出國報告（出國類別：其他-參加國際會議）

參加
2013 年第八屆亞洲資訊安全國際研討會

服務機關：國立高雄第一科技大學資管系
姓名職稱：莊文勝/教授
派赴國家：韓國
出國期間：2013/7/24-2013/7/26
報告日期：2013/8/15

摘要

2013 年第八屆亞洲資訊安全國際會議(The 8th Asia Joint Conference on Information Security，AsiaJCIS 2013) 為亞洲地區聯合舉辦的資訊安全之國際會議。今年於韓國首爾舉辦。由於資訊安全應用越來越成熟，相關的議題也普遍受到各國重視。本人因計畫需要利用暑假期間撥空參與此盛會，以探討相關安全議題。此會議論文發表共兩天。會議第一天共兩場邀請演講與四個場次的論文發表。會議第二天有一場邀請演講與兩個場次的論文發表。另外 Asia Joint Conference on Information Security 是目前亞洲區台、日、韓、大陸輪流舉辦相當成功的國際會議之一，參與此會議也讓本人更了解資訊安全於亞洲地區發展的最新趨勢，也對資訊安全議題的探討會有相當助益。這次參與 2013 年第八屆亞洲資訊安全國際會議本人發表一篇論文，名稱為 “An Efficient and Practical Fair Buyer-anonymity Exchange Scheme Using Bilinear Pairings”，另外藉由觀摩此會議的進行與相關議題的探討，對資訊安全的趨勢發展會有所幫助且對未來協助主辦相關國際會議也會有相當的幫助。

目次

摘要……………………………………………………………..

目的……………………………………………………………..1

過程……………………………………………………………..2

心得及建議……………………………………………………..3

附件……………………………………………………………..4

目的

Asia Joint Conference on Information Security 每年舉辦一次，為亞洲地區資訊安全有名的國際會議。會議討論議題涵蓋所有資訊安全理論與實務應用。Asia Joint Conference on Information Security 今年於韓國首爾舉辦。今年此次會議共有共有三場邀請演講與 20 篇論文發表。會議主題涵蓋密碼協定、認證、網路安全、數位鑑識、國際標準等。主要參與之學者有大陸、台灣、韓國、日本亞洲等國資訊安全學者。

本次會議有兩天論文發表議程，其中含 20 篇論文發表。整體觀之，Asia Joint Conference on Information Security 是以資訊安全應用議題為主軸，內容相當多元。

所接受論文發表包括密碼協定、認證、網路安全、數位鑑識、國際標準等議題。本人於會中發表一篇認證應用的論文，名稱為 “An Efficient and Practical Fair Buyer-anonymity Exchange Scheme Using Bilinear Pairings”，以下簡述本人發表論文摘要內容。

公平交換方案能用於電子商務中交換數位商品與付款。為了提供離線交易，大部分的公平交易方案需要可信賴的第三方去解決爭議並保證交換中的公平性。另外，如果交換的內容一部分為付款，買方匿名性將是提供一個好的屬性來吸引消費者使用所提出的機制。為解決上述問題，我們提出一安全且有效能的買方匿名公平交換機制。在我們我提出的方法上，我們使用橢圓曲線上的雙線性配對來降低計算與通訊成本。由於在交換階段只有客戶與商家需要參與，我們所提出的方案提供真正的離線式交易。另外我們所提出的方案提供買方匿名性的功能。

過程

本次會議有兩天論文發表議程，其中含 20 篇論文發表與三場邀請演講。Asia Joint Conference on Information Security 是以資訊安全應用議題為主軸，內容相當多元。所接受發表的論文發表包括密碼協定、認證、網路安全、數位鑑識、國際標準等主題。本人於會中發表一篇論文，名稱為 “An Efficient and Practical Fair Buyer-anonymity Exchange Scheme Using Bilinear Pairings” 。

本次會議中邀請演講與論文發表皆相當精采。茲選錄如下：

第一場邀請演講題目為“Embedding Secrets in Digital Images” 。講者為在逢甲大學服務的張講座教授真誠。張教授為國內資訊安全領域的啟蒙老師，也是中華民國資訊安全學會第一屆理事長，對國內資安研究與人才的培養有不可取代的貢獻。去年也獲頒此會議的終身成就獎。其介紹數位影像內嵌祕密的相關技術與研究。

第二場邀請演講題目為“Introduction of a Concept for Cyber-Security Management” 。講者為在日本 KDDI 服務的 Nakao 博士。Nakao 博士於日本負責許多大型的資安計畫。最近幾年跟台灣有許多的合作交流。今年獲頒此會議的終身成就獎。Nakao 博士介紹資訊安全管理與網路安全聯合防護的關係與應用。

第三場邀請演講題目為“Growth Strategies of Information Security Industry in Korea” 。講者為在韓國 KASIT 服務的 Kim 博士。Kim 博士介紹韓國資安產業的現況與成長策略。

發表中有一篇論文題目為“Design and Implementation of Digital Forensic Software for iPhone” 。其作者為高雄師範大學陳忠男學者，楊中皇教授與政治大學的左瑞麟教授。此篇論文使用 Object C 與 Shell Script 來開發 iOS 的數位鑑識系統，本篇論文也得到今年的最佳論文獎。

一篇論文題目為“Secure Certificateless Signature Scheme Supporting Batch Verification” 。其作者為中山大學的范俊逸教授，Pei-Hsiu Ho 學者，黃政嘉學者與 Yi-Fan Tseng 學者。Pei-Hsiu Ho 學者於發表中介紹其所設計的支援批次驗證的無憑證簽章方案。

一篇論文題目為“Detect Zero by Using Symmetric Homomorphic Encryption” 。其作者為中山大學的官大智教授, Chen-Yu Tsai 學者與 E. S. Zhuang 學者。官教授於發表中分析同態加密偵測零，相等的一些性質。

一篇論文題目為“Detecting HTTP-based Botnet based on Characteristic of the C&C session using by SVM” 。其作者為九州大學 Kazumasa Yamauchi 學者，佐賀大學的 Yoshiaki Hori 教授與九州大學的 Kouichi Sakurai 教授。Kazumasa Yamauchi 學者於發表中介紹使用支援向量機器來偵測 Http-based 殭屍網路。

另有一篇論文題目為“Present Cyber Threat Management” 。其作者為韓國釜慶大學的 B. G. Mawudor 學者。B. G. Mawudor 學者於發表中介紹各式網路攻擊與防護管理措施。

心得及建議

此次赴韓國首爾參加 2013 年第八屆亞洲資訊安全國際會議，有機會與亞洲學者一同深入討論資訊安全應用研究未來的可能發展方向。參加此次會議，可以強烈感受到資訊安全研究在亞洲地區的蓬勃發展，令人印象深刻。另外由於資訊安全應用的蓬勃發展, 其所帶來的機會與挑戰也於會中學者所注意與熱烈討論。而資訊安全應用與實務所面臨的資訊安全管理，隱私保護，認證等安全問題也也是推行這些應用所必須面對與解決的迫切問題。非常感謝國科會能提供足夠的經費讓本人參加此盛會。對本人而言，目睹亞洲學者在資訊安全應用研究工作上的表現，也讓我們能掌握資訊安全應用的主流研究趨勢。

附錄

1. 攜回資料

本次參加會議所攜回之資料有下列兩項：

●會議論文集。

●大會議程手冊。

2. 相片

圖一：參加 AsiaJCIS 2013 會議

圖二：AsiaJCIS 2013 會議發表論文

3. 發表論文

論文題目**: An Efficient and Practical Fair Buyer-anonymity Exchange Scheme Using Bilinear Pairings**

2013 Eighth Asia Joint Conference on Information Security

An Efficient and Practical Fair Buyer-anonymity Exchange Scheme Using Bilinear Pairings

Wen-Sheng Juang
Department of Information Management
National Kaohsiung First University of Science and Technology
Kaohsiung, Taiwan
wsjuang@nkfust.edu.tw

***Abstract*—A practical and efficient fair exchange scheme can be used in electronic commerce for exchanging digital goods with payment. In order to provide offline transaction, most of the practical and flexible fair exchange schemes need the involving of the trusted third parties to resolve the disputes and ensure the fairness in the exchange. Also, if a fair exchange service deals with the exchange between the payment and the digital goods, buyer-anonymity is a nice function to attract customers to use this service. In this paper, we propose a practical and efficient fair buyer-anonymity exchange scheme for electronic commerce. In our scheme, we use bilinear pairings in elliptic curves to reduce the computation and communication cost. Since only the customer and the merchant are involved during the exchange phase, our scheme can provide truly offline transaction. Also, the buyer-anonymity is preserved in our scheme for attracting customers to use this service.**

Keywords—fair exchange, electronic cash, digital goods, buyer-anonymity, tamper-resistant smartcard, electronic commerce, bilinear pairing, elliptic curve cryptosystem.

I. Introduction

Due to the fast progress of the communication and computer technology, many value added services, e.g. shopping, payment, etc., can be conducted over the Internet [1], [2], [3], [6], [7], [8], [9], [10], [16], [17], [18], [21], [22], [23], [26], [28]. The key success factors of electronic commerce are information flow, money flow, and goods flow. For providing flexible and practical money flow and information flow, many fair exchange schemes or payment schemes have been provided [1], [2], [3], [6], [7], [8], [9], [10], [16], [17], [18], [21], [22], [23], [26], [28], [29], [30]. From a customer's point of view, security, anonymity, fairness, and efficiency are the basic criteria of fair exchange schemes and from the merchant's point of view, security and efficiency are most important criteria of fair exchange schemes [1], [2], [7], [8], [16], [17], [18], [21], [22], [23], [26], [28]. Since the network often is not reliable or some network nodes suffer the denial of service attacks, there may be disconnected between any two network participants. Offline transaction is a key success factor for attracting customers to use fair exchange services [1], [2], [7], [16], [17], [18], [21], [22], [23], [28]. Also, some schemes investigated the fair exchange between the digital goods and the payment, in which the customer exchange the digital goods with the payment from the merchant [1], [7], [17], [22], [28]. In these schemes [1], [7], [17], [22], [28], if the buyer-anonymity can be provided, it will attract customers to use this service. For provide a more flexible offline fair exchange scheme, some optimistic fair exchange protocols have been proposed [1], [21]. In these schemes [1], [21], only two exchange participants are involved in the exchange phase.

A secure fair buyer-anonymity exchange scheme can be regarded as a protocol involving a customer, a merchant, a service provider, and a bank [1], [7], [17], [22], [28]. Both the merchant and the customer have their accounts in the bank. Also, the merchant will register his digital goods in the service provider. The customer will want to exchange the digital goods owned by the merchant with the payment fairly. Most of the fair buyer-anonymity schemes are not truly offline schemes [1], [7], [17], [22], [28]. In the exchange phase of these schemes, the merchant needs to contact with the bank for preventing the double-spending. Also, the communication cost and computation cost is still high since most of the related schemes are based on the factoring hard problem.

To remedy all the above problems, we propose a practical and efficient buyer-anonymity fair exchange scheme. For achieving buyer-anonymity property, the concept of digital pseudonyms combined with partially blind signatures using bilinear pairing is adopted and the customer uses the corresponding private key of the pseudonym to sign the encrypted payment. By this novel approach, the computation cost and communication cost is reduced and the buyer-anonymity property is also preserved. Also, by using the tamper-proof devices as e-cash smartcards, our proposed scheme can provide exact payment and truly offline transaction during the exchange phase. During the exchange phase of our proposed scheme, only the customer and the merchant is involved. The bank and the service provider are not involved in the exchange phase. Truly offline fair transaction makes our scheme more efficient and flexible. Thus, our proposed scheme can be used in various network environments including a P2P environment.

The remainder of the paper is organized as follows: In Section II, a brief description of basic tools used in our scheme is given. In Section III, we present our scheme. Section IV is devoted to correctness and security considerations. In Section V, we discuss the performance and functionality. In Section VI, we discuss the implementation considerations. Finally, a concluding remark is given in Section VII.

II. Basic Tools

In this section, we will introduce two basic bilinear signature schemes used in our proposed scheme. Let $(G_1, +)$ and $(G_2, \cdot)$ be two cyclic groups of the prime order q [5],

978-0-7695-5075-6/13 $26.00 © 2013 IEEE
DOI 10.1109/ASIAJCIS.2013.11

[27]. Let $H(\cdot)$ and $h(\cdot)$ be two cryptographic hash function where H:$\{0,1\}^* \rightarrow G_1$ and h:$\{0,1\}^* \rightarrow Z_q$ and let P be a generator of the group G_1. The bilinear pairing is given as $\widehat{e}$: $G_1 \times G_1 \rightarrow G_2$, which satisfies the following requirements:

1) Bilinearity: For all x,y,z $\in$ G_1, $\widehat{e}(x+y,z)$=$\widehat{e}(x,z)\widehat{e}(y,z)$ and $\widehat{e}(x,y+z)$=$\widehat{e}(x,y)$ $\widehat{e}(x,z)$.
2) Non-degeneracy: There exists two $x, y \in G_1$ such that $\widehat{e}(x,y) \neq 1$.
3) Computability: There exists an efficient algorithm to compute $\widehat{e}(x,y)$ for all $x, y \in G_1$.

A. Digital pseudonyms using bilinear pairings

The concept of digital pseudonym was introduced in [4]. A digital pseudonym is a pseudo identification combined with her/his random chosen public key certificated by the trusted third party. Using the corresponding private key of a digital pseudonym, one person can sign a message and keep his identification secretly. For using digital pseudonyms, a digital signature scheme must be adopted. In 2004, a signature scheme using bilinear pairings was introduced [27]. We will briefly review the signature scheme in [27] in the following.

Let x be a signer's secret key and the corresponding public key be $P_{pub} = xP$. When the signer wants to sign a message m, then she/he performs the following.

1) The signature generation: The signer does the following:

1) Compute $s = \frac{1}{h(m)+x}P$.
2) The signature of m is s.

2) The signature verification:

1) To verify the signer's signature s on m, the verifier can verify if $\widehat{e}(h(m)P + P_{pub}, s) = \widehat{e}(P, P)$.

In the following, the correctness of the signature s for the message m can be justified.

$\widehat{e}(h(m)P + P_{pub}, s) = \widehat{e}((h(m)+x)P, (h(m)+x)^{-1}P) = \widehat{e}(P,P)^{(h(m)+x)(h(m)+x)^{-1}} = \widehat{e}(P,P)$.

B. Partially blind signature in bilinear pairings

Two improved partially blind signature schemes were proposed in [5]. In this subsection, we will introduce the PKI-based partially blind signature scheme proposed in [5].

When a requester requests a partially blind signature from the signer, she/he negotiates with the signer a common information c. Let $x \in Z_q$ be the signer's secret key. The corresponding public key is $P_x = xP$. Then they do the following.

1) The signature generation:

1) The signer randomly chooses a number $r \in_R Z_q$, computes $U = rH(c)$ and then sends U to the requester.
2) After receiving U, the requester generates two random numbers $\alpha, \beta \in_R Z_q$, computes $U^{'} = \alpha(h(U)+\beta)H(c)$ and $\delta \equiv_q \alpha^{-1}h(m, U^{'}) + \beta$. She/He then sends δ back to the signer.
3) Upon getting δ, the signer computes $V \equiv_q (h(U) + \delta)x + r$ and then sends V back to the requester.
4) After getting V, the requester computes $V^{'} = \alpha(VH(c) - U)$. The signature of m is (U', V', c).

2) The signature verification: To verify the signature (U', V', c) on the message m, anyone can check if the equation $\widehat{e}(V^{'}, P)$= $\widehat{e}(U^{'} + h(m, U^{'})H(c)), P_x)$ holds.

The correctness of the signature (U', V', c) on the message m can be verified in the following.

Proposition 1. *If the requester and the signer follow the signature generation protocol properly, then the following equation holds:* $\widehat{e}(V^{'}, P) = \widehat{e}(U^{'} + h(m, U^{'})H(c), P_x)$*, which is used in the signature verification process to verify the validation of the signature* (U', V', c) *on the message* m.

$$\begin{aligned}
&\widehat{e}(V^{'}, P)\\
&=\widehat{e}(\alpha(VH(c) - U), P)\\
&=\widehat{e}(\alpha((h(U)+\delta)x + r)H(c) - \alpha U, P)\\
&=\widehat{e}(\alpha((h(U) + \alpha^{-1}h(m, U^{'}) + \beta)x + r)H(c) - \alpha U, P)\\
&=\widehat{e}(\alpha(h(U) + (\alpha^{-1}h(m, U^{'}) + \beta))H(c), xP)\\
&=\widehat{e}(\alpha h(U)H(c) + \alpha\beta H(c) + h(m, U^{'})H(c)), P_x)\\
&=\widehat{e}(U^{'} + h(m, U^{'})H(c), P_x). \qquad \square
\end{aligned}$$

III. Our proposed scheme

Without loss of generality, we assume that the fair exchange scheme is executed in a secure transaction, e.g. SSL, like all other well-known fair exchange schemes. We assume that there are two persons for charging the preparation and resolving the dispute of the fair exchange scheme. One is the trusted bank for issuing smartcards and anonymous e-cash, and the other is the trusted service provider for issuing smartcards, and registering and certificating digital goods. We also assume that the smart cards issued by these two trusted bank and service provider and used in our scheme are tamper-resistant.

Our scheme consists of five phases: (1) the initializing phase, (2) the setup phase, (3) the preparation phase, (4) the exchange phase, and (5) the resolving dispute phase. In the initializing phase, the bank and the service provider generate their private keys and publish the corresponding public keys. Then, in the setup phase, the bank will issue an e-cash smartcard to a customer. In this phase, a digital pseudonym is issued by the bank by a partially blind signature scheme and stored in this tamper-proof smartcard. Also, the service provider will issue a smartcard containing a digital pseudonym to a merchant. This phase only needs to be executed once for a customer or a merchant except that she/he had revorked her/his smartcard. In the preparation phase, the merchant will prepare the certificated encrypted digital goods by the help of the service provider. The customer will request partially blind signatures as anonymous e-coins from the bank. This phase can be executed offline and in advance. In the exchange phase, the customer and the merchant exchanges the digital goods with the anonymous e-coins. If there exists any error, the customer

TABLE I. NOTATIONS USED IN OUR PROPOSED SCHEME

Symbol	Description
S	The identity of the trusted service provider
B	The identity of the trusted bank
C	The identity of a customer
M	The identity of a merchant
x_b	The private key of the bank
x_s	The private key of the service provider
P_b	The public key of the bank
P_s	The public key of the service provider
x_{c_pse}	The private key of the customer's smart card pseudonym
P_{c_pse}	The public key of the customer's smart card pseudonym
x_{m_pse}	The private key of the merchant's smart card pseudonym
P_{m_pse}	The public key of the merchant's smart card pseudonym
$expire_c$	The expiration date of the customer's smartcard
$expire_m$	The expiration date of the merchant's smartcard
(U'_{b_set}, V'_{b_set})	The certificate of the public key P_{c_pse}
(U'_{s_set}, V'_{s_set})	The certificate of the public key P_{m_pse}
c	The related information of an e-coin including the expiration date and the denomination
(α, β)	The binding factors of a blind e-coin (U', V', c)
(U', V', c)	The blind e-coin
sk_{sm}	The one-time common key between S and M
$timestamp_{sm}$	The timestamp for generating the one-time common key between S and M
$goods$	The digital goods
sk_{bc}	The one-time common key between B and C
$timestamp_{bc}$	The timestamp for generating the one-time common key between B and C
$desc$	The description of the digital goods
E_{goods}	The encrypted digital goods
s'	The signature of the encrypted digital goods
E_{e-coin}	The encrypted e-coin
s'_{pse}	The signature of the encrypted e-coin and the description of digital goods
P	The generator of the group G_1 with the prime order q
$\widehat{e}()$	The billinear pairing function
$\|\|$	The string concatenation operator
$E_x()$	The symmetric encryption function using the secret key x
$D_x()$	The symmetric decryption function using the secret key x

or the merchant can do the dispute resolving by the help of the service provider or the bank.

Let $(G_1, +)$ and $(G_2, \cdot)$ be two cyclic groups of the prime order q. Let $H(\cdot)$ and $h(\cdot)$ be two cryptographic hash functions where $H : \{0,1\}^* \rightarrow G_1$ and $h : \{0,1\}^* \rightarrow Z_q$. Let P be a generator of the group G_1. Let $\widehat{e} : G_1 \times G_1 \rightarrow G_2$ be a bilinear pairing function. Let S be the identity of the trusted service provider for preparing and certificating digital goods, B be the identity of the trusted bank, C be the identity of a customer, and M be the identity of a merchant. Let $||$ be the string concatenation operator, and $E_x()(D_x())$ be the symmetric encryption(decryption) function using the secret key x. We summarize the notations used in our proposed scheme in Table I.

The proposed scheme is in the following.

(1) **the initializing phase**:

B generates his private key $x_b \in Z_q$. Let $P_b = x_b P$ be the corresponding public key. Also, S generates his private key $x_s \in Z_q$. Let $P_s = x_s P$ be the corresponding public key. The public keys P_b and P_s are published.

(2) **the setup phase:**

(2.1) The customer's smartcard setup

Before C can withdraw an e-coin from B, she/he must setup his e-cash smartcard. The issue of the e-cash smartcard is controlled by B. C's smartcard and B then do the following.

1) B randomly chooses a number $r_{b\_set} \in Z_q$ and computes $U_{b\_set} = r_{b\_set} H(expire_c)$, where $expire_c$ is the expiration date of C's e-cash smartcard. B then sends U_{b_set} to C's smartcard.
2) After getting U_{b_set}, C's smartcard does the following.
   a) Choose randomly a private key $x_{c\_pse} \in Z_q$ of her/his e-cash smartcard pseudonym and $P_{c\_pse} = x_{c\_pse} P$ be the corresponding public key for her/his smartcard pseudonym.
   b) Choose two random numbers $\alpha_{b\_set} \in Z_q$ and $\beta_{b\_set} \in Z_q$, compute $U'_{b\_set} = \alpha_{b\_set}(h(U_{b\_set}) + \beta_{b\_set})H(expire_c)$ and $\delta_{b\_set} \equiv_q \alpha^{-1}_{b\_set} h(P_{c\_pse}, U'_{b\_set}) + \beta_{b\_set}$.
   c) He then send δ_{b_set} to the bank.
3) Upon receiving δ_{b_set}, B computes $V_{b\_set} \equiv_q (h(U_{b\_set}) + \delta_{b\_set}) x_b + r_{b\_set}$ and sends V_{b_set} back to the smartcard.
4) After receiving V_{b_set}, the smartcard computes $V'_{b\_set} = \alpha_{b\_set}((V_{b\_set})H(expire_c) - U_{b\_set})$. After the signature generation process, the secret key x_{c_pse}, the corresponding public key P_{c_pse}, the certificate of the corresponding public key (U'_{b_set}, V'_{b_set}) and the expiration date of this e-cash smartcard $expire_c$ is stored in the smartcard.

(2.2) The merchant's smartcard setup

Before M can sell the digital goods, she/he must setup his tamper-resistant smartcard. The issue of the tamper-resistant smartcard is controlled by S. M's smartcard and S then do the following.

1) S randomly chooses a number $r_{s\_set} \in Z_q$ and computes $U_{s\_set} = r_{s\_set} H(expire_m)$, where $expire_m$ is the expiration date of M's smartcard. S then sends U_{s_set} to the smartcard.
2) After getting U_{s_set}, the smartcard does the following.
   a) Choose randomly a private key $x_{m\_pse} \in Z_q$ of her/his smartcard pseudonym and $P_{m\_pse} = x_{m\_pse} P$ be the corresponding public key for her/his smartcard pseudonym.
   b) Choose two random numbers $\alpha_{s\_set} \in Z_q$ and $\beta_{s\_set} \in Z_q$, compute $U'_{s\_set} = \alpha_{s\_set}(h(U_{s\_set}) + \beta_{s\_set})H(expire_m)$ and $\delta_{s\_set} \equiv_q \alpha^{-1}_{s\_set} h(P_{m\_pse}, U'_{s\_set}) + \beta_{s\_set}$.
   c) He then send δ_{s_set} to S.
3) Upon receiving δ_{s_set}, S computes $V_{s\_set} \equiv_q (h(U_{s\_set}) + \delta_{s\_set}) x_s + r_{s\_set}$ and sends V_{s_set} back to the smartcard.
4) After receiving V_{s_set}, the smartcard computes $V'_{s\_set} = \alpha_{s\_set}((V_{s\_set})H(expire_m) - U_{s\_set})$. After the signature generation process, the secret key x_{m_pse}, the corresponding public key P_{m_pse}, the certificate of the corresponding public key (U'_{s_set}, V'_{s_set}) and the expiration date of M's smartcard $expire_m$ is stored in the smartcard.

(3) **the preparation phase:**

(3.1) Getting anonymous e-coins

Before exchanging the digital goods with e-coins, C needs to withdraw anonymous e-coins. To withdraw an anonymous e-coin, C's smart card and B do the following.

1) B randomly chooses a number $r_b \in Z_q$ and computes $U_b = r_b H(c)$,where c is the withdrawal date of this e-coin. Then she/he sends U_b to C's smartcard.
2) After getting U_b, C's smartcard does the following.
    a) Choose two random numbers $\alpha \in Z_q$ and $\beta \in Z_q$, compute $U_b' = \alpha(h(U_b) + \beta)H(c)$ and $\delta \equiv_q \alpha^{-1}h(m, U') + \beta$, where m is the blind message contained a predefined message pattern for the e-coin.
    b) She/he then send δ to B.
3) Upon receiving δ, B computes $V_b \equiv_q (h(U_b)+\delta)x_b + r_b$ and sends V_b back to C's smartcard. B deducts w dollars from C's bank account for this e-coin, where w is the denomination of this e-coin.
4) After receiving V_b, C's smartcard computes $V' = \alpha(V_b H(c) - U_b)$. The e-coin is (U', V', c) and will be stored in C's smartcard for being used in the exchange phase.

(3.2) Getting the certificate of the digital goods

Before exchanging the digital goods with e-coins, M needs to request the digital goods and get the certificate of this digital goods from S. To do this, M's smart card and S do the following.

1) The smartcard sends her/his certificate (U'_{s_set}, V'_{s_set}), the expiration date $expire_m$, and the corresponding public key P_{m_pse} and the description of the digital goods $desc$ to S for requesting the digital goods.
2) If the certificate has not been used and verified before, S verifies the validability of this certificate (U'_{s_set}, V'_{s_set}) by checking if $\widehat{e}(V'_{s\_set}, P)$= $\widehat{e}(U'_{s\_set} + h(P_{m\_pse}, U'_{set})\ H(expire_m)), P_s)$. If the verification is valid or it had verified before, she/he then computes the common key $sk_{sm} = h(x_s P_{m\_pse}, timestamp_{sm})$ between S and M for this transaction, where $timestamp_{sm}$ is the timestamp for generating the one-time common key between S and M. She/he then encrypts the digital goods $E_{goods} = E_{sk_{sm}}(goods)$. Then she/he signs the encrypted goods, and the description of the digital goods $desc$ on the digital goods $goods$ by computing $s' = (1/(h(E_{goods}||desc) + x_s))P$, stores $(U'_{s\_set}, V'_{s\_set}, s')$ in his database, and sends the encrypted goods E_{goods}, the certificate of this encrypted goods s', and the timestamp $timestamp_{sm}$ to M.
3) After receiving $(E_{goods}, s', timestamp_{sm})$, M's smartcard will store it for the later use in the exchange phase.

(4) **the exchange phase:**

When C wants to exchange the digital goods with the payment, C's smartcard and M's smartcard do the following.

1) C's smartcard computes the common key $sk_{bc} = h(x_{c\_pse}P_b, timestamp_{bc})$ between S and M for this transaction, where $timestamp_{bc}$ is the timestamp for generating the one-time common key between B and C, and encrypts the payment $E_{e-coin} = E_{sk_{bc}}(payment)$, where $payment$ is the collection of valid e-coins $(U', V', c)s$ withdrawn in the preparation phase and the total value of $payment$ is equal to the value of the exchanged goods $goods$. Then she/he signs the encrypted payment $E_{payment}$, the description of the digital goods $desc$, and the timestamp $timestamp_{bc}$ by computing $s'_{pse} = (1/(h(E_{payment}||desc||timestamp_{bc}) + x_{c\_pse}))P$, stores $(U', V', s'_{pse}, c, timestamp_{bc})$ in his database, and sends the encrypted payment information and the certificate $(E_{payment}, s'_{pse}, c, timestamp_{bc})$ to M. If this is the first time to visit M, she/he also sends the pseudonym $(P_{c\_pse}, U'_{b\_set}, V'_{b\_set}, expire_c)$ to M.
2) If this is the first time for C to visit M, M can verify the validity of the pseudonym by checking if $\widehat{e}(V'_{b\_set}, P) = \widehat{e}(U'_{b\_set} + h(P_{c\_pse}, U'_{b\_set})H(expire_c)), P_b)$. If the verification is valid or it had verified before, this pseudonym is valid issued by B. M then checks if $(E_{payment}, s'_{pse})$ is already in his database for preventing the double-spending. M then checks the validability of s'_{pse} by checking if $\widehat{e}(h(E_{payment}||desc||timestamp_{bc})P + P_{c\_pse}, s'_{pse}) = \widehat{e}(P, P)$. If yes, she/he sends (E_{goods}, s') to C.
3) C checks the validity of s' by checking if $\widehat{e}(h(E_{goods}||desc)P + P_s, s') = \widehat{e}(P, P)$. If yes, she/he sends the common key sk_{cb} to M.
4) M then can decrypt the encrypted payment $E_{payment}$ by computing $D_{sk_{bc}}(E_{payment}) = payment$. She/he then sends the common key sk_{ms} to C.
5) After receiving sk_{sm} from M, C then can decrypt the encrypted digital goods E_{goods} by computing $D_{sk_{sm}}(E_{goods}) = goods$.

Since our proposed can achieve offline transaction by using tamper-resistant smartcard, M can send the payment $payment$ to the bank for depositing the payment after the end of the exchange process. The bank can check if this payment $payment$ is already in his database for preventing the double-deposition of the merchant.

(5) **the offline resolving dispute phase:**

If there exists any dispute, C or M can request the help of S or B to send sk_{ms} or sk_{cb} to decrypt the encrypted goods or payment.

(5.1) Case 1: the customer requesting help

1) C sends $(E_{goods},\ s',\ timestamp_{sm})$ and $(P_{m\_pse}, U'_{m\_set}, V'_{m\_set}, expire_m)$ to S.
2) S verifies the validity of (U'_{s_set}, V'_{s_set}) and s' by checking if $\widehat{e}(V'_{s\_set}, P) = \widehat{e}(U'_{s\_set} + h(P_{m\_pse}, U'_{s\_set})H(expire_m)), P_s)$ and $\widehat{e}(h(E_{goods}||desc)P + P_s, s') = \widehat{e}(P, P)$. If yes, S computes $sk_{sm} = h(x_s P_{m\_pse}, timestamp_{sm})$ and sends sk_{sm} back to C.

(5.2) Case 2: the merchant requesting help

1) M sends $(E_{e-coin}, s'_{pse}, c, timestamp_{bc})$ and $(P_{c\_pse}, U'_{b\_set}, V'_{b\_set}, expire_c)$ to B.
2) B verifies the validity of (U'_{b_set}, V'_{b_set}) and s'_{pse} by checking if $\widehat{e}(V'_{b\_set}, P) = \widehat{e}(U'_{b\_set} + h(P_{c\_pse}, U'_{b\_set})H(expire_c)), P_b)$ and $\widehat{e}(h(E_{payment}||desc||timestamp_{bc})P + P_{c\_pse}, s'_{pse}) = \widehat{e}(P, P)$. If yes, B computes $sk_{bc} = h(x_b P_{c\_pse}, timestamp_{bc})$ and sends sk_{bc} back to M.

IV. Correctness and security considerations

A. Correctness

In our scheme, the customer first withdraws anonymous e-coins from the bank by the partially blind scheme in the preparation phase. Then her/his smartcard will encrypt the payment $payment$ and sign anonymously the encrypted payment using the private key of her/his pseudonym. The following proposition ensures the correctness of our proposed scheme .

Proposition 2. *If the customer and the bank follow the protocol in the preparation phase of section 3 correctly, then the following equation holds: $\widehat{e}(h(E_{payment}||desc||timestamp_{bc})P + P_{c\_pse}, s'_{pse}) = \widehat{e}(P, P)$, which is used in the exchange phase to verify the validity of the encrypted payment.*

By means of our scheme, we have

$$\widehat{e}(h(E_{payment}||desc||timestamp_{bc})P + P_{c\_pse}, s'_{pse})$$

$$=\widehat{e}((h(E_{payment}||desc||timestamp_{bc}) + x_{c\_pse})P, (h(E_{payment}||desc||timestamp_{bc}) + x_{c\_pse})^{-1}P)$$

$$=\widehat{e}(P, P) \qquad \square$$

Proposition 3. *If the customer and the bank follow the protocol in the setup phase of section 3 correctly, then the following equation holds: $\widehat{e}(V'_{b\_set}, P) = \widehat{e}(U'_{b\_set} + h(P_{c\_pse}, U'_{b\_set}) H(expire_c)), P_b)$, which is used in the exchange phase to verify the validity of the certificate for the public key of the customer's pseudonym.*

By means of our scheme, we have

$$\widehat{e}(V'_{b\_set}, P)$$

$$=\widehat{e}(\alpha_{b\_set}((V_{b\_set})H(expire_c) - U_{b\_set}), P)$$

$$=\widehat{e}(\alpha_{b\_set}((h(U_{b\_set}) + \delta_{b\_set})x_b + r_{b\_set})H(expire_c) - \alpha_{b\_set}U_{b\_set}, P)$$

$$=\widehat{e}(\alpha_{b\_set}((h(U_{b\_set}) + \alpha^{-1}_{b\_set}h(P_{c\_pse}, U'_{b\_set}) + \beta_{b\_set})x_b + r_{b\_set})H(expire_c) - \alpha_{b\_set}U_{b\_set}, P)$$

$$=\widehat{e}(\alpha_{b\_set}((h(U_{b\_set}) + \alpha^{-1}_{b\_set}h(P_{c\_pse}, U'_{b\_set}) + \beta_{b\_set})x_b + r_{b\_set})H(expire_c) -$$

$$\alpha_{b\_set}(r_{b\_set}H(expire_c)), P)$$

$$=\widehat{e}(\alpha_{b\_set}((h(U_{b\_set}) + \alpha^{-1}_{b\_set}h(P_{c\_pse}, U'_{b\_set}) + \beta_{b\_set})x_b)H(expire_c), P)$$

$$=\widehat{e}(\alpha_{b\_set}((h(U_{b\_set}) + \alpha^{-1}_{b\_set}h(P_{c\_pse}, U'_{b\_set}) + \beta_{b\_set}))H(expire_c), x_bP)$$

$$=\widehat{e}(\alpha_{b\_set}((h(U_{b\_set}) + \alpha^{-1}_{b\_set}h(P_{c\_pse}, U'_{b\_set}) + \beta_{b\_set}))H(expire_c), P_b)$$

$$=\widehat{e}(\alpha_{b\_set}h(U_{b\_set})H(expire_c) + \alpha_{b\_set}\beta_{b\_set}H(expire_c) + h(P_{c\_pse}, U'_{b\_set})H(expire_c), P_b)$$

$$=\widehat{e}(U'_{b\_set} + h(P_{c\_pse}, U'_{b\_set})H(expire_c)), P_b) \qquad \square$$

Proposition 4. *If the merchant and the service provider follow the protocol in the preparation phase of section 3 correctly, then the following equation holds: $\widehat{e}(h(E_{goods}||desc)P + P_s, s') = \widehat{e}(P, P)$, which is used in the exchange phase to verify the validity of the encrypted digital goods.*

By means of our scheme, we have

$$\widehat{e}(h(E_{goods}||desc)P + P_s, s')$$

$$=\widehat{e}((h(E_{goods}||desc) + x_s)P, (h(E_{goods}||desc) + x_s)^{-1}P)$$

$$=\widehat{e}(P, P)^{(h(E_{goods}||desc)+x_s)(h(E_{goods}||desc)+x_s)^{-1}}$$

$$=\widehat{e}(P, P) \qquad \square$$

Proposition 5. *If the merchant and the service provider follow the protocol in the setup phase of section 3 correctly, then the following equation holds: $\widehat{e}(V'_{s\_set}, P) = \widehat{e}(U'_{s\_set} + h(P_{m\_pse}, U'_{s\_set})H(expire_m)), P_s)$, which is used in the offline resolving phase to verify the validity of the certificate for the public key of the merchant's pseudonym.*

By means of our scheme, we have

$$\widehat{e}(V'_{s\_set}, P)$$

$$=\widehat{e}(\alpha_{s\_set}((V_{s\_set})H(expire_m) - U_{s\_set}), P)$$

$$=\widehat{e}(\alpha_{s\_set}((h(U_{s\_set}) + \delta_{s\_set})x_s + r_{s\_set})H(expire_m) - \alpha_{s\_set}U_{s\_set}, P)$$

$$=\widehat{e}(\alpha_{s\_set}((h(U_{s\_set}) + \alpha^{-1}_{s\_set}h(P_{m\_pse}, U'_{s\_set}) + \beta_{s\_set})x_s + r_{s\_set})H(expire_m) - \alpha_{s\_set}U_{s\_set}, P)$$

$$=\widehat{e}(\alpha_{s\_set}((h(U_{s\_set}) + \alpha^{-1}_{s\_set}h(P_{m\_pse}, U'_{s\_set}) + \beta_{s\_set})x_s + r_{s\_set})H(expire_m) -$$

$$\alpha_{s\_set}(r_{s\_set}H(expire_m)), P)$$

$$=\widehat{e}(\alpha_{s\_set}((h(U_{s\_set}) + \alpha^{-1}_{s\_set}h(P_{m\_pse}, U'_{s\_set}) + \beta_{s\_set})x_s)H(expire_m), P)$$

$$=\widehat{e}(\alpha_{s\_set}((h(U_{s\_set}) + \alpha^{-1}_{s\_set}h(P_{m\_pse}, U'_{s\_set}) + \beta_{s\_set}))H(expire_m), x_sP)$$

$$=\widehat{e}(\alpha_{s\_set}((h(U_{s\_set}) + \alpha^{-1}_{s\_set}h(P_{m\_pse}, U'_{s\_set}) + \beta_{s\_set}))H(expire_m), P_s)$$

$$=\widehat{e}(\alpha_{s\_set}h(U_{s\_set})H(expire_m) + \alpha_{s\_set}\beta_{s\_set}H(expire_m) + h(P_{m\_pse}, U'_{s\_set})H(expire_m), P_s)$$

$$=\widehat{e}(U'_{s\_set} + h(P_{m\_pse}, U'_{s\_set})H(expire_m)), P_s) \qquad \square$$

B. Fairness

An exchange protocol is fair if and only if the merchant receives the payment if and only if the customer receives the digital goods. Under the assumption of the smartcard is a trusted tamper-proof device, the encypted payment will correctly be encrypted by the common key sk_{bc} and signed by the private key of the digital pseudonym issued by the bank. Also, the encrypted digital goods will be prepared by the service provider properly. If any error occurs, the customer or the merchant can request the help of the service provider or the bank to do the offline resolving dispute, get the common secret key, and decrypt the encrypted payment or digital goods. So our proposed scheme can provide fair transaction.

C. Double-spending prevention

In the exchange phase, the merchant will check if the payment $(E_{payment}, s'_{pse})$ is already in his database for preventing the customer from double-spending. If the customer can generate a different payment $(E'_{payment}, s'_{pse})$ from $(E_{payment}, s'_{pse})$, she/he can do double-spending. Based on the assumption of the digital signature scheme mentioned in Section 2 is secure and the smartcard is a trusted tamper-proof device, the customer can not do double-spending.

D. Double-deposition prevention

After the bank receiving the payment $payment$, she/he will check if the used e-coin has been deposited by the merchant for preventing the merchant from double-deposition. For managing the e-coins stored in the trusted tamper-resistant smartcard concisely, the signed payment $s''_{pse} = (1/(h(E_{payment}||desc||timestamp_{bc}) + x_{c\_pse}))P$ can be slightly modified to $s''_{pse} = (1/(h(E_{payment}||desc||timestamp_{bc}||M) + x_{c\_pse}))P$. This will include the identity of the merchant M in the signed payment and prove that these e-coins were spent in this merchant.

E. Buyer-anonymity

An exchange protocol is buyer-anonymous if and only if the customer's identity is not revealed after the exchange phase in the protocol. Under the assumption of secure partially blind signature scheme in Section 2, all partially blind signatures as e-coins signed by the bank are unlinkable regarding the same withdrawal date. No one, except the customer, can know who withdraws this e-coin.

F. Truly offline transaction

An optimistic exchange protocol is offline if and only if the merchant and the customer can exchange their digital valued goods without needing the help of any third party when participants are honest and if any error occurs, a trusted third party can do the offline dispute resolving. In the exchange phase of our proposed scheme, only the customer and merchant are involved. Under the assumption of the smartcard is a trusted tamper-proof device, the encypted payment will correctly be encrypted by the common key sk_{bc}. Also, the encrypted digital goods will be prepared by the service provider properly in advance. If any error occurs, the customer or the merchant can request the help of the service provider or the bank to do the offline resolving dispute. So our proposed scheme can provide truly offline transaction for fair exchange.

TABLE II. PERFORMANCE COMPARISONS AMONG OTHER SCHEMES AND OUR PROPOSED SCHEME

	[17]	[1]	Our scheme
C1	N/A	6E $\cong$ 1440M	5EC$_M$+1EC$_A$+6M+8H+1S $\cong$ 161 M
C2	31E+9M+24S+16H $\cong$ 2373M	14E $\cong$ 3360M	4EC$_P$+4EC$_M$+2EC$_A$+1M+4H+5S $\cong$ 436 M
C3	12E+4H+5S $\cong$ 908M	9E $\cong$ 2160M	4EC$_P$+2EC$_M$+2EC$_A$+4H $\cong$ 370M
C4	N/A	5248	1364
C5	15232	11424	1128
C6	3072	7168	976

C1: Compuation cost of the preparation phase
C2: Compuation cost of the exchange phase
C3: Compuation cost of the offline resolving dispute phase
C4: Communication cost of the preparation phase (bits)
C5: Communication cost of the exchange phase (bits)
C6: Communication cost of the offline resolving dispute phase (bits)
N/A: Being combined into the exchange phase

V. PERFORMANCE AND FUNCTIONALITY COMPARISONS

We summarize the communication and computation complexity of related fair exchange schemes in Table II. For security consideration [14], [19], let p be of 1024 bits and q be of 160 bits in [19] and n be of 1024 bits in [14] in order to make the discrete logarithm problem or the factoring problem infeasible [14], [19]. Let the output size of secure one-way hashing functions [20] be 160 bits. Let E be the time of one modular exponential operation in a 1024-bit modulo, H be the time of one hashing operation, S be the time of one block symmetric encryption/decryption operation, M be the time for one modular multiplication in a 1024-bit modulo, EC_M be the time for the multiplication of a number over an elliptic curve, EC_P be the time for the bilinear pairing operation of two numbers over an elliptic curve, and EC_A be the time for the addition of two numbers over an elliptic curve [11], [12], [13]. Assume that an elliptic curve over a 163-bit field has the same level of the security of 1024-bit public key cryptosystems such as the Diffie-Hellman or the RSA cryptosystem [13]. Since a point in an elliptic curve consists of (x,y)-coordinate and for any x-coordinate, so only two possible y values are in an elliptic curve. We can efficiently encode a point in an elliptic curve over a 163-bit field using a 164-bit value. Assume the digital goods if of 128 bits for measuring the performance of the related schemes. The size of the payment will depend on the payment scheme used in each scheme. Assume that E $\cong$ 8.24 EC_M for the implementation with the StrongARM processor in 200MHz as referenced in [13]. We also find the relationship E $\cong$ 600H, E$\cong$ 240 M, $EC_A \cong$ 5M, and E $\cong$ 3.2 EC_P in [15], [24], [25] . We also can find the relationship S $\cong$ 3.4H in [24], where the hash function is SHA and the corresponding symmetric cryptosystem is IDEA used in the construction of the Abreast Davies-Meyer one-way hash function.

Since the initializing phase is executed only once, we do not compare this cost with related schemes. For a customer or a merchant, since the setup phase is executed only once for her/his smartcard and then this smartcard can be used until it is revoked, we also do not compare this cost with related schemes.

The computation cost of the preparation phase is not clear since it is merged to the exchange phase in [17]. The computation cost of the preparation phase is about six exponential operations in [1], and that is of five multiplication operations of a number over an elliptic curve, one addition operation of two numbers over an elliptic curve, six multiplication operations, eight hash operations and one block symmetric encryption in our scheme.

The computation cost of the exchange phase is of 31 exponential operations, nine multiplication operations, 24 blocks of symmetric encryption operations, and 16 hash operations in [17], that is about 14 exponential operations in [1], and that is of four pairing operations over an elliptic curve, four multiplication operations of a number over an elliptic curve, two addition operation of two numbers over an elliptic curve, one multiplication operation, four hash operations, and five blocks of symmetric encryption operations in our scheme.

The computation cost of the offline resolving dispute phase is about 12 exponential operations, five blocks of symmetric encryption operations, and four hash operations in [17], that is about 9 exponential operations in [1], and that is of four pairing operations over an elliptic curve, two multiplication operations of a number over an elliptic curve, two addition operation of two numbers over an elliptic curve, and four hash operations in our scheme.

The communication cost for the preparation phase is not clear since it is merged to the exchange phase in [17]. The communication cost for the preparation phase is of 1024+1024+128+1024+1024+1024=5248 bits in [1], and that is of (164+160+160)+(164+164+32+164+32+128+164+32)=1364 bits in our scheme, where the expiration date $expire_m$, the description of the digital goods $desc$, and the timestamp $timestamp_{sm}$ are all of 32 bits.

The communication cost for the exchange phase is of (128+128+1024+1024)+(1024*3+128)+1024*3+2*1024+256+128+2*1024+2*1024+128=15232 bits in [17], that is of (32+1024+1024+1024+1024+1024)+(128+1024+1024+1024+1024) +1024+1024=11424 bits in [1], and that is of ($\lceil(164+164+32)/128\rceil * 128$+164+32+32+128+164+128+128)=1128 bits in our scheme, where the related information of an e-coin c, and the timestamp $timestamp_{bc}$ are both of 32 bits.

The communication cost for the offline resolving dispute phase is of (1024+128)+(1024 +128)+(1024+128)+128+128=3072 bits in [17], that is of (1024+1024+1024+1024+1024) +1024+1024=7168 bits in [1], and that is of (128+164+32+164+164+164+32+128)=976 bits in our scheme.

We summarize the functionality and complexity of related buyer-anonymity fair exchange schemes in Table III. In our scheme, by using the tamper-resistant smartcard, offline fair exchange can be achieved by the help of the offline third party. In the schemes [1], [17], although the trusted third party is not involved in the exchange phase, the bank must be involved in the the exchange phase for preventing the double-spending of the customer. They only can achieve the offline fair exchange partially.

Both the schemes in [1], [17] do not address how to deal with the exact payment of the digital goods. The value of the e-coin must be same with the exchanged digital goods. In our scheme, the total value of the payment $payment$ is the sum of all withdrawn e-coins and is the same as the exchanged digital goods. Our proposed scheme can provide exact payment and is more flexible.

TABLE III. FUNCTIONALITY COMPARISONS AMONG OTHER SCHEMES AND OUR PROPOSED SCHEME

	[17]	[1]	Our scheme
C1	No	Yes	Yes
C2	Partially	Paritially	Yes
C3	No	No	Yes
C4	Yes	No	Yes
C5	No	No	Yes
C6	Factoring	Factoring	Billinear pairing
C7	High	High	Low
C8	High	High	Low
C9	High	High	Low
C10	High	High	Low
C11	High	High	Low
C12	High	High	Low

C1: Optimistic fair exchange
C2: Offline fair exchange
C3: Exact payment
C4: Buyer-anonymity
C5: Using tamper-resistant smartcards
C6: The fundamental hard problem of the scheme
C7: Compuation cost of the preparation phase
C8: Compuation cost of the exchange phase
C9: Computation cost of the offline resolving dispute phase
C10: Communication cost of the preparation phase
C11: Communication cost of the exchange phase
C12: Communication cost of the offline resolving dispute phase

TABLE IV. OPERATING SYSTEM AND HARDWARE

Equipment	Description
Operating system	Windows 7 Professional
Main board	Acer EG 31 MR 01-B 4 L
Processor	Intel (R) Core (TM) 2 Duo CPU E 8400@ 3.00 GHz
RAM	Single-Channel DDR 2@ 399 MHz, 4GB
Hard Disk	Hitachi (233 GB)

All the schemes in [1], [17] and our scheme use untraceable e-cash to exchange the digital goods, and can provide buyer-anonymity. For providing a flexible and offline, tamper-resistant smartcards are used in our proposed scheme.

Since our scheme is based on bilinear pairing on elliptic curve, the communication and computation cost is lower than the schemes in [1], [17].

VI. IMPLEMENTATION CONSIDERATIONS

In this section, we describe the environments of our implementation considerations as follows. We used the open source java pairing based cryptography library (jPBC) and the Bouncy Castle Crypto APIs for the Java Cryptography Extension (JCE) and the Java Cryptography Architecture (JCA) to implement our proposed method. Table IV shows the operating system and hardware used in our implementation. Also, the related computation cost is shown in Table V.

VII. CONCLUSIONS

In this paper, we have proposed a practical and efficient fair buyer-anonymity exchange scheme using bilinear pairing. In our proposed scheme, we use bilinear pairings in elliptic curve to reduce the communication and computation cost.

TABLE V. RELATED COMPUTATION COST AND KEY SIZE BASED ON BILINEAR PAIRING

Operation	Execution time or key size
EC_A	0.213 minisecond
EC_P	63.715 miniseconds
K_S	152 bits

EC_A: The execution time of two points addition operation on elliptic curve
EC_P: The execution time for bilinear pairing operation on elliptic curve
K_S: The public/private key size based on bilinear pairing

Also, tamper-resistant smartcards are used in our proposed scheme for providing the truly offline and fair transaction. Our proposed scheme can provide the buyer-anonymity function that will attract privacy concerned customers to use this value added service. Compared with the related schemes, our proposed fair buyer-anonymity exchange scheme is more efficient, flexible, and practical for various network environments.

Acknowledgment

This work was supported in part by the National Science Council of the Republic of China under the Grant NSC 100-2221-E-327-019-MY2.

REFERENCES

[1] A. Alaraj and M. Munro, ”An Efficient e-Commerce Fair Exchange Protocol That Encourages Customer and Merchant to Be Honest,” SAFECOMP 2008, LNCS 5219, pp. 193-206, 2008.

[2] F. Bao, R. Deng and W. Mao, ”Efficient and Practical Fair Exchange Protocols With Off-line TTP,” In IEEE Symposium on Security and Privacy, pp. 77-85,1998.

[3] C. Chang and Y. Lai, ”A Flexible Date-attachment Scheme on E-cash,” *Computers & Security*, Vol. 22, No. 2, pp. 160-166, 2003.

[4] D. Chaum. ”Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms,” *Commu. of the ACM*, Vol. 24, No. 2, pp. 84-88, 1981.

[5] S. Chow, L. Hui, S. Yiu and K. Chow, ”Two Improved Partially Blind Signature Schemes From Bilinear Pairings,” Cryptology ePrint Archive, Report 2004/108.

[6] P. Ezhilchelvan and S. Shrivastava, ”A family of Trusted Third Party Based Fair-exchange Protocols,” IEEE Transactions on Dependable and Secure Computing, Vol. 2, No. 4, pp. 273-286, 2005.

[7] C. Fan and Y. Liang, ”Anonymous Fair Transaction Protocols Based on Electronic Cash,” International Journal of Electronic Commerce, Vol. 13, No. 1, pp. 131-151, 2008.

[8] N. Gonzalez-Deleito and O. Markowitch, ”Exclusions and Related Trust Relationships in Multi-party Fair Exchange Protocols,” Electronic Commerce Research and Applications, Vol. 6. No. 3, pp. 343-357, 2007.

[9] W. Juang, C. Lei and H. Liaw, ”Privacy and Anonymity Protection with Blind Threshold Signatures,” *International Journal of Electronic Commerce*, Vol. 7 , No. 2, pp. 145-159, Winter 2002-2003.

[10] W. Juang, ”D-Cash: A Flexible Pre-paid E-cash Scheme for Date-attachment,” Electronic Commerce Research and Applications, Vol. 6, No. 1, pp. 74-80, New York, Elsevier Press, 2007.

[11] A. Jurisic and A. Menezes, Elliptic Curves and Cryptography, pp.1-13, 1997.

[12] N. Koblitz, A. Menezes and S. Vanstone, ”The State of Elliptic Curve Cryptography,” Designs, Codes and Cryptography, Vol. 19, pp. 173-193, 2000.

[13] K. Lauter, ”The Advantages of Elliptic Curve Cryptography for Wireless Security,” *IEEE Wireless Communications*, Vol. 11, No. 1, pp. 62-67, 2004.

[14] A. Lenstra, E. Tromer, A. Shamir, W. Kortsmit, B. Dodson, J. Hughes and P. Leyland, ”Factoring Estimates for a 1024-bit RSA Modulus,” In Laih, C. (ed.), Advances in Cryptology-AsiaCrypt’03, Lecture Notes in Computer Science, 2894, pp. 55-74, Springer, New York, 2003.

[15] Z. Li, J. Higgins and M. Clement, ”Performance of Finite Field Arithmetic in an Elliptic Curve Cryptosystem,” Ninth IEEE International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunications Systems (MASCOTS’01), pp. 249-256, 2001.

[16] X. Liang, Z. Cao, R. Lua and L. Qin, ”Efficient and Secure Protocol in Fair Document Exchange,” Computer Standards & Interfaces, Vol. 30, No. 3, pp. 167-176, 2008.

[17] S. Lin and D. Liu, ”A Fair-Exchange and Customer-Anonymity Electronic Commerce Protocol for Digital Content Transactions,” Proceedings of 4th International Conference on Distributed Computing and Internet Technology- ICDCIT 2007, LNCS 4882, pp. 321-326, 2007.

[18] S. Micali, ”Simple and Fast Optimistic Protocols for Fair Electronic Exchange,” Proceedings of the twenty-second annual symposium on Principles of distributed computing, pp. 12-19, 2003.

[19] NIST FIPS PUB 186-2, ”Digital Signature Standard,” National Institute of Standards and Technology, U. S. Department of Commerce, 2001.

[20] NIST FIPS PUB 180-2, ”Secure Hash Standard,” National Institute of Standards and Technology, U. S. Department of Commerce, 2004.

[21] Y. Okada, Y. Manabe and T. Okamoto, ”Optimistic Fair Exchange Protocol for E-Commerce,” Proceedings of Symposium on Cryptographic and Information Security-SCIS 2006, 2006.

[22] I. Ray, I. Ray and N. Natarajan, ”An Anonymous and Failure Resilient Fair-exchange e-Commerce Protocol,” Decision Support Systems, Vol. 39, pp. 267-292, 2005.

[23] 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, No. 2, pp. 247-259, 2008.

[24] B. Schneier, Applied Cryptography, 2nd edition, John Wiley & Sons Inc., 1996.

[25] K. Takashima, ”Scaling Security of Elliptic Curves with Fast Pairing Using Efficient Endomorphisms,” IEICE Trans. on Fundamentals, Vol. E90-A, No.1, pp.152-159, 2007.

[26] H. Vogt, H. Pagnia and F. Gartner, ”Using Smart Cards for Fair Exchange,” The Second International Workshop on Electronic Commerce -WELCOM 2001, LNCS 2232, pp. 101-111, 2001.

[27] F. Zhang, R. Safavi-Naini and W. Susilo, ”An Efficient Signature Scheme from Bilinear Pairings and Its Applications,” In G. Goos, J. Hartmanis, and J. van Leeuwen (ed.), Public Key Cryptography-PKC 2004, Lecture Notes in Computer Science, 2947, pp. 277-290, Springer, New York, 2004.

[28] N. Zhang, Q. Shi, M. Merabti and R. Askwith, ”Practical and Efficient Fair Document Exchange Over Network,” The Journal of Network and Computer Applications, Vol. 29, No. 1, pp. 46-61, 2006.

[29] L. Zhang, Q. Wu and B. Qin, ”Identity-based optimistic fair exchange in the standard model,” Security and Communication Networks, doi: 10.1002/sec.652, 2012.

[30] Y. Zhao, ”An Optimistic Protocol for Distributed Fair Exchange,” Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing(IMIS), pp. 395-399, July 2012.