \overset{SK_{SL}}{\leftrightarrow} L$
$G8$ $L|\equiv S|\equiv S \overset{SK_{SL}}{\leftrightarrow} L$
$G9$ $S|\equiv ID_B$
$G10$ $S|\equiv B|\equiv ID_B$
$G11$ $B|\equiv ID_S$
$G12$ $B|\equiv S|\equiv ID_S$
G11 $L|\equiv ID_S$
G12 $L|\equiv S|\equiv ID_S$
G11 $S|\equiv ID_L$
G12 $S|\equiv L|\equiv ID_L$

According to the purchase phase, BAN logic is used to produce an idealized form, as follows:

$M1$ $(\{R_B, ID_B\}prk_B, \{R_S, ID_S, ID_B, M_B, M_{product}\}SK_{BS})$,
$M2$ $(\{R_S, ID_S\}prk_S, \{R_B, ID_B\}SK_{BS})$,
$M3$ $(\{R_S, ID_S\}prk_S, \{R_L, ID_L, ID_S, M_S, ID_B, M_B\}SK_{SL})$,
$M4$ $(\{R_L, ID_L\}prk_L, \{R_S, ID_S\}SK_{BS})$.

In order to analyze the proposed improved scheme, this study makes the following assumptions:

$A1$ $S|\equiv \#(R_B)$
$A2$ $B|\equiv \#(R_B)$
$A3$ $S|\equiv \#(R_S)$
$A4$ $B|\equiv \#(R_S)$
$A5$ $L|\equiv \#(R_S)$
$A6$ $S|\equiv \#(R_S)$
$A7$ $L|\equiv \#(R_L)$
$A8$ $S|\equiv \#(R_L)$
$A9$ $S|\equiv \#SK_{BS}$
$A10$ $B|\equiv \#SK_{BS}$
$A11$ $L|\equiv \#SK_{SL}$
$A12$ $S|\equiv \#SK_{SL}$
$A13$ $B|\equiv |\overset{pubB}{\rightarrow} S$
$A14$ $S|\equiv |\overset{pubB}{\rightarrow} S$
$A15$ $B|\equiv |\overset{pubS}{\rightarrow} B$
$A16$ $S|\equiv |\overset{pubS}{\rightarrow} B$
$A17$ $L|\equiv |\overset{pubS}{\rightarrow} L$
$A18$ $S|\equiv |\overset{pubS}{\rightarrow} L$
$A19$ $L|\equiv |\overset{pubL}{\rightarrow} S$
$A20$ $S|\equiv |\overset{pubL}{\rightarrow} S$
$A21$ $S|\equiv B|\Rightarrow S \overset{SK_{BS}}{\leftrightarrow} B$
$A22$ $B|\equiv S|\Rightarrow S \overset{SK_{BS}}{\leftrightarrow} B$

$A23$ $L|\equiv S|\Rightarrow S \overset{SK_{SL}}{\leftrightarrow} L$
$A24$ $S|\equiv L|\Rightarrow S \overset{SK_{SL}}{\leftrightarrow} L$
$A25$ $S|\equiv B|\Rightarrow ID_B$
$A26$ $B|\equiv S|\Rightarrow ID_S$
$A27$ $L|\equiv S|\Rightarrow ID_S$
$A28$ $S|\equiv L|\Rightarrow ID_L$

According to these assumptions and the rules of BAN logic, this study shows the session key generation and order request phases of the proposed scheme as follows:

a. Seller S authenticates Buyer B By $M1$ and the seeing rule, derive the following:

$$S \triangleleft (\{R_B, ID_B\}prk_B, \{R_S, ID_S, ID_B, M_B, M_{product}\}SK_{BS}). \quad \text{(Statement 1)}$$

By $A1$ and $A2$ and the freshness rule, derive the following:

$$S|\equiv \#(\{R_B, ID_B\}prk_B, \{R_S, ID_S, ID_B, M_B, M_{product}\}SK_{BS}). \quad \text{(Statement 2)}$$

By (Statement 1), $A9$, $A13$, and $A14$ and the message meaning rule, derive the following:

$$S|\equiv B|\sim \#(\{R_B, ID_B\}puk_B, \{R_S, ID_S, ID_B, M_B, M_{product}\}SK_{BS}). \quad \text{(Statement 3)}$$

By (Statement 2), (Statement 3), and the verification rule, derive the following:

$$S|\equiv B|\equiv (\{R_B, ID_B\}puk_B, \{R_S, ID_S, ID_B, M_B, M_{product}\}SK_{BS}. \quad \text{(Statement 4)}$$

By (Statement 4) and the belief rule, derive the following:

$$S| \equiv B| \equiv S \overset{SK_{BS}}{\leftrightarrow} B. \quad \text{(Statement 5)}$$

By (Statement 5), $A21$, and the jurisdiction rule, derive the following:

$$S| \equiv S \overset{SK_{BS}}{\leftrightarrow} B. \quad \text{(Statement 6)}$$

By (Statement 6) and the belief rule, derive the following:

$$S|\equiv B|\equiv ID_{B.} \quad \text{(Statement 7)}$$

By (Statement 7), $A25$, and the belief rule, derive the following:

$$S|\equiv ID_B. \quad \text{(Statement 8)}$$

b. Buyer B authenticates Seller S By $M2$ and the seeing rule, derive the following:

$$B \triangleleft (\{R_S, ID_S\}prk_S, \{R_B, ID_B\}SK_{BS}). \quad \text{(Statement 9)}$$

By $A3$, $A4$, and the freshness rule, derive the following:

$$B\ |\equiv \#(\{R_S, ID_S\}prk_S, \{R_B, ID_B\}SK_{BS}). \quad \text{(Statement 10)}$$

By (Statement 9), $A10$, $A15$, $A16$, and the message meaning rule, derive the following:

$$B|\equiv S|\sim \#(\{R_S, ID_S\}puk_S, \{R_B, ID_B\}SK_{BS}). \quad \text{(Statement 11)}$$

By (Statement 10), (Statement 11) and the verification rule, derive the following:

$$B|\equiv S|\equiv(\{R_S,ID_S\}prk_S,\{R_B,ID_B\}SK_{BS}). \quad \text{(Statement 12)}$$

By (Statement 12) and the belief rule, derive the following:

$$B| \equiv S| \equiv S \overset{SK_{BS}}{\leftrightarrow} B. \quad \text{(Statement 13)}$$

By (Statement 13), $A22$ and the jurisdiction rule, derive the following:

$$B| \equiv S \overset{SK_{BS}}{\leftrightarrow} B. \quad \text{(Statement 14)}$$

By (Statement 14) and the belief rule, derive the following:

$$B|\equiv S|\equiv IDS \quad \text{(Statement 15)}$$

By (Statement 15), $A26$ and the belief rule, derive the following:

$$B|\equiv ID_S. \quad \text{(Statement 16)}$$

By (Statement 6), (Statement 8), (Statement 14), and (Statement 16), it is proved that buyer B and seller S authenticate each other in the proposed scheme. The seller authenticates the buyer by (5). If it passes the verification, the seller authenticates the legality of the buyer and then the buyer authenticates the seller by (14).

c. Logistics L authenticates Seller S By $M3$ and the seeing rule, derive the following:

$$L\triangleleft(\{R_S,ID_S\}prk_S, \{R_L,ID_L,ID_S,M_S,ID_B,M_B\}SK_{SL}). \quad \text{(Statement 17)}$$

By $A5$, $A6$, and the freshness rule, derive:

$$L|\equiv\#(\{R_S,ID_S\}prk_S, \{R_L,ID_L,ID_S,M_S,ID_B,M_B\}SK_{SL}). \quad \text{(Statement 18)}$$

By (Statement 17), $A11$, $A17$, $A18$, and the message meaning rule, derive the following:

$$L|\equiv S|\sim\#(\{R_S,ID_S\}puk_S, \{R_L,ID_L,ID_S,M_S,ID_B,M_B\}SK_{SL}). \quad \text{(Statement 19)}$$

By (Statement 18), (Statement 19), and the verification rule, derive the following:

$$L|\equiv S|\equiv(\{R_S,ID_S\}puk_S, \{R_L,ID_L,ID_S,M_S,ID_B,M_B\}SK_{SL}). \quad \text{(Statement 20)}$$

By (Statement 20) and the belief rule, derive the following:

$$L| \equiv S| \equiv S \overset{SK_{BS}}{\leftrightarrow} B. \quad \text{(Statement 21)}$$

By (Statement 21), $A23$, and the jurisdiction rule, derive the following:

$$L| \equiv S \overset{SK_{BS}}{\leftrightarrow} B. \quad \text{(Statement 22)}$$

By (Statement 22) and the belief rule, derive the following:

$$L|\equiv S|\equiv ID_S. \quad \text{(Statement 23)}$$

By (Statement 23), *A*27, and the belief rule, derive the following:

$$L|\equiv ID_S. \quad \text{(Statement 24)}$$

d. Logistics *L* authenticates Seller *S* By *M*4 and the seeing rule, derive the following:

$$S\lhd(\{R_L,ID_L\}prk_L, \{R_S,ID_S\}SK_{BS}). \quad \text{(Statement 25)}$$

By *A*7, *A*8, and the freshness rule, derive the following:

$$S|\equiv\#(\{R_L,ID_L\}prk_L, \{R_S,ID_S\}SK_{BS}). \quad \text{(Statement 26)}$$

By (Statement 25), *A*12, *A*19, *A*20 and the message meaning rule, derive the following:

$$S|\equiv L|\sim\#(\{R_L,ID_L\}prk_L, \{R_S,ID_S\}SK_{BS}). \quad \text{(Statement 27)}$$

By (Statement 26), (Statement 27), and the verification rule, derive the following:

$$S|\equiv L|\equiv(\{R_L,ID_L\}prk_L, \{R_S,ID_S\}SK_{BS}). \quad \text{(Statement 28)}$$

By (Statement 28) and the belief rule, derive the following:

$$S| \equiv L| \equiv S \overset{SK_{SL}}{\leftrightarrow} L. \quad \text{(Statement 29)}$$

By (Statement 29), *A*24, and the jurisdiction rule, derive the following:

$$S| \equiv S \overset{SK_{SL}}{\leftrightarrow} L. \quad \text{(Statement 30)}$$

By (Statement 30) and the belief rule, derive the following:

$$S|\equiv L|\equiv ID_L. \quad \text{(Statement 31)}$$

By (Statement 31), *A*28, and the belief rule, derive the following:

$$S|\equiv ID_L. \quad \text{(Statement 32)}$$

By (Statement 22), (Statement 24), (Statement 30), and (Statement 32), it is proved that logistics L and seller S authenticate each other in the proposed scheme. The logistics authenticates the seller by (14): If it passes the verification, the logistics provider authenticates the legality of the seller and then the buyer authenticates the logistics as (21).

4.2. Non-Repudiation Issue

The proposed scheme uses digital signatures to achieve non-repudiation between the parties in each phase. The sender uses their private key to sign the transmitted message and then the receiver verifies the received message. The receiver uses their private key to sign the response message. Table 1 shows the non-repudiation of the proposed scheme.

Table 1. Non-repudiation of the proposed scheme.

Phase / Party	Proof	Issuer	Holder	Verification
Session key generation and order request phase	(R_B,ID_B)	Buyer	Seller	$V_{pukB}(Sig_{BS}) \stackrel{?}{=} (R_B,ID_B)$
	(R_S,ID_S)	Seller	Buyer	$V_{pukS}(Sig_{SB}) \stackrel{?}{=} (R_S,ID_S)$
	(R_S,ID_S)	Seller	Logistics	$V_{pukS}(Sig_{SL}) \stackrel{?}{=} (R_S,ID_S)$
	(R_L,ID_L)	Logistics	Seller	$V_{pukL}(Sig_{LS}) \stackrel{?}{=} (R_L,ID_L)$
Package collection phase	(ID_D,ID_L,TID,Sig_L)	Logistics	Seller	$V_{pukL}(Sig_L) \stackrel{?}{=} (ID_D,ID_L,TID)$
Product transfer phase	$(ID_S,ID_D,ID_L,TID,Sig_S)$	Seller	Buyer	$V_{pukS}(Sig_S) \stackrel{?}{=} (ID_S,ID_D,ID_L,TID)$
	$(ID_B,ID_S,ID_D,ID_L,TID,Sig_B)$	Buyer	Logistics	$V_{pukB}(Sig_B) \stackrel{?}{=} (ID_B,ID_S,ID_D,ID_L,TID)$

4.3. Anonymity Issue

All personal information, $Tag_{DS} = (ID_S,M_S) \oplus ID_D$ and $Tag_{DB} = (ID_B,M_B) \oplus ID_D$, is protected so that only the legal identities ID_D, ID_S, and ID_B can read the content. Therefore, the contents will not disclose any information about buyer or seller.

4.4. Low Overhead Issue

In the package collection phase and the product transfer phase, this study uses exclusive operation or encryption to quickly verify and reduce the verification cost. This study also uses session keys to substitute public key encryption to enhance calculation speed, thus meeting the low overhead requirement.

4.5. Data Integrity Issue

This study uses digital signatures to ensure data integrity. A malicious attack can be detected using digital signatures to verify the integrity of the data, even if an attacker has tampered with the transmitted data. Thus, attackers cannot tamper with the transmitted data without being detected. Therefore, the proposed scheme achieves data integrity.

4.6. Security Against Known Attacks

4.6.1. Modification Attack

In the information transmission process, encryption is performed using session keys, preventing the modification of transmitted data:

(1) The session key generation and order request phase is as follows:

$$C_1 = E_{SK_{BS}}(R_B,ID_B), \quad (7)$$
$$C_3 = E_{SK_{SL}}(R_S,ID_S), \quad (12)$$
$$C_2 = E_{SK_{BS}}(R_S,ID_S,ID_B,M_B,M_{product}), \quad (18)$$
$$C_4 = E_{SK_{SL}}(R_L,ID_L,ID_S,M_S,ID_B,M_B), \quad (25)$$
$$C_5 = E_{SK_{SL}}(Tag_{DB},TID), \quad (29)$$
$$C_6 = E_{SK_{BS}}(TID). \quad (31)$$

(2) Package collection phase:

$$C_7 = E_{SK_{SL}}(\mathrm{ID_D},\mathrm{ID_L},\mathrm{TID}), \quad (34)$$
$$C_8 = E_{SK_{SB}}(\mathrm{ID_S},\mathrm{ID_D},\mathrm{ID_L},\mathrm{TID}). \quad (42)$$

4.6.2. Impersonation Attack

In the session key generation and order request phase, package collection phase, and product transfer phase of information transmission, digital signatures cannot be disguised.

(1) The session key generation and order request phase is as follows:

$$Sig_{BS} = S_{prkB}(R_B, ID_B), \quad (2)$$
$$Sig_{SL} = S_{prkS}(R_S, ID_S), \quad (4)$$
$$Sig_{SB} = S_{prkS}(R_S, ID_S), \quad (8)$$
$$Sig_{LS} = S_{prkL}(R_L, ID_L). \quad (13)$$

(2) Package collection phase:

$$Sig_{SL} = S_{prkS}\ (ID_S, ID_D, ID_L, TID). \quad (41)$$

(3) Product transfer phase:

$$Sig_{BL} = S_{prkB}(ID_B, ID_S, ID_D, ID_L, TID), \quad (48)$$

4.6.3. Man-in-the-Middle Attack

The proposed scheme uses signature mechanisms $Sig_{BS} = S_{prkB}(R_B, ID_B)$, $Sig_{SL} = S_{prkS}(R_S, ID_S)$, and $Sig_{LS} = S_{prkL}(R_L, ID_L)$ to prevent modification of the R_B, R_S, and R_L, and uses those variables to generate session keys $SK_{BS} = h((r_s * R_B) || ID_B || ID_S)$ and $SK_{SL} = h((r_L * R_S) || ID_S || ID_L)$. The session key encryption/decryption offers security against man-in-the-middle attacks.

4.6.4. Clone Attack

In the package collection phase and the product transfer phase, the deliverer must give their own information, ID_D and Tag_{DS}, and the seller can then execute the exclusive-or operation or encrypt the Tag_{DS} and verify the identity of the deliverer $ID_D{}^* = Tag_{DS} \oplus (ID_S, M_S)$. In the product transfer phase of the proposed scheme, the deliverer must give their own information, ID_D and Tag_{DB}, and the buyer can then execute the exclusive-or operation or encrypt the Tag_{DB} and verify the identity of the deliverer $ID_D{}^* = Tag_{DB} \oplus (ID_B, M_B)$, thus preventing a clone attack.

4.7. Computation Cost

Table 2 shows the computation costs of the proposed scheme.

Table 2. Computation costs of the proposed scheme.

Party \ Phase	Buyer	Seller	Logistics	Deliverer
Session key generation and order request phase	$2T_{asy} + 3T_{sys} + 1T_h + 1T_{mul}$	$4T_{asy} + 6T_{sys} + 2T_h + 2T_{mul}$	$2T_{asy} + 3T_{sys} + 1T_h + 1T_{xor} + 1T_{mul}$	*N/A*
Package collection phase	*N/A*	$2T_{asy} + 2T_{sys} + 1T_{xor}$	$1T_{asy} + 1T_{sys} + 1T_{xor}$	$2T_{xor}$
Product transfer phase	$1T_{asy} + 1T_{sys} + 1T_{xor}$	*N/A*	$2T_{asy}$	*N/A*

Notes:

T_{asy} The time required for an asymmetrical signature/verifying a signature.
T_{sys} The time required for a symmetrical encryption/decryption operation.
T_h The time required for a one-way hash function.
T_{xor} The time required for an exclusive-or operation.
T_{mul} The time required for a multiplication operation.

In Table 2, the proposed scheme's computation costs are analyzed for the buyer, seller, logistics, and deliverer in each phase. Due to the insignificant comparison operation impacts, they are not considered. For the highest computation cost reduction in the session key generation and order request phase, a buyer needs three asymmetrical signatures/verifying a signature, three symmetrical encryption/decryption operations, one hash function operation, and one multiplication operation. A seller needs four asymmetrical signatures/verifying a signature, six symmetrical encryption/decryption operations, two hash function operations, and two multiplication operations. The logistics provider needs two asymmetrical signatures/verifying a signature, three symmetrical encryption/decryption operations, one hash function operation, one exclusive-or operation, and one multiplication operation.

4.8. Communication Cost

Table 3 shows the communication cost of the proposed scheme.

Table 3. Communication cost of the proposed scheme.

Phase / Party	Message Length	Round	3.5G (14 Mbps)	4G (100 Mbps)
Session key generation and order request phase	$4T_{sig} + 6T_{sys} = 4 \times 1024 + 6 \times 256 = 5632$ bits	8	5632/14000 = 0.402 ms	5632/100000 = 0.056 ms
Package collection phase	$3T_{sig} + 3T_{sys} + 3T_{xor} = 3 \times 1024 + 3 \times 256 + 3 \times 80 = 4080$ bits	3	4080/14000 = 0.291 ms	4080/100000 = 0.041 ms
Product transfer phase	$3T_{Sig} + 1T_{sys} + 1T_{xor} = 3 \times 1024 + 1 \times 256 + 1 \times 80 = 3408$ bits	3	4432/14000 = 0.243 ms	4432/100000 = 0.044 ms

Notes:

T_{sig} The time required to transmit a signature (1024 bits).
T_{sys} The time required to transmit a symmetric encryption/decryption ciphertext (256 bits).
T_{xor} The time required to transmit an exclusive-or operation (80 bits).

From Table 3, the communication cost of the proposed scheme during the transaction process of each phase was analyzed and, since other operations have little impact, they were not considered in the communication cost. For the highest communication cost reduction in the session key generation and order request phase, four signature operations and six symmetric encryption/decryption operations must be transmitted. It thus requires $1024 \times 4 + 256 \times 6 = 5632$ bits. In a 3.5G environment, the maximum transmission speed is 14 Mbps, which only takes 0.402 ms to transfer all messages. In a 4G environment, the maximum transmission speed is 100 Mbps and the transmission time is reduced to 0.056 ms (ITU 2016).

4.9. Storage Cost

Table 4 shows the storage cost of the proposed scheme.

Table 4. Storage cost of the proposed scheme.

Phase / Party	Buyer	Seller	Logistics	Deliverer
Session key generation and order request phase	$1T_{asy} + 1T_{sys} + 1T_h + 2T_{mul} + 4T_{other}$ = 2176 bits	$2T_{asy} + 3T_{sys} + 2T_h + 3T_{mul} + 5T_{other}$ = 4208 bits	$1T_{asy} + 2T_{sys} + 1T_h + 2T_{mul} + 7T_{other}$ = 2672 bits	*N/A*
Package collection phase	*N/A*	$1T_{asy} + 1T_{sys} + 5T_{other}$ = 1680 bits	$1T_{asy} + 1T_{sys} + 6T_{other}$ = 1760 bits	$1T_{other}$ = 80 bits
Product transfer phase	$5T_{other}$ = 400 bits	*N/A*	$1T_{asy} + 5T_{other}$ = 1424 bits	*N/A*

Notes:

T_{asy}	The space required to storage an asymmetrical signature (1024 bits).
T_{sys}	The space required to storage a symmetrical encryption/decryption ciphertext (256 bits).
T_h	The space required to storage a one-way hash function calculated message (256 bits).
T_{mul}	The space required to storage a multiplication calculated message (160 bits).
T_{other}	The space required to storage other messages (80 bits).

In Table 4, the storage cost of the proposed scheme was analyzed for the buyer, seller, logistics and deliverer in each phase. For the highest storage cost in the session key generation and order request phase, a seller needs two asymmetrical signatures storage space, three symmetrical encryption/decryption ciphertexts storage space, two one-way hash function calculated messages storage space, three multiplication calculated messages storage space, and five other messages storage space. It thus requires $1024 \times 2 + 256 \times 3 + 256 \times 2 + 160 \times 3 + 80 \times 5 = 4208$ bits storage space.

5. Conclusions

In recent years, e-commerce services have prospered and online shopping has become a current trend. The security of personal information exchanged when purchasing a product online has thus become an important issue. This paper proposes a tag-based protection of personal information and a non-repudiable logistics system. The proposed scheme can effectively provide the secure transmission of personal information transmitted by items.

In the session key generation and order request phases, digital signatures are used to transmit data from the sender to the receiver, which ensures that the data cannot be modified. In the package collection phase and product transfer phase, tags containing hidden personal information are used to prevent personal information being leaked and to speed up the verification of the deliverer for buyers and sellers. The proposed scheme offers a reduction of computation costs, compared to other related works. The logistics can use the proposed system to achieve non-repudiation and to complete transactions by examining the digital signatures of the buyer and seller.

(1) The process of communication between buyers and sellers is mutual authentication.
(2) The non-repudiation of the goods delivery process is achieved through the signature mechanism.
(3) Personal information protection is achieved through exclusive-or operations.
(4) Tags use lightweight authentication technology to reduce the computation cost, compared to related works.

Future work will include the payment flow and applying block-chain technology to track the stream of and to prevent the loss of goods.

Author Contributions: Supervision and methodology, C.-L.C.; writing—original draft, D.-P.L.; validation, Y.-Y.D.; surveyed related work, H.-C.C. and C.-F.L.

Funding: This research was funded by the Ministry of Science and Technology, Taiwan, ROC, under contract number MOST 108-2221-E-324-013.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Aijaz, A.; Bochow, B.; Dotzer, F.; Festag, A.; Gerlach, M.; Kroh, R.; Leinmuller, T. Attacks on inter vehicle communication systems—An analysis. In Proceedings of the 3rd International Workshop on Intelligent Transportation, Hamburg, Germany, 14–15 March 2006; pp. 189–194.
2. Burrows, M.; Abadi, M.; Needham, R. A logic of authentication. *ACM Trans. Comput. Syst.* **1990**, *8*, 18–36. [CrossRef]
3. Chen, C.L.; Chiang, M.L.; Peng, C.C.; Chang, C.H.; Sui, Q.R. A Secure Mutual Authentication Scheme with Non-repudiation for Vehicular Ad Hoc Networks. *Int. J. Commun. Syst.* **2015**, *30*, e3081. [CrossRef]
4. Cui, J.; She, D.; Ma, J.; Wu, Q.; Liu, J. A New Logistics Distribution Scheme Based on NFC. In Proceedings of the 2015 International Conference on Network and Information Systems for Computers, Wuhan, China, 23–25 January 2015; pp. 492–495.
5. Cho, J.-S.; Jeong, Y.-S.; Park, S. Consideration on the brute-force attack cost and retrieval cost: A hash-based radio-frequency identification (RFID) tag mutual authentication protocol. *Comput. Math. Appl.* **2015**, *69*, 58–65. [CrossRef]
6. Liu, S.; Wang, J. A Security-Enhanced Express Delivery System Based on NFC. In Proceedings of the 2016 13th IEEE International Conference on Solid-State and Integrated Circuit Technology, Hangzhou, China, 25–28 October 2016; pp. 1534–1536.
7. Speranza, M.G. Trends in transportation and logistics. *Eur. J. Oper. Res.* **2018**, *264*, 830–836. [CrossRef]
8. Gope, P.; Amin, R.; Hafizul Islam, S.K.; Kumar, N.; Bhalla, V.K. Lightweight and privacy-preserving RFID authentication scheme for distributed IoT infrastructure with secure localization services for smart city environment. *Future Gener. Comput. Syst.* **2018**, *83*, 629–637. [CrossRef]
9. Liang, K.; Susilo, W. Searchable attribute-based mechanism with efficient data sharing for secure cloud storage. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 1981–1992. [CrossRef]
10. Das, A.K.; Goswami, A. A robust anonymous biometric-based remote user authentication scheme using smart cards. *J. King Saud Univ. Comput. Inf. Sci.* **2015**, *27*, 193–210. [CrossRef]
11. Madhusudhan, R.; Hegde, M. Security bound enhancement of remote user authentication using smart card. *J. Inf. Secur. Appl.* **2017**, *36*, 59–68. [CrossRef]
12. Qi, M.; Chen, J. A fresh Two-party Authentication Key Exchange Protocol for Mobile Environment. In Proceedings of the International Conference on Industrial Technology and Management Science, Tianjin, China, 27–28 March 2015; Volume 30, pp. 933–936.
13. Ray, B.R.; Abawajy, J.; Chowdhury, M.; Alelaiwi, A. Universal and secure object ownership transfer protocol for the Internet of Things. *Future Gener. Comput. Syst.* **2017**, *78*, 838–849. [CrossRef]
14. Rajput, U.; Abbas, F.; Eun, H.; Oh, H. A Hybrid approach for Efficient Privacy-Preserving Authentication in VANET. *IEEE Access* **2017**, *5*, 12014–12030. [CrossRef]
15. Sharma, V.; Vithalkar, A.; Hashmi, M. Lightweight security protocol for chipless RFID in Internet of Things (IoT) applications. In Proceedings of the 2018 10th International Conference on Communication Systems & Networks (COMSNETS), Bengaluru, India, 3–7 January 2018; pp. 468–471.
16. Tu, Y.; Piramuthu, S. Lightweight non-distance-bounding means to address RFID relay attacks. *Decis. Support Syst.* **2017**, *102*, 12–21. [CrossRef]
17. Whitmore, A.; Agarwal, A.; Da, X.L. The internet of things: A survey of topics and trends. *Inf. Syst. Front.* **2015**, *17*, 261–274. [CrossRef]

18. Wang, J.; Floerkemeier, C.; Sarma, S.E. Session-based security enhancement of RFID systems for emerging open-loop applications. *Pers. Ubiquitous Comput.* **2014**, *18*, 1881–1891. [CrossRef]
19. Zhao, S.; Aggarwal, A.; Frost, R.; Bai, X. A survey of applications of identity-based cryptography in mobile ad-hoc networks. *IEEE Commun. Surv. Tutor.* **2012**, *14*, 380–400. [CrossRef]