Published in IET Information Security
Received on 4th December 2009
Revised on 26th January 2010
doi: 10.1049/iet-ifs.2009.0250

Special Issue on Multi-Agent & Distributed Information Security

ISSN 1751-8709

Digital product transaction mechanism for electronic auction environment

C.-T. Yen[1,2] *T.-C. Wu*[1,2] *M.-H. Guo*[3] *C.-K. Yang*[1] *H.-C. Chao*[4,5]

[1]*Department of Information Management, National Taiwan University of Science and Technology, Taipei, Taiwan*
[2]*Taiwan Information Security Center at NTUST, Taipei, Taiwan*
[3]*Department of Information Management, Shih-Hsin University, Taipei, Taiwan*
[4]*Department of Electronic Engineering, Institute of Computer Science and Information Engineering, National Ilan University, I-Lan, Taiwan*
[5]*Department of Electrical Engineering, National Dong Hwa University, Hualien, TaiwanHualien, Taiwan*
E-mail: hcc@niu.edu.tw

Abstract: The rapid development in electronic commerce and information technology drives the traditional physical product trading evolved to digital product trading. With the effect of the multi-agents system in the Internet environment and the promotions of Government, digital product industry grows fast. The authors proposed a digital product transaction mechanism for electronic auction in the multi-agents system environment. The research introduced a convenient platform to protect the privacies of both buyers and sellers, and track digital product further in an electronic auction environment. In addition, by using simple cryptography techniques supplemented with encryption, the authors ensure the security of information transactions, thereby providing a mechanism of safe and fair digital product electronic auction.

1 Introduction

Information technology provides a significant assistance to the evolution of human culture. As the ability of computer quickly improved, more information services are developed and upgraded. Among these modern applications and technologies, the intelligent multi-agents system plays an important role. In a multi-agent system, there are many intelligent agents distributed in the network. The agents with high information ability can make the electronic commerce become more widespread, and help the traditional physical product trading evolved to digital product trading more successful.

In the electronic commerce, albeit the auction of physical commodities has matured, there remain shortcomings concerning the issue of digital content product. Without substantial protection of digital content publication, the intellectual property right of digital content providers can be easily violated and digital content providers are apt to encounter further problems such as damage of property. Intellectual property right will be soundly protected and valued after digital product providers combined digital rights management (DRM) to solve illegal authorisation and distribution. This protection of right can indirectly encourage more authors to create and heighten the quality of product as well to facilitate the digital content market of electronic commerce (e-commerce).

Modes of online shopping can be classified into two main categories, which are physical and virtual stores. Physical product can be accessibly discussed and accepted through electronic auction. However, the mode of selling digital content publication through electronic auction is never carried out. The main reasons are there is no existing transaction mode of digital product, complex division and acquisition of intellectual property right, protecting mechanism of right management, and so on. Furthermore, the selling mode of electronic auction is completely different from that of the traditional physical commodities, including the differences of rights transfer, authorisation, tracking, and so on.

In order to provide a dependable trust, security and privacy environment for e-commerce, some proper security issues are

necessary. In this paper, we proposed the digital product transaction mechanism with DRM for electronic auction in the multi-agent system environment. The research contains the characteristics in using reliable cryptology system to protect digital contents when uploading, embedding digital fingerprints for tracking, arbitration and proposing a safe, fair e-auction mechanism of digital product.

The outline of this paper is organised as follows. In Section 2, we review the basic DRM model and electronic auction of physical commodities. In Section 3, we propose a new digital product transaction mechanism for electronic auction environment. In Section 4, an analysis of our mechanism and other related works are presented. Finally, the conclusion of this research is in Section 5.

2 Literature review

In this section, we will briefly introduce the basic DRM model and electronic auction of physical commodities. DRM consists of content provider, content distributor, consumer and clearinghouse [1]. Fig. 1 shows an example of DRM model, and the following are the operations explained as they are numbered in the figure:

1. Content provider uses a safe and reliable cryptography system to protect the digital contents which are going to issue.

2. Content provider sends the protected digital content to content distributor in order to distribute it.

3. Content provider sends the policies that are used and the decryption key of the digital content to clearinghouse.

4. Before consumer uses the protected digital content, he/she must have the legal license.

5. Consumer pays to clearinghouse in order to have the license of the digital content.

6. Clearinghouse transfers the license to consumer.

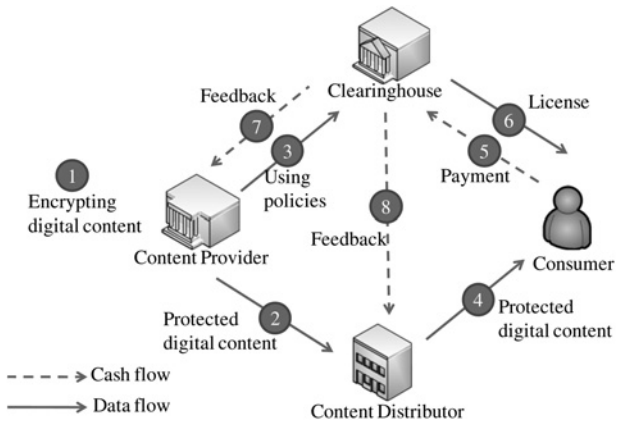

Figure 1 *DRM system operation model [1]*

7. Clearinghouse and content provider share the payment according to the contract agreement.

8. Clearinghouse and content distributor share the payment according to the contract agreement, too.

Recent studies on transmission of digital content focus on different ways. The first one is to study the rights file separating the model between digital content and its copyright [2–4]. Second, there are some researches related to authentication and tracking based on DRM [1, 5–10], while others studied e-cash [11–13], mobile environment [14, 15], digital rights language [16] and watermarking [17, 18]. The followings are introduction of related works.

Yang [4] proposed a transferable DRM system to solve the fair-use dispute. Moreover, he pointed out two new business models, including AV (Audio/Visual) rental shops and AV used product shops. However, there were some issues which were not mentioned in this research, such as the allocation of money, piracy, privacy, tracing and the electronic commerce following added-value extending.

Liaw *et al.* [6] proposed a secure and simple digital rights publication mechanism. This research was about payment and it solved the transaction of rights on the Internet. In addition, they supported flexible payment methods for each e-commerce. But if the transaction environment was changed, the way of purchase and acquisition will be altered as well. Therefore the above-mentioned details increase the efficiency of digital product and price competition.

The e-payment mechanism encouraged digital product providers to create high-quality digital content by using incentives proposed by Lin and Liu [13]. Moreover, it can rely on trusting the third party to identify the digital contents created by content providers. The above advantage is to increase accuracy and convenience of purchase. However, the core of this research lies not in the management of digital content product bought by consumers or product authorisation after being purchased, but in the protection of rights and tracking of privacy.

The mechanism proposed in this research protects digital content rights and sellers' privacy and avoiding malevolent distribution from buyers by inserting digital watermark, digital fingerprint and digital signature in the process of transaction. Although this mechanism protects digital content rights and further tracks digital product, it fails to consider the privacy of both parties in the process of transaction. Therefore applying anonymous transaction can protect both buyers and sellers from revealing identities in the networks.

Fair exchange and customers' anonymity are two crucial features of e-commerce transacting mode. The e-payment mechanism encourages digital content providers to create

high-quality digital content by using incentives proposed by Lin and Liu [13]. Moreover, it can rely on trusting the third party to identify the digital contents created by content providers. This mechanism enables a secure transaction by transacting digital content product with e-payment.

The above advantage is to increase the accuracy of purchase. However, this mechanism fails to protect digital content authors and their product with legal authorisation and application after digital product are purchased. In this research, consumers do not have proper management about the digital content product after they purchase, and they cannot protect the digital content by using whether authorisation or not. Moreover, the rights are unable to trace after rights authorising or transferring rights to consumers. The final goal of digital content product consists in security and fairness in the transaction of digital content product. Related works and comparisons of this topic are shown in Table 1.

3 Digital product transaction mechanism for electronic auction environment

3.1 System architecture

In this section, we will introduce a digital product transaction mechanism for electronic auction environment. The proposed mechanism is working on the platform constructed by the multi-agents system, and the system architecture is depicted in Fig. 2. Each role in the system fabric can be operated by the intelligent agent to improve the working performance, and the roles of the mechanism are explained as follows:

1. Bidder (BI): He/she bids the digital product provided and advertised by digital product auctioneer (PA).

2. Certificate authority (CA): It is a trusted third party and manages certificates in the proposal. The CA provides registration, authentication, certificates issuing, certificates revoking, certificates management and audit. It solves the argument between the buyer and the seller during an auction. Moreover, it issues the licenses of auctions, leases and appreciations.

3. Auction manager (AM): AM manages the valid BIs and the entire auction transactions. He also provides the storage service to save digital product uploaded by digital PA, and encrypted the digital product bided with the watermark.

4. Bank (BK): It is responsible for payment, but the details in payment process are not discussed in this research.

5. Digital PA: PA provides digital product (B2C, C2C) or resells digital product to BIs (C2).

3.2 Notations

In this section, we show the notations of all steps in this research in Table 2.

3.3 System processes

3.3.1 Registration phase: Each role in the auction must register with CA. The buyers and the sellers in the auction must register their personal information with AM, and all information is delivered via a secure channel. Fig. 3 shows the process, and the details are listed in the following:

1. PA registers to AM with PA_Info, ID_{PA} and PW_{PA}.

2. AM saves PA_Info.

3. BI registers to AM with BI_Info, ID_{BI} and PW_{BI} encrypted by pkAM.

4. AM saves BI_Info.

Table 1 Comparisons of related works

Items	Lin [19]	Yang [4]	Liaw *et al.* [6]	Wang *et al.* [18]	Lin *et al.* [13]
registration	△	○	○	△	△
authentication	×	×	○	×	△
advertisement	×	○	△	×	×
payment	○	×	○	×	○
rights transfer	○	○	○	×	×
usage tracking	×	×	○	○	×
arbitration	×	×	×	○	○
lease	○	○	○	×	×

○: achieved; △: partially achieved; ×: not achieved

IET Inf. Secur., 2010, Vol. 4, Iss. 4, pp. 248–257
doi: 10.1049/iet-ifs.2009.0250

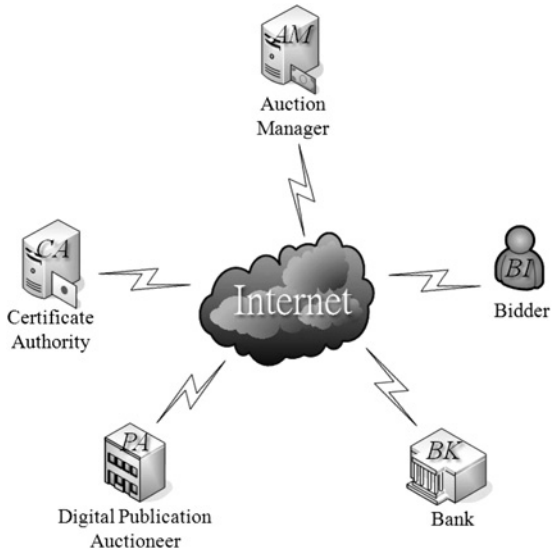

Figure 2 *System architecture in this research*

3.3.2 Authentication phase: Before starting an auction, BI and PA must authenticate with AM through login. Fig. 4 shows the process, and the details are listed in the following:

1. BI enters his/her ID_{BI} and PW_{BI} and sends ID_{BI}, PW_{BI} and $H(ID_{BI} \oplus Time)$ to AM for authentication. If BI is valid, he/she can login into the auction system.

2. The authentication process of PA is the same as above.

3.3.3 Advertisement phase: After PA is identified, he/she can advertise his digital product for making auctions. However, the digital product must be identified by CA for the correctness of it. Fig. 5 shows the process, and the details are listed in the following:

1. PA has two modes to bid PN. The first mode is C2C, and because PN is already encrypted by last PA, the PA verifies sk_PA(PN) and Code. The other mode is B2C, where PA encrypts PN by advanced encryption standard for first auction, and then the advertisement starts. In order to restrict the usage of PN before the winner is announced, the DRM system will prohibit PA to use PN until it is revoked.

2. PA selects a random number R, signs the information with PA_Id, PN_Name, Price and R and sends the signature and sk_PA(PN) to AM.

3. In order to preserve the integrity of Price, AM hashes Price with R, and transmits PN_Name, Price and $H(R\|Price)$ to CA.

4. PA decides the grant rights mode first which is Usagerule (written by XrML), including print right, usage times, usage

Table 2 Notations for the proposed mechanism

Notations	Descriptions
$H()$	the hash function
$\oplus$	the XOR operation
pk_X	the public key of X
Sk_X	the private key of X
$E_K(X)$	using the key K to encrypt the plaintext X
$Cert_X$	the certificate of X
ID_X	the identify of X
PW_X	the password of X
X, N, Y, R, Z	the random number
k_X	the random number of X's template key
$Sign_X$	making a signature with the key X
Price	the starting price of the auction
Order	the bid price
OrderOK	the successful bid price
PriceMAX	the maximum bid price of the auction
Pay	accounts payable
Paid	account paid
PaidOK	the message of successful transaction
PA_Id	the identify of PA
PA_Info	the personal information of PA
BI_Id	the identify of BI
BI_Info	the personal information of BI
PN	the digital product
sk_PA(PN)	the protected digital product
sk_PN	the secret key of PN
PN_Id	the identify of PN
PN_Info	the information of PN
PN_Name	the name of PN
License	the license of PN
Usagerule	the usage policies of License
W	digital fingerprint
Code	the encoding method of PN
Time	a timestamp
PN_Fee	the fee of PN
PN_AM_Fee	the fee of PN for AM
PN_PA_Fee	the fee of PN for PA
Mode	the payment terms
Revoke()	revoking

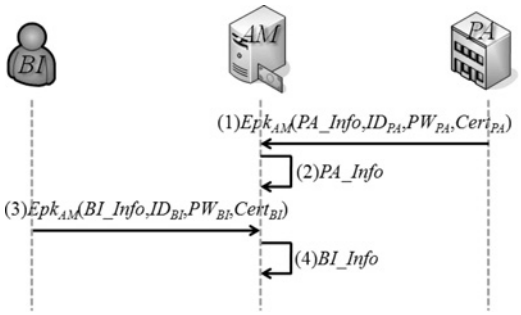

Figure 3 *Registration phase*

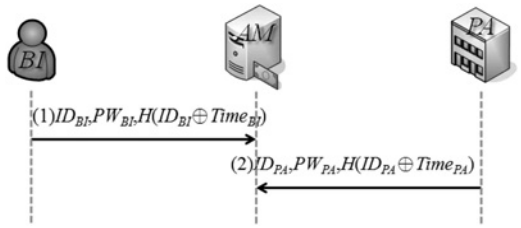

Figure 4 *Authentication phase*

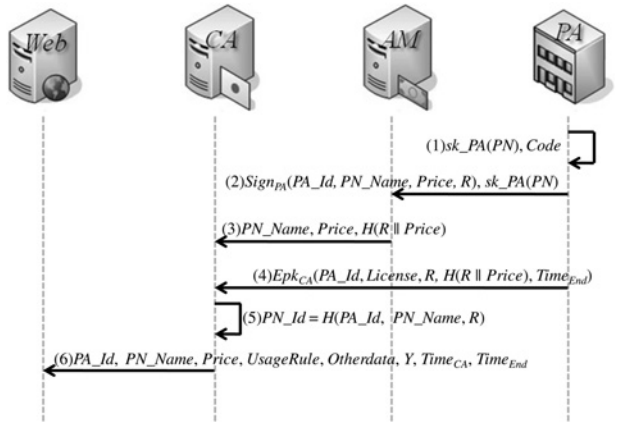

Figure 5 *Advertisement phase*

durations, and so on. After that, PA encrypts the information and sends it to CA.

5. If the two $H(R\|\text{Price})$ from AM and PA are the same, CA will generate the new PN_Id by computing H(PA_Id, PN_Name, R).

6. After verification, CA advertises the digital product in Web.

3.3.4 Bidding phase: BI browses the digital product advertised by PA, and can bid the interested one. Fig. 6 introduces the process, and the details are listed in the following:

1. BI browses Web, finds PN that he/she wants to bid and sends request to Web for getting PN_Info.

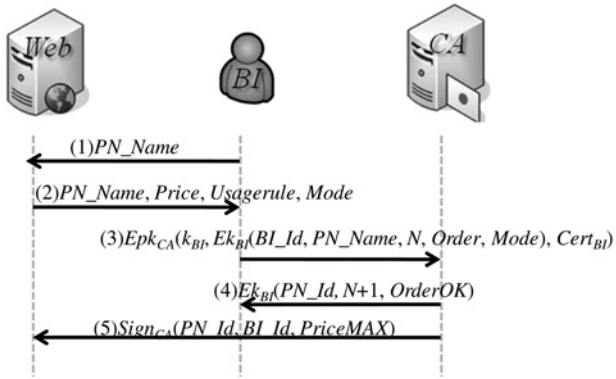

Figure 6 *Bidding phase*

2. Web transfers PN_Info to BI, including PN_Name, Price, Usagerule and the payment terms mode.

3. BI decides a random number N, a bid price Order and Mode. Then, he encrypts the information and transmits it to CA.

4. If the Order received is larger than PriceMAX, CA respond that the bid is successful.

5. If the bid is successful, CA will update the PriceMAX of PN on the Web.

3.3.5 Winner announcement phase: When an auction arrives at the ending time set up by PA, it is stopped and the winner is announced. The winner announcement phase is showed in Fig. 7, and the steps are listed in detail as follows:

1. CA notifies AM to transfer PN to BI. The notification is encrypted and includes BI_Id, PN_Name, PriceMAX and Mode.

2. In order to provide the fairness and verifiability of the auction, CA will announce the bid winner information on Web. The information is signed by CA and includes BI_Id, PN_Name and PriceMAX.

3. Then, CA informs the winner. The notification is signed by CA and includes BI_Id, PN_Name and PriceMAX.

3.3.6 Payment phase: This phase is the payment phase after bidding, and the payment phase is displayed in Fig. 8. The application of secure socket layer (SSL) to protect the winning BI and BK is demonstrated, too, and the steps are listed in detail as follows:

1. AM receives the winning BI's information with BI_Id and PN_Name from CA. It computes the digital fingerprint $W_{(\text{Time})}$ of PN_Name and saves $W_{(\text{Time})}$ to the database.

doi: 10.1049/iet-ifs.2009.0250

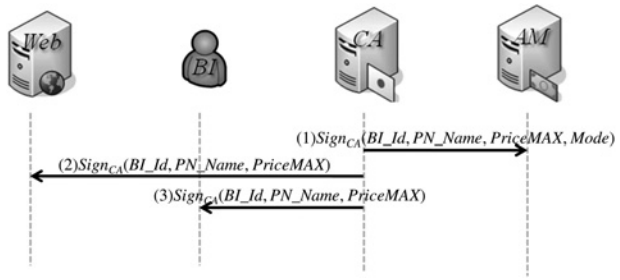

Figure 7 *Winner announcement phase*

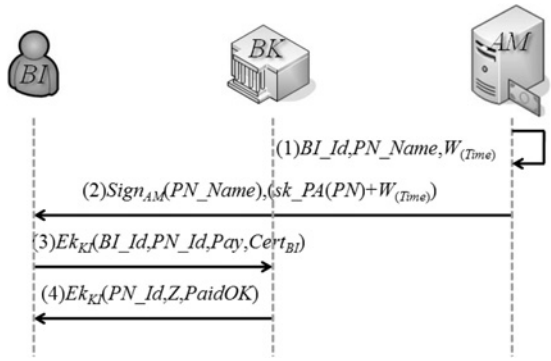

Figure 8 *Payment phase*

2. AM transfers PN_Name, the protected digital product and the digital fingerprint, to BI.

3. BI pays to obtain template key kKI in order to use the digital product received.

4. BK returns PaidOK and a random number Z to finish the payment phase.

3.3.7 Right transfer phase: After the payment phase, CA transfers the rights of PN to BI who wins the bid, for BI can play PN, and CA distributes profit to PA and AM. Fig. 9 shows the process, and the details are listed in the following:

1. BI encrypts the information with BI_Info, PaidOK and Z with pk_{CA}, and sends to CA to request for the license.

2. CA requests PA to revoke PN. Because PN is bided by BI, PA is not able to keep PN anymore.

3. CA regenerates a license of PN for BI, and sends License to BI.

4. If BI can play PN with License, PN and License are valid, and BI sends PN_OK to CA.

5. CA pays PN_PA_Fee to PA and PN_AM_Fee to AM via BK.

6. BK verifies CA's notification, and pays PN_PA_Fee to PA.

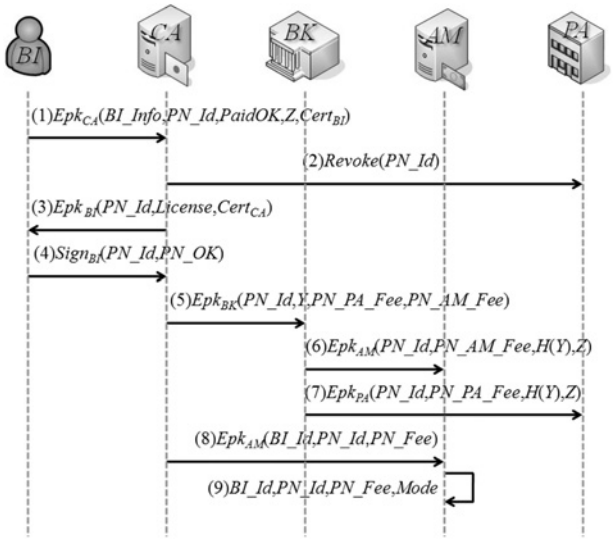

Figure 9 *Right transfer phase*

7. BK verifies CA's notification, and pays PN_AM_Fee to AM.

8. CA sends BI_Id, PN_Id and PN_Fee to AM.

9. AM saves the received information for auditing in the future.

3.3.8 Usage tracking phase: Even if PN is transferred, AM can trace PN by verifying the digital fingerprint of PN to prevent from duplication. Fig. 10 displays the processes, and the details are listed in the following:

1. Because the DRM system will request to verify AM when he/she uses the digital product, in this phase, BI will request AM to verify whether PN is valid or not automatically.

2. AM returns the digital fingerprint of PN to BI.

3. BI verifies PN with the digital fingerprint.

3.3.9 Arbitration phase: If there were any invalid duplication after usage tracking, AM could go to

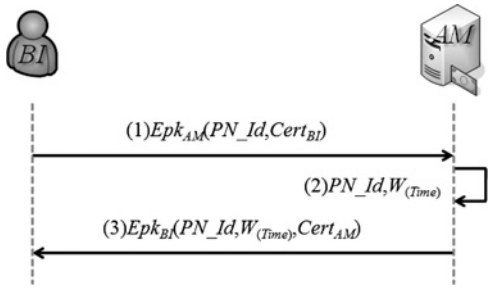

Figure 10 *Usage tracking phase*

arbitration. Fig. 11 shows the processes, and the details are listed in the following:

1. AM sends BI_Id, $W_{(Time)}$ and $Cert_{AM}$ to CA for arbitration. In order to avoid attacks, AM will sign these information before it is delivered to CA.

2. CA encrypts a random number X and BI_Id′, and returns it to AM as receipt for confirmation.

3. CA compares PN_Id′ of PN_Info and PN_Id extracted from BI. If they are not the same, CA will request to revoke PN of BI.

4. If the previous comparison is not the same, in order to preserve the fairness of auction, PN of BI is revoked.

3.3.10 Appreciation phase: In order to make sure the correct digital product which BI really wants to bid, it supports a sample show of PN in this phase. Moreover, the above action can reduce the arguments between BI and PA. In addition, it is convenient because BI can appreciate a sample of PN by providing personal information. Fig. 12 displayed the processes, and the details are listed in the following:

1. BI sends a request to AM for appreciation.

2. AM receives the request from BI and sends a request to CA for applying rights of the appreciation.

3. CA returns the rights which are applied by AM to AM.

4. AM encrypts PN and sends the protected digital product sk_PA(PN) and the license of the appreciation to BI.

5. AM saves BI_Info, PN_Name and Mode for auditing in the future.

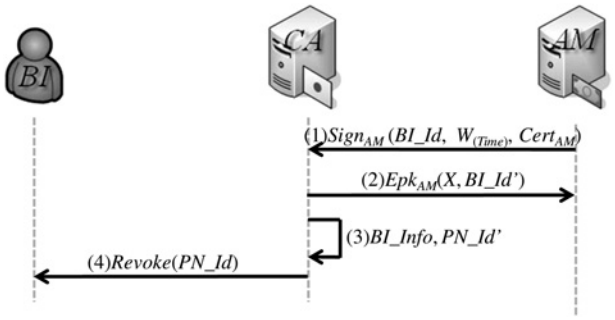

Figure 11 *Arbitration phase*

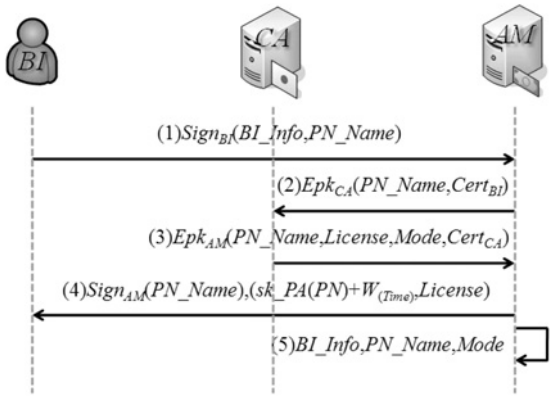

Figure 12 *Appreciation phase*

4 Analysis

The followings are comparisons of security, function and performance with related literature [4, 6, 13, 18, 19]. This research focuses on the transaction mode of e-auction platform. We find that if there were better security and privacy in the transmission process, the e-auction platform would be more popular. Table 3 shows the security comparisons for the related works, and the analysis of security is discussed in the following:

Table 3 Security comparisons for the related works

Items	Lin [19]	Yang [4]	Liaw *et al.* [6]	Wang *et al.* [18]	Lin *et al.* [13]	Our proposal
anonymity	–	○	○	△	○	○
unforgeability	–	○	○	○	○	○
non-repudiation	–	○	○	○	○	○
verification of digital product	×	○	–	×	○	○
privacy	–	○	○	○	○	○
digital product protection	○	○	○	○	×	○
replay attack resistance	–	○	○	○	○	○
web-based attack resistance	–	×	×	×	×	○
eavesdropping resistance	–	○	○	○	○	○

○: achieved; △: partially achieved; ×: not achieved; –: non-mentioned.

doi: 10.1049/iet-ifs.2009.0250

Table 4 Function comparisons for the related works

Items	Lin [19]	Yang [4]	Liaw *et al.* [6]	Wang *et al.* [18]	Lin *et al.* [13]	Our proposal
register once	△	○	○	–	–	○
fairness	×	○	×	×	×	○
audit	×	○	×	×	×	○
immediate feedback	×	△	○	×	○	○
rights transfer	○	○	○	×	×	○
usage tracking	×	×	○	○	×	○
transaction modes	B2C	C2C	B2C	B2C	B2C	B2C, C2C
flexible price	×	×	×	×	×	○
arbitration	×	×	–	○	○	○
appreciation	×	×	–	×	×	○
easy distribution	×	○	×	×	×	○

○: achieved; △: partially achieved; ×: not achieved; –: non-mentioned

1. Anonymity: This researched mechanism enables both parties BI_Id, PA_Id merely show their identities at the phase of login and bidding. Their real identities are kept by the auction host and will not be revealed to other buyers or sellers.

2. Unforgeability: In the advertisement phase, CA can verify $H(R\|\text{Price})$ to check if PA information provided by AM is fake or not. In the bidding phase, any BI applies a temporary key to generate kBI, so that other BIs will be unable to forge and bid. After bidding, BIs are unable to fabricate the signature of the certificate centre or announce it at the auction website. In the payment phase, the digital product with digital fingerprint and time mark $W_{(\text{Time})}$ can avoid forging digital fingerprint. Finally, in the rights transfer phase, the payment certificate PaidOK is complete, so it is impossible to fabricate any information of payment.

Table 5 Notations for the performance analysis

Notations	Explanations
T_{exp}	time to execute an asymmetric encryption
T_{sym}	time to execute a symmetric encryption
T_{SSL}	time to execute one SLL process
T_{h}	time to execute a hash function
$T_{\oplus}$	time to execute an XOR operation
T_{ECC}	time to execute an ECC encryption
T_{sig}	time to execute an ECC signature
T_{mul}	time to execute a mode operation

3. Non-repudiation: The auctioneer transmits a random number R to the auction centre; therefore it is impossible to propose a non-repudiation announcement.

4. Privacy: In the phase of payment, the bank only knows the number of the bidden digital product PN_Id and its price; therefore the bank will not be able to trace the BI or the product.

5. Digital product protection: The auction centre will first check the coding of the digital product, and encrypt the digital product with regular key to further protect the digital product. In Wang *et al.* [18] mechanism, it inserts digital watermark onto digital product to trace illegally distributed duplications.

As shown in Table 4, function analysis displays that this research extends the authorised transaction modes of digital rights in the existing e-auction environment.

The performance analysis displays the differences of this research and related literature. Table 5 shows the notations of performance analysis, and Table 6 shows the time complexity analysis. As shown in the previous tables, our mechanism does not provide better performance than others. This is because the proposal does not only include the digital content delivery and protection, such as in [4, 6, 13, 18, 19], but also to provide the digital product transaction model with auction system.

The proposal combines e-auction platform and DRM in the multi-agent system environment. It provides a new way to distribute digital product, to gain profit by bidding and helps users to obtain the most cost-effective amount.

Table 6 Performance comparisons for the related works

Items	Lin [19]	Yang [4]	Liaw *et al.* [6]	Wang *et al.* [18]	Lin *et al.* [13]	Our proposal
registration	–	–	$3T_{exp}$	–	–	$2T_{exp}$
authentication	–	–	$1T_{exp} + 1T_{\oplus}$	–	–	$2T_h + 2T_{\oplus} + 2T_{SSL}$
advertisement	–	$3T_{exp}$	$1T_{exp}$	–	$14T_{sym} + 11T_{exp} + 7T_{SSL} + 4T_{sig} + 14T_h + 1T_{mul}$	$1T_{sig} + 1T_{exp} + 1T_{sym} + 2T_h + 2T_{\oplus}$
bidding	–	–	–	–		$2nT_{sym} + nT_{exp} + nT_{sig}$
winner announcement						$3T_{sig}$
payment	–	–	$2T_{sig} + 4T_{exp} + 2T_{ECC} + 2T_h$	–		$1T_{sig} + 2T_{SSL}$
rights transfer	–	$3T_{sig} + 1T_{sym} + 2T_{exp} + 1T_h$	$3T_{sig} + 4T_{exp} + 2T_{ECC} + 2T_{\oplus} + 6T_h$	–	–	$1T_{sig} + 6T_{exp} + 2T_h$
usage tracking	–	–	$2T_{sig} + 1T_{exp} + 2T_{ECC} + 4T_h$	$2T_{sig} + 2T_{exp}$	–	$2T_{exp}$
arbitration	–	–		$2T_{sig} + 2T_{exp}$	$2T_{exp} + 6T_h$	$T_{sig} + T_{exp}$
appreciation	–	–	–	–	–	$2T_{sig} + 2T_{exp}$

-: non-mentioned

5 Conclusions

To reach effective distribution of digital product and solve the problems of e-commerce, we propose a digital product transaction mechanism for electronic auction in the multi-agent system environment. Its characteristics include multiplex transaction modes, feedback to the providers, usage tracking, rights transfer, and so on. The above characteristics improve the existing e-auction mechanism [12] and DRM mechanism [6].

The contributions of this research are integration of DRM and e-auction platform, rights transfer, usage tracking, distribution of digital product by e-auction, the new profit way of e-commerce, multiplex transaction modes, security and fairness. Because of above advantages, we create a new business opportunities for digital product industry.

We suggest some research directions in the future. The first is to integrate entire product and digital product into an auction platform. The platform can provide more multiplex product for transaction. Second, we can apply all these ideas to the mobile environment. It can help digital product auction to proceed anytime anywhere in a more convenient way. Finally, we can improve authentication of this mechanism by using smart card or radio frequency identification.

6 Acknowledgment

This research is supported in part by SHU under contract numbers P9509 and P9610. The authors would also like to thank Professor Horng-Twu Liaw and Miss Hui-Ting Fang of Shih-Hsin University for their help with this paper.

7 References

[1] LIU Q., SAFAVI-NAINI R., SHEPPARD N.P.: 'Digital rights management for content distribution'. Proc. Australasian Information Security Workshop, 2003, vol. 21, pp. 49–58

[2] HWANG S.O.: 'How viable is digital rights management', *Computer*, 2009, **42**, (4), pp. 28–34

[3] IANNELLA R.: 'Digital rights management (DRM) architectures', *D-Lib. Mag.*, 2001, **7**, (6), Available at http://www.dlib.org/dlib/june01/iannella/06iannella.html

[4] YANG K.C.: 'The research of transferable digital rights management system and its applications in electronic commerce' (Institute of Information Systems and Application, National Tsing Hua University, 2005)

[5] BANERJEE S., KARFORMA S.: 'A prototype design for DRM based credit card transaction in e-commerce', *Ubiquity*, 2008, **9**, (18)

doi: 10.1049/iet-ifs.2009.0250

[6] LIAW H.T., GUO M.H., LIAO W.P., HSIAO L.L.: 'Digital right issuing management mechanism and implementation strategy', *J. Comput. Sci. Appl.*, 2007, **3**, (1), pp. 23–42

[7] MOHANTY S.P.: 'A secure digital camera architecture for integrated real-time digital rights management', *J. Syst. Arch.*, 2009, **55**, (10–12), pp. 468–480

[8] MUHLBAUER A., SAFAVI-NAINI R., SALIM F., SHEPPARD N.P., SURMINEN M.: 'Location constrains in digital rights management', *Comput. Commun.*, 2008, **31**, (6), pp. 1173–1180

[9] NAGAMALLESWARA RAO N., THRIMURTHY P., RAVEENDRA BABU B.: 'A novel scheme for digital rights management of images using biometrics', *Int. J. Comput. Sci. Netw. Secur.*, 2009, **9**, (3), pp. 157–167

[10] SUN M.K., LAIH C.S., YEN H.Y., KUO J.R.: 'A ticket based digital rights management model'. Proc. IEEE Consumer Communications and Networking Conf., 2009, pp. 1–5

[11] ALARAJ A., MUNRO M.: 'An e-commerce fair exchange protocol for exchanging digital product and payments'. Proc. 2nd Int. Conf. Digital Information Management, 2007, vol. 1, Issue (28–31), pp. 248–253

[12] CHAO P.C.: 'An electronic bidding auction mechanism with smart cards' (Department of Information Management, Shih Hsin University, 2006)

[13] LIN S.J., LIU D.C.: 'An incentive-based electronic payment scheme for digital content transactions over the Internet', *J. Netw. Comput. Appl.*, 2009, **32**, (3), pp. 589–598

[14] CATTELAN R.G., HE S., KIROVSKI D.: 'Prototyping a novel platform for free-trade of digital content'. ACM Int. Conf. Proc. Ser., 2009, vol. 192

[15] LIN C.C., CHIANG P.H.: 'A mobile trading scheme for digital content based on digital rights'. Proc. 8th Int. Conf. Intelligent Systems Design and Applications 3, 2008, pp. 451–456

[16] WANG X., LAO G., DEMARTINI T., REDDY H., NGUYEN M., VALENZUELA E.: 'XrML–eXtensible rights Markup Language'. Proc. ACM Workshop on XML Security, 2002, pp. 71–79

[17] JIN C., XU D., QU Z.: 'Applications of digital fingerprinting and digital watermarking for E-commerce security mechanism'. Proc. Int. Conf. Audio, Language and Image Processing, 2008, pp. 536–540

[18] WANG F., LI C., WANG Z., CHENG Z.: 'Security scheme research of digital product online transactions'. Proc. IEEE Int. Conf. Automation and Logistics, 2008, pp. 1521–1525

[19] LIN Y.J., HSU H.C., YEH W.H.: 'Digital content rights issuing management mechanism'. Workshop on Research and Development Efforts for Taiwan e-Learning and Digital Archives Program, Taipei, 2004, pp. 297–304