行政院國家科學委員會專題研究計畫 成果報告

安全的公平交換文件技術之研究與實作
研究成果報告(精簡版)

計 畫 類 別 ：個別型
計 畫 編 號 ：NSC 97-2221-E-032-019-
執 行 期 間 ：97 年 08 月 01 日至 98 年 07 月 31 日
執 行 單 位 ：淡江大學資訊工程學系

計 畫 主 持 人：黃仁俊

計畫參與人員：碩士班研究生-兼任助理人員：王維浩
碩士班研究生-兼任助理人員：劉彥甫
碩士班研究生-兼任助理人員：陳揚毅

報 告 附 件 ：出席國際會議研究心得報告及發表論文

處 理 方 式 ：本計畫可公開查詢

中 華 民 國 98 年 10 月 29 日

行政院國家科學委員會補助專題研究計畫成果報告

安全的公平交換文件技術之研究與實作

The Study and Implementation of Secure Fair Document Exchange Protocol

計畫類別：■ 個別型計畫　　□ 整合型計畫
計畫編號：NSC 97-2221-E-032 -019
執行期間：　97　年　8　月　1 日至　98　　年　7　月　31　日

計畫主持人：黃仁俊
共同主持人：
計畫參與人員：　王維浩、劉彥甫、陳揚毅

成果報告類型(依經費核定清單規定繳交)：■精簡報告　□完整報告

本成果報告包括以下應繳交之附件：
□赴國外出差或研習心得報告一份
□赴大陸地區出差或研習心得報告一份
■出席國際學術會議心得報告及發表之論文各一份
□國際合作研究計畫國外研究報告書一份

處理方式：除產學合作研究計畫、提升產業技術及人才培育研究計畫、列管計畫及下列情形者外，得立即公開查詢
□涉及專利或其他智慧財產權，□一年□二年後可公開查詢

執行單位：淡江大學資訊工程系

中　華　民　國　九十八　年　十　月　廿　日

一、英文摘要

An efficient provable fair document exchange protocol with transaction privacy is proposed in this project. The fair document exchange protocol is a primary technology of e-commerce. Transaction privacy is an important issue nowadays. In our protocol, any untrustworthy parties can fairly exchange the respective digital document without any assistance of on-line trusted third party in order to overcome the communication bottleneck problem. Furthermore, each digital document only needs to be notarized by its notary once, and the notarized document can be exchanged repeatedly to different parties without disclosing the identities of participators. According to the formally security and performance analyses, our protocol not only enhances backward secrecy, forward secrecy, message unforgeability and authorized exchange, but also reduces the computational cost and communication cost compared with previous works especially for huge documents in the multi-receivers e-commerce environment. In particular, the merchant with a large-scale digital goods or the same digital goods e-commerce transactions with a number of different customer scenarios to highlight more of the performance of our approach.

Keywords: *Digital signature; Electronic commerce*; *Fair document exchange*; *Network Security*; *Privacy*

二、中文摘要

本計畫成果設計出一有效率且具保護交易隱私的公平交換文件協定。公平交換文件協定是電子商務中一重要的基礎功能，而交易隱私權的保護也是現今討論網路交易的重要議題。在我們所設計的協定中任意雙方可以不需要線上(on-line)公證第三者協助即可達成公平文件交易以改善公證第三者協助可能成為網路交易瓶頸的問題。所交換文件，只要經由公證單位認證一次，擁有者即可與多位或多次與其他網路成員以該文件進行公平文件交換，但不會損及交易隱私或公平性，這是過去學者所提出的方法尚待努力的方向。我們以正規方法分析與論證，我們的方法不僅確實達到 strong fairness、non-repudiation 與 message confidentiality 等公平交換文件協定的基本安全功能，也強化 backward secrecy、forward secrecy、transaction privacy、message unforgeability 和 authorized exchange 等安全功能，在通訊與計算效能都比過去學者的方法略勝一籌，尤其商家以一大型數位商品或同一數位商品與多個不同客戶電子商務交易情境將更突顯我們的方法之效能。計畫成果達成我們計畫書規劃的目標而且也準備投稿到著名的電子商務期刊。

關鍵詞：數位簽章；電子商務；公平文件交換；網路安全；隱私

三、報告內容：

1. Introduction

The Internet acts as an important role of people's lives especially for Internet-based electronic commerce (e-commerce) recently. In e-commerce, both parties usually have no fully trust in each other. This problem has motivated one of the principal issues, that is, fair exchange of respective digital document between mutually mistrusting parties. For example, a customer would like to fairly purchase the digital product such as digital film, video or music from an on-line merchant using the electronic cash [21, 58]. Besides that, in order to protect the valuable documents and authenticate the legal owner, the cryptographic primitives including encryption and digital signature are usually adopted. However, for preventing fraud or misbehavior in the important business transactions, the strong fairness property, non-repudiation of origin (NOO) and non-repudiation of receipt (NOR) are necessary [5]. Hence, a fair document exchange protocol must provide following basic security requirements [52, 53]:

(1) *Strong fairness*: either each party can obtain an expected digital document from the opposing party in the end of the protocol. Otherwise, neither of them has any advantage while any party misbehaves or prematurely aborts;
(2) *Non-repudiation of origin (NOO)*: The designated receiver must have ability to prove that received document is indeed sent by the sender;
(3) *Non-repudiation of receipt (NOR)*: The sender must have ability to prove that the document is indeed received by the designated receiver;
(4) *Message confidentiality*: only the legal participators can get the expected document without disclosing any information to the adversary during transaction.

A number of fair exchange protocols have been proposed. According to the content type to be exchanged, fair exchange protocols can be classified into following types: fair document exchange protocols [2, 3, 25, 36, 52, 53, 62, 63, 64], non-repudiation protocols [23, 26, 27, 50, 56, 65], electronic contract signing protocols [6, 8, 11, 22, 24, 39, 40], certified e-mail delivery [1, 7, 18, 20, 31, 34, 37, 38, 41, 46, 47, 51, 66] and certified e-goods delivery [33 ,45, 48, 49].

The purpose of fair document exchange protocol is to provide fairly and securely exchange for any type of digital documents between mutually distrusting parties. Any type of digital document means that the message format is not restricted. For example, it may be a piece of password, business report, purchase order, video file, electronic letter, digital contract, digital cash, or digital signature. Hence, the fair document exchange protocols can be regarded as the generalization case of all kind of fair exchange protocols. Moreover, the fair document exchange protocol must exactly ensure NOO and NOR in order to provide enough arbitration evidences and to reduce the dispute while unexpectedly aborting or misbehaving during the transaction.

The on-line trusted third party (TTP) is adopted between both participators to provide fairness during each transaction [25, 35]. Unfortunately, the on-line and centralized TTP will cause the communication bottleneck and will become the target of denial-of-service attack [64]. Up to now, some fair document exchange protocols [2, 3, 36, 52, 53, 64] with the assistant of the off-line TTP are proposed. The off-line TTP only involved while dispute occurs to maintain strong fairness. The principal ideas of previous studies are firstly sending the ciphertext of his/her own document before obtaining the expect document from the opposite party. Afterward, both parties will engage in fairly exchanging the decryption keys of the ciphertext. The ciphertext must satisfy verifiability and recoverability in order to provide strong fairness. The verifiability means that the legal receiver is capable of verifying the correctness of the received ciphertext before obtaining the real document. The recoverability permits the real document can be recovered with the help of the off-line TTP while any party misbehaves or prematurely aborts.

This project proposes an efficient and provable fair digital document exchange protocol with transaction privacy. The TTP of our protocol is really off-line in Internet-based multi-receivers e-commerce environment. The proposed protocol not only achieves the basic security functionality: strong fairness, non-repudiation of origin, non-repudiation of receipt, and message confidentiality, but also provides following enhanced security functions for multi-receivers e-commerce environment:

(1) *Backward and forward secrecy*: no body except the original legal receiver can obtain the

session key in previous or next transaction even if the current session key compromised by the adversary in the multi-receivers e-commerce environment.

(2) *Transaction Privacy*: The identity of the legal participators and which documents to be exchanged can be kept secret in each transaction against the adversary. Moreover, the legal receiver finished one fair document exchange transaction still can not trace the behavior and the notarized key of the other transactions of the sender, which the sender fair exchanges the same document with another party.

(3) *Message unforgeabilty and authorized exchange*: The original owner of the notarized document can be verified to against unauthorized exchange. In other words, the proposed protocol can prevent the unauthorized party to re-exchange previously received document.

(4) *Resistance for replay attack*: no one can replay previous eavesdropped messages to impersonate the legal participators to obtain any digital documents.

Unlike the work mentioned in previous studies, furthermore, each document only needs to be notarized by the off-line notary once in our protocol. The authorized party can exchange the same document with the same *recovery certificate* to several different parties without losing the transaction privacy. Additionally, the off-line notary is needless to store any message or to maintain any public database after notarizing any digital documents. Hence, the proposed protocol is practical and cost-effective than previous works for multi-receivers e-commerce. We demonstrates the security functions of our protocol regularly. The proposed protocol reduces the computational cost and communication cost compared to the previous works especially for huge document in the multi-receivers e-commerce environment.

2. Preliminaries

Section 2.1 defines notations used in the proposed protocol. Next, Section 2.2 gives some assumptions.

2.1 Notations

- A, B: The unique identities for Alice A, Bob B, respectively.
- T: The unique identity for the notary T of Alice A.
- T′: The unique identity for the notary T′ of Bob B.
- M_A: The digital document that Alice A would like to transmit to Bob B for fair exchange.
- M_B: The digital document that Bob B would like to transmit to Alice A for fair exchange.
- $description_A$, $description_B$: the public description information of M_A and M_B, respectively.
- PR_u: RSA-based [55] private key of user U, where $PR_u=<d_u, N_u>$ and $U\in\{A, B, T, T'\}$.
- PU_u: RSA-based public key of user U, where $PU_u=<e_u, N_u>$ and $U\in\{A, B, T, T'\}$.
- K_{1A}: The notarized key randomly selected by the notary T for M_A.
- K_{1B}: the notarized key randomly selected by the notary T′ for M_B.
- K_2: the session key randomly selected by the initiator of fair exchange, i.e., Alice A.
- $a \bmod n$: a modular n.
- $E(PU_u, X)$: RSA-based encryption of plaintext X using public key PU_u, where $E(PU_u, X)=(X)^{e_u} \bmod N_u$.
- $D(PR_u, Y)$: RSA-based decryption of ciphertext Y using private key PR_u, where $D(PR_u, Y)=(Y)^{d_u} \bmod N_u$. Obviously, the equation $X=D(PR_u, E(PU_u, X))$ is satisfied.
- $S(PR_u, X)$: RSA-based signature generation of plaintext X using private key PR_u, where $S(PR_u, X)=(X)^{d_u} \bmod N_u$.
- $V(PU_u, Y)$: RSA-based message recovery of signature Y using public key PU_u, where $V(PU_u, Y)=(Y)^{e_u} \bmod N_u$. Obviously, the equation $X=V(PU_u, S(PR_u, X))$ is satisfied.
- $E[K_i, X]$: Symmetric encryption of message X using key K_i such as AES-128 [42].
- $D[K_i, Y]$: Symmetric decryption of ciphertext Y using key K_i.
- ||: $(x||y)$ represents x concatenated with y.
- ⊕: $(x \oplus y)$ represents bitwise exclusive-OR of x and y for multiple-bit variables.
- $|x|$: the bit length of the value x.
- H: the collision-resistance one-way hash function [44], where $H: \{0, 1\}^* \rightarrow \{0, 1\}^{|K_{1A}|}$.
- G: the collision-resistance one-way hash function, where $G: \{0, 1\}^* \rightarrow \{0, 1\}^{3|K_2|/2}$.

- $\Rightarrow$: A$\Rightarrow$T:{X} means that the sender A sends the messages X to the receiver T by secure channel or out-of-band method.
- $\rightarrow$: A$\rightarrow$B:{Y} means that the sender A sends the messages Y to the receiver B by public channel.

2.2 Assumptions

Without lost of generality, we assumed that Alice A want to obtain the digital document M_B from Bob B, and Bob B want to obtain the digital document M_A from Alice A in a fair way. The notaries T and T′ are the off-line third parties trusted by both Alice A and Bob B. The notary T and T′ should not conspire with any participants. Moreover, the description information of digital documents can be known by anybody.

3. Our fair document exchange protocol

Our fair document exchange protocol contains three phases: *notarization phase*, *fair exchange phase* and *arbitration phase*. In the notarization phase, the notary T assists Alice A to notarize the digital product M_A. The notary T′ assists Bob B to notarize the digital product M_B. In the fair exchange phase, Alice A can use the notarized document M_A to fairly exchange the notarized document M_B from Bob B. The involvement of the notaries T and T′ are completely needless in the fair exchange phase. If dispute or misbehavior occurs, the notary T or T′ can assist both participators retrieve their expected document in the arbitration phase. The following sections show the details of these phases. Section 3.1 describes the notarization phase. Next, the fair exchange phase is shown in Section 3.2. Finally, Section 3.3 represents the arbitration phase.

3.1 Notarization phase

In our protocol, each digital document is necessary to be notarized once by their respective notary. Each original owner can generate the related recovery certificate for his/her digital document after notarization phase. The recovery certificate is not only to maintain the strong fairness, but also to protect the digital document against unauthorized exchanging or re-distribution during fair exchange phase. Moreover, the notarized document can be exchanged to several different parties with message confidentiality and transaction privacy. Without lost of generality, we give the example to explain the procedures of the notarization phase. That is, Alice A runs the following Steps N1 to N3 to obtain the recovery certificate Ψ_A ={W_A, s_A, C_A, $description_A$, σ_A} for M_A. Similarly, Bob B will run the same procedures to obtain the recovery certificate Ψ_B ={W_B, s_B, C_B, $description_B$, σ_B} for M_B by assistance of T′.

Step N1: A$\Rightarrow$T: {M_A, $description_A$}

Alice A prepares digital document M_A and properly description information $description_A$ to send to the notary T by the secure channel or out-of-band method.

Step N2: T$\rightarrow$A: {π_A, s_A, Ω}

The notary T generates ciphertext C_A of M_A by using the notarized key K_{1A}. The public key of Alice A and ciphertext C_A will be notarized by the signature σ_A of the notary T. The notarized key K_{1A} will be protected by the warrant W_A. As the following Sub-steps N2-1 to N2-10, the notary T will generate and sends the messages {π_A, s_A, Ω} for {K_{1A}, C_A, W_A} to Alice A:

Sub-step N2-1: authenticates that Alice A is indeed the legitimate owner of M_A;
Sub-step N2-2: randomly selects the notarized key $K_{1A}=(k_{1x}||k_{1y})$, where $|k_{1x}|=|k_{1y}|=|K_{1A}|/2$;
Sub-step N2-3: selects a random integer r_1, where $|r_1|=|K_{1A}|$;
Sub-step N2-4: computes $d_1=(k_{1y}||r_1)$ and $c_1=(k_{1x}||0^{|K_{1A}|/2})\oplus H(d_1)$;
Sub-step N2-5: computes $w_A=G(c_1)\oplus d_1$ and $s_A=H(w_A)\oplus c_1$;
Sub-step N2-6: computes $\pi_A=E(PU_a, S(PR_t, w_A))$ and $C_A=E[K_{1A}, M_A]$;
Sub-step N2-7: computes warrant $W_A=E[K_t, w_A]$, where $K_t=H(PR_t)$;
Sub-step N2-8: generates the digital signature $\sigma_A=S(PR_t, H(W_A||s_A||C_A||description_A||PU_a))$;
Sub-step N2-9: computes $\Omega=E[K_{1A}, (W_A||\sigma_A)]$;
Sub-step N2-10: sends the messages {π_A, s_A, Ω} to Alice A.

Step N3: Alice A runs the following Sub-steps N3-1 to N3-8 to get the recovery certificate Ψ_A ={W_A, s_A, C_A, $description_A$, σ_A} of the notarized document M_A.

Sub-step N3-1: recovers w_A by computing $V(PU_t, D(PR_a, \pi_A))$;

Sub-step N3-2: computes c_1=H(w_A)⊕s_A and d_1=G(c_1)⊕w_A=(k_{1y}||r_1);

Sub-step N3-3: computes the value u_1=c_1⊕H(d_1) and verifies the rightmost bits of u_1 with length |u_1|/2 are all zero;

Sub-step N3-4: obtains the notarized key K_{1A} =(k_{1x}||k_{1y});

Sub-step N3-5: recovers (W_A||σ_A) by computing D[K_{1A}, Ω];

Sub-step N3-6: computes the ciphertext C_A=E[K_{1A}, M_A];

Sub-step N3-7: verifies whether V(PU_t, σ_A) is equal to H(W_A||s_A||C_A||*description*$_A$||PU_a);

Sub-step N3-8: stores the recovery certificate Ψ_A ={W_A, s_A, C_A, *description*$_A$, σ_A} of M_A.

3.2 Fair exchange phase

Without lost of generality, we assume that the initiator, Alice A, wants to obtain M_B from Bob B, and Bob B wants to get M_A from Alice A in a fair way. The detail steps of fair exchange phase are described as following Steps F1 to F4.

Step F1: A→B: {π_2, s_2, Π_2}

Alice A generates the session key K_2 and sends the messages {π_2, s_2, Π_2} to Bob B in order to protect the recovery certificate Ψ_A={W_A, s_A, C_A, *description*$_A$, σ_A} and the request information *req_info* by the following Sub-steps F1-1 to F1-8:

Sub-step F1-1: generates *req_info*=(A||B||T||T′||*description*$_A$||*description*$_B$||T_{stamp}), where T_{stamp} is the time stamp;

Sub-step F1-2: randomly selects a session key K_2=(k_{2x}||k_{2y}), where |k_{2x}|=|k_{2y}|=|K_2|/2;

Sub-step F1-3: selects a random integer r_2, where |r_2|=|K_2|;

Sub-step F1-4: computes d_2=(k_{2y}||r_2) and c_2=(k_{2x}||$0^{|K_2|/2}$)⊕H(d_2);

Sub-step F1-5: computes w_2=G(c_2)⊕d_2;

Sub-step F1-6: computes π_2=E(PU_b, (PU_a||α_A)) and s_2=H(w_2)⊕c_2, where α_A=S(PR_a, w_2);

Sub-step F1-7: computes Π_2=E[K_2, (K_2||Ψ_A||*req_info*)];

Sub-step F1-8: sends the messages {π_2, s_2, Π_2} to Bob B.

Step F2: B→A: {δ_B}

Bob B recovers the session key K_2 and Ψ_A, and then sends the ciphertext δ_B to Alice A by the following Sub-steps F2-1 to F2-10:

Sub-step F2-1: derives (PU_a||v)=D(PR_b, π_2) and recovers (w_2||h_A) by computing V(PU_a, v);

Sub-step F2-2: computes c_2=H(w_2)⊕s_2 and d_2=G(c_2)⊕w_2=(k_{2y}||r_2);

Sub-step F2-3: computes u_2=c_2⊕H(d_2)=(k_{2x}||$0^{|K_2|/2}$) and verifies the rightmost bits of u_1 with length |u_1|/2 are all zero;

Sub-step F2-4: obtains the session key K_2=(k_{2x}||k_{2y});

Sub-step F2-5: recovers (K_2′||Ψ_A||*req_info*) by computing D[K_2, Π_2];

Sub-step F2-6: checks the identities of the participators and time stamp T_{stamp} in *req_info*;

Sub-step F2-7: verifies whether K_2′ is equal to the session key K_2;

Sub-step F2-8: verifies whether V(PU_t, σ_A) is equal to H(W_A||s_A||C_A||*description*$_A$||PU_a);

Sub-step F2-9: generates the signature S_B=S(PR_b, H(*req_info*||Ψ_A||M_B));

Sub-step F2-10: sends the message δ_B=E[K_2, (K_{1B}||Ψ_B||S_B||PU_b)] back to Alice A, where K_{1B} is the notarized key obtained from the notarization phase by the notary T′.

Step F3: A→B: {δ_A}

Alice A recovers the expected M_B, and sends back the ciphertext δ_A to Bob B by the following Sub-steps F3-1 to F3-5:

Sub-step F3-1: derives (K_{1B}||Ψ_B||S_B||PU_b) by computing D[K_2, δ_B] and gets M_B =D[K_{1B}, C_B];

Sub-step F3-2: verifies whether V($PU_{t'}$, σ_B) is equal to H(W_B||s_B||C_B||*description*$_B$||PU_b);

Sub-step F3-3: verifies whether V(PU_b, S_B) is equal to H(*req_info*||Ψ_A||M_B);

Sub-step F3-4: generates the receipt S_A=S(PR_a, H(*req_info*||M_A||M_B));

Sub-step F3-5: sends the message δ_A=E[K_2, (K_{1A}||S_A)] to Bob B.

Step F4: Bob B runs the following Sub-steps F4-1 to F4-2 to verify the expected M_A:

Sub-step F4-1: recovers (K_{1A}||S_A) by computing D[K_2, δ_A], and obtains M_A=D[K_{1A}, C_A].

Sub-step F4-2: verifies whether V(PU_a, S_A) is equal to H(*req_info*||M_A||M_B). If verification is

valid, the fair exchange phase is complete. Otherwise, Bob B can initiate the arbitration phase to maintain strong fairness.

3.3 Arbitration phase

Any participators can prematurely stop to run next steps in the fair exchange phase. According to Table 1, we show all possible cases for arbitration during fair exchange phase. Case 1 means that Alice A tries to initiate arbitration phase after sending $\{\pi_2, s_2, \Pi_2\}$ of Step F1 of the fair exchange phase. However, the notary will not help Alice A to recover M_B because of lacking of recovery certificate Ψ_B for M_B. Case 2 means that Bob B prematurely stops to run the following steps, and tries to obtain M_A by directly initiating arbitration phase. Although Bob B is able to get M_A in the arbitration phase, the notary will also help Alice A to get M_B, simultaneously. In Case 3, one of participators has already obtained the expected document from the opposite party but stops to run the Steps F2, F3 or F4 and tries to make the unfair situation. In Case 3, because of any parties have already obtained enough recovery information for their expected document, they can initiate the arbitration phase to recover their expected document to maintain the strong fairness. Hence, the arbitration phase is designed to be able to satisfy strong fairness in any cases as shown in Table 1.

Table 1: All cases for arbitration during fair exchange phase

	Request for arbitration from Alice A	Request for arbitration from Bob B
After Step F1	Case 1	Case 2
After Steps F2, F3 or F4	Case 3	Case 3

Case 1: Alice A tries to initiate arbitration phase after sending messages $\{\pi_2, s_2, \Pi_2\}$ of Step F1.
Case 2: Bob B prematurely stops to run following steps, and directly initiates arbitration phase.
Case 3: Alice A or Bob B directly performs arbitration phase without sending her/his document.

Without lost of generality, we use Case 3 of Table 1 to explain the procedures of the arbitration phase. While Alice A has already received M_B from Step F2 of fair exchange phase and prematurely stops to run Step F3, Bob B can provide messages from Step F1 to recover M_A by initiating the arbitration phase. The notary T can perform the following Steps T1 to T2 to recover M_A for Bob B and M_B for Alice A, simultaneously.

Step T1: B⇒T: $\{M_B, \Psi_B, \Psi_A, req\_info, w_2, v, PU_a\}$

The requester, Bob B, must send his own document M_B with its recovery certificate Ψ_B and the previously received messages $\{\Psi_A, req\_info, w_2, v, PU_a\}$ of Step F2 of fair exchange phase to the notary T of Alice A by secure channel.

Step T2: T⇒A: $\{M_B, \Psi_B\}$ and T⇒B: $\{M_A, \Psi_A\}$

The notary T runs the following Sub-steps T2-1 to T2-7 to verify the request messages and send back $\{M_B, \Psi_B\}$ to Alice A and $\{M_A, \Psi_A\}$ to Bob B by secure channel, simultaneously:

Sub-step T2-1: verifies whether $V(PU_a, v)$ is equal to $(w_2 || H(\Psi_A || req\_info))$;

Sub-step T2-2: verifies whether $V(PU_t, \sigma_A)$ is equal to $H(W_A||s_A||C_A||description_A||PU_a)$ and $V(PU_{t'}, \sigma_B)$ is equal to $H(W_B||s_B||C_B||description_B||PU_b)$;

Sub-step T2-3: recovers $w_A=D[K_t, W_A]$, where warrant W_A is included in Ψ_A and $K_t=H(PR_t)$;

Sub-step T2-4: recovers the notarized key K_{1A} using the values $\{w_A, s_A\}$ by the procedures as same as Sub-step N3-2 to Sub-step N3-4 of the notarization phase above.

Sub-step T2-5: recovers the digital document $M_A=D[K_{1A}, C_A]$.

Sub-step T2-6: verifies M_A by $description_A$ and M_B by $description_B$;

Sub-step T2-7: sends $\{M_B, \Psi_B\}$ to Alice A and sends $\{M_A, \Psi_A\}$ to Bob B by secure channel, simultaneously. For example, the notary can encrypt messages by using the public key of the designated recipient.

4. Discussions

This section analyzes the performances of ours and previous works [2, 3, 36, 52, 53, 64] for fair document exchange. Section 4.1 makes the comparisons with functionalities among ours and previous works. Next, the computational cost is demonstrated in Section 4.2. At last, Section 4.3 shows the comparison results about the communication cost.

4.1 The comparisons of functionalities

Security functionalities are the most important issues for fair document exchange protocols especially in multi-receivers e-commerce environment. Section 4 already has demonstrated that our proposed protocol can provide message confidentiality, backward and forward secrecy, transaction privacy, non-repudiation of origin (NOO), non-repudiation of receipt (NOR), authorized exchanging, strong fairness, and resistance of replay attack. However, no of previous works [2, 3, 36, 52, 53, 64] can support all of these functionalities as ours. The comparison results are shown in Table 2. As described in Section 1, the transaction privacy, the message confidentiality and backward/forward secrecy of previous works such as [2, 3, 52, 53, 64] will be compromised while one party attempts to fairly exchange the same document to a number of different parties without re-encrypting the document and re-generating new *certified commitment* by the off-line TTP. In addition, Alaraj and Munro's protocols [2, 3] and Liang et al.'s protocol [36] do not provide non-repudiation of receipt (NOR) for both participators. Zhang et al.'s protocol [64] only provide NOO and NOR for one party. Hence, previous works [2, 3, 36, 64] do not provide enough arbitration evidences when unexpectedly aborting or misbehaving during the transaction. Alaraj and Munro's protocols [2, 3] require each party to run pre-exchange phase to obtain the authorized certificate for his/her document from the off-line TTP. Thus, only our protocol and Alaraj and Munro's protocols [2, 3] provide authorized exchange function. Moreover, the replay attack is only considered in ours and Ray et al's protocols [52, 53]. The encryption method of fair document exchange protocol will influence the computational performance, because the exchanged document may be a very huge digital product such as the video. Our protocol and previous works [2, 3, 64] is efficient for the huge documents because of using the symmetric encryption algorithm.

Table 2: The comparisons based on functionalities

	Ours	Alaraj et al. [2, 3]	Liang et al. [36]	Ray et al. [52, 53]	Zhang et al. [64]
Message confidentiality	Yes	Yes	Yes	Yes	Yes
Backward/Forward secrecy	Yes	No	Yes	No	No
Transaction privacy	Yes	No	Yes	No	No
Non-repudiation of origin	Yes	Yes	Partial	Yes	Partial
Non-repudiation of receipt	Yes	No	No	Yes	Partial
Authorized exchange	Yes	Yes	No	No	No
Strong fairness	Yes	Yes	Yes	Yes	Yes
Resistance for replay attack	Yes	No	No	Yes	No
Efficiency for huge document	Yes	Yes	No	No	Yes
The TTP should be on-line in multi-receivers e-commerce environment	No	Yes	No	Yes	Yes

4.2 The comparisons of computational cost

In the previous protocols [2, 3, 36, 52, 53, 64] and ours, the heaviest operations during fair document exchange protocols are the admissible bilinear pairing [9, 13] and modular exponentiation (i.e., RSA-based signing, decryption, verification and encryption [55]), which take more computational cost than the other operations including modular multiplication, modular addition, one-way hash function and symmetric encryption [32, 60]. Hence, we will ignore the computational cost of modular multiplication, modular addition, one-way hash function and symmetric encryption in the comparison results. By Cao et al.'s results [15], the computational time of public key operations under the same security strength are shown in Table 3, where $T_{RSA\text{-}SIG\text{-}DEC}$, $T_{RSA\text{-}VFY\text{-}ENC}$, T_{PAIR}, and T_{ECSM}, denote one RSA signing/decryption with 1024-bit modulus, one RSA verification/encryption with 1024-bit modulus, one admissible bilinear pairing,

and one elliptic curve-based scalar multiplication as suggested by IEEE Standard P1363.3 [30], respectively. All the public key operations are built with MIRACL [57], a standard cryptographic library. The implementation platform is on a 32 bit Intel Pentium IV processor at 3GHz with 512-MB memory and Microsoft Windows XP operation system. Table 4 shows the comparison results of main computational cost for the fair exchange phase. Clearly, the previous works [2, 3, 36, 52, 53, 64] take more computational cost than ours.

Table 3: Computational time on different public key-based operations [15]

Operation	Computational time (in milliseconds)
RSA verification and encryption ($T_{RSA\text{-}VFY\text{-}ENC}$)	0.20
RSA signing and decryption ($T_{RSA\text{-}SIG\text{-}DEC}$)	3.84
Elliptic curve-based scalar multiplication (T_{ECSM})	6.38
Pairing (T_{PAIR})	20.04

Table 4: The comparisons based on the main computational cost in the fair exchange phase

Various protocols	Main computational cost (in milliseconds)	Faster than previous works	Document encryption method
Our protocol	$6\times T_{RSA\text{-}VFY\text{-}ENC}+4\times T_{RSA\text{-}SIG\text{-}DEC}$ **≈ 15.36 ms**	-	symmetric
Alaraj-Munro [2]	$6\times T_{RSA\text{-}VFY\text{-}ENC}+5\times T_{RSA\text{-}SIG\text{-}DEC}$ **≈ 20.4 ms**	24.7%	symmetric
Alaraj-Munro [3]	$7\times T_{RSA\text{-}VFY\text{-}ENC}+7\times T_{RSA\text{-}SIG\text{-}DEC}$ **≈ 28.28 ms**	45.7%	symmetric
Liang et al. [36]	$5\times T_{ECSM}+2\times T_{PAIR}$ **≈71.98 ms**	78.7%	asymmetric
Ray et al. [52, 53]	$16\times T_{RSA\text{-}VFY\text{-}ENC}+11\times T_{RSA\text{-}SIG\text{-}DEC}$ **≈ 45.44 ms**	66.2%	asymmetric
Zhang et al. [64]	$12\times T_{RSA\text{-}VFY\text{-}ENC}+8\times T_{RSA\text{-}SIG\text{-}DEC}$ **≈ 33.12 ms**	53.6%	symmetric

Note: $T_{RSA\text{-}VFY\text{-}ENC}\approx 0.20$ms, $T_{RSA\text{-}SIG\text{-}DEC}\approx 3.84$ms, $T_{ECSM}\approx 6.38$ms, and $T_{PAIR}\approx 20.04$ms [15].

4.3 The comparisons of communication cost

National Institute of Standards and Technology (NIST) [43] provides comparable security strengths for the approved cryptographic algorithms. According to the recommended key lengths from NIST, AES-128 has the same security strength as RSA with modulus sizes of 3072 bit. Under above security strength, Table 5 shows the comparisons for total communication cost and the amounts of message during transaction (#round) in the fair exchange phase, while AES-128 and RSA-3072 are used. Moreover, Alaraj and Munro's protocols [2, 3] also need to take the communication cost of the irrefutable receipts into account when they want to provide non-repudiation of receipt. Obviously, our protocol has lower communication cost to provide complete functionalities.

Table 5: The comparisons of the communication cost in the fair exchange phase

Various protocols	Total communication cost (bits)	reducing communication cost than previous works	#rounds
Our protocol	$\|M_A\|+\|M_B\|+20144$ (with irrefutable receipt)	-	3
Alaraj and Munro [2]	$\|M_A\|+\|M_B\|+21896$	8.0%	3
Alaraj and Munro [3]	$\|M_A\|+\|M_B\|+31760$	36.6%	4
Ray et al. [52, 53]	$\|M_A\|+2\|M_B\|+33792$ (with irrefutable receipt)	40.4% + $\|M_B\|$	5

Zhang et al. [64]	$\|M_A\|+\|M_B\|+24760$ (with irrefutable receipt)	18.6%	4

5. Conclusions

This Project proposes an efficient provable fair document exchange protocol with transaction privacy for the multi-receivers e-commerce environment. Each digital document only needs to be notarized once by assistance of off-line notary. The authorized owners can continually do fair exchange with different parties without disclosing the privacy of participators. As the security analyses, our protocol not only provides principal security requirements of fair document exchange, but also enhances backward/forward secrecy, transaction privacy and authorized exchange. It provides the strongest security protection, while the remaining ones provide only partial security functionalities. Moreover, our fair document exchange protocol is actually an efficient scheme for the multi-receivers e-commerce environment by the considerations of the communication and computational costs.

四、計畫成果自評

本計畫依循計畫書規劃內容進行研發設計，提出一公平交換文件協定相較於相關研究的技術不僅確實達到 strong fairness、non-repudiation 與 message confidentiality 等公平交換文件協定的基本安全功能，也強化 backward secrecy、forward secrecy、transaction privacy、message unforgeability 和 authorized exchange 等安全功能，並以較嚴謹的正規方法論證我們提出之方法的安全性，礙於篇幅我們在本成果報告書沒有納入論證內容，但將併入學術論文一併發表，此外我們的方法在通訊與計算效能都比過去學者的方法略勝一籌相關分析請參考報告內容之第 4 節分析。此外在電子商務中常見的商家以一大型數位商品或同一數位商品與多個不同客戶進行交易，在此交易情境將更顯我們的方法的效能，而這也是過去一些相關研究之技術在實用上較弱的一環。最後我們也實作部份功能以瞭解運作效能。綜合而論，我們計畫成果符合計畫書之目標，我們的方法提供較多的安全功能且有正規的分析論證，加上其效能又較相關研究技術高，所以我們認為有投稿到學術期刊之價值，目前也準備投稿到 International Journal of Electronic Commerce，其 Impact factor 為 1.366。

五、參考文獻

1. Abadi, M.; Glew, N.; Horne, B.; and Pinkas, B. Certified email with a light on-line trusted third party: design and implementation. *Proceedings of 2002 International World Wide Web Conference*, (May 2002), 387-395.
2. Alaraj, A. and Munro, M. An e-commerce fair exchange protocol that enforces the customer to be honest. *International Journal of Product Lifecycle Management*, 3, 2/3 (2008), 114-131.
3. Alaraj, A. and Munro, M. An efficient e-commerce fair exchange protocol that encourages customer and merchant to be honest. *Proceedings of the 27th international conference on Computer Safety, Reliability, and Security*, 5219, (September 2008), 193-206.
4. Arnab, A. and Hutchison, A. Digital rights management – a current review. *Technical Report CS04-04-00, Department of Computer Science, University of Cape Town*, (April 2004), http://pubs.cs.uct.ac.za/archive/00000114/, Accessed on September 30, 2009.
5. Asokan, N.; Schunter, M.; and Waidner, M. Optimistic protocols for fair exchange. *Proceedings of the 4th ACM conference on Computer and communications security*, (April 1997), 7-17.
6. Asokan, N.; Schunter, M.; and Waidner, M. Optimistic fair exchange of digital signatures. *IEEE Journal on Selected Areas in Communications*, 18, 4 (April 2000), 593-610.
7. Bahreman, A. and Tygar, J.D. Certified electronic mail. *Proceedings of Symposium on Network and Distributed Systems Security*, (1994), 3-19.
8. Bao, F.; Wang, G.; Zhou, J.; and Zhu, H. Analysis and improvement of Micali's fair contract signing protocol. *Information Security and Privacy*, LNCS 3108, (2004), 176-187.
9. Barreto, P.; Kim, H.; Bynn, B.; and Scott, M. Efficient algorithms for pairing-based cryptosystems. *Proceedings of CRYPTO 2002*, LNCS 2442, (2002), 354-368.
10. Bellare, M. and Rogaway, P. Random oracles are practical: A paradigm for designing efficient protocols. *Proceedings of the 1st ACM Conference on Computer and Communication Security*, (Nov. 1993), 62-73.
11. Ben-Or, M.; Goldreich, O.; Micali, S.; Rivest, R.L. A fair protocol for signing contracts. *IEEE Transactions on Information Theory*, 36, (1990), 40-46.
12. Buhse, W. and Meer, J. The open mobile alliance digital rights management. *IEEE Signal Processing Magazine*, (2007), 140-143.
13. Boneh, D. and Franklin, M. Identiy-based encryption from Weil pairing. *Proceedings of CRYPTO 2001*, LNCS 2139, (2001), 213-229.
14. Boneh, D.; Gentry, C.; Lynn, B.; and Shacham, H. Aggregate and verifiably encrypted signatures from bilinear maps. *Proceedings of EUROCRYPT 2003*, LNCS 2656, (2003), 416-432.
15. Cao, X.; Zeng, X.; Kou, W.; and Hu, L. Identity-based anonymous remote authentication for value-added services in mobile networks. *IEEE Transactions on Vehicular Technology*, 58, 7 (September 2009), 3508-3517.
16. Chen, C.-L. A secure and traceable E-DRM system based on mobile device. *Expect System with Applications*, 35, 3 (2007), 878-886.
17. Chen, L; Kudla, C.; Paterson, G.K. Concurrent signatures. *Proceedings of EUROCRYPT 2004*, LNCS 3027, (2004), 287-305.
18. Deng, R.; Gong, L.; Lazar, A.; and Wang, W. Practical protocol for certified electronic mail. *Journal of Network and Systems Management*, 4, 3 (1996), 279-297.
19. Dhawan, P., Microsoft Developer Network (MSDN), *Performance Comparison: Security Design Choices*, October 2002, http://msdn.microsoft.com/en-us/library/ms978415.aspx, Accessed on September 30, 2009.
20. Dodis, Y.; Lee, P. J.; and Yum, D. H. Optimistic fair exchange in a multi-user setting. *Journal of Universal Computer Science*, 14, (2008), 318-346.
21. Fan, C.-I; Huang, S.-Y.; Ho, P.-H.; and Lei, C.-L. Fair anonymous rewarding based on electronic cash. *Journal of Systems and Software*, 82, 7 (July 2009), 1168-1176.
22. Frikken, K.B. and Atallah, M.J. Achieving fairness in private contract negotiation. *Proceedings of the 9th Financial Cryptography and Data Security*, LNCS 3570, (2005)

270-284.
23. Gao, W.; Li, F.; and Xu, B. An abuse-free optimistic fair exchange protocol based on BLS signature, *International Conference on Computational Intelligence and Security*, 2, (2008), 278-282.
24. Garay, J.A. and Pomerance, C. Timed fair exchange of standard signatures: [extended abstract]. *Proceedings of the 7th Financial Cryptography and Data Security*, LNCS 2742, (2004) 190-207.
25. Gonza'lez-Deleito, N. and Markowitch, O. Exclusions and related trust relationships in multi-party fair exchange protocols. *Electronic Commerce Research and Applications*, 6, (2007) 343-357.
26. Gurgens, S.; Rudolph, C.; and Vogt, H. On the security of fair non-repudiation protocols. *Proceedings of Information Security Conference*, LNCS 2851, (2003) 193-207.
27. Hernandez-Ardieta, J.L.; Gonzalez-Tablas, A.I.; and Alvarez, B.R. An optimistic fair exchange protocol based on signature policies. *Computers & Security*, 27, (2008), 309-322.
28. Huang, Z.; Huang, R.; and Lin, X. Perfect concurrent signature protocol, *Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing*, 1, (2007) 467-472.
29. Huang, Z.; Lin, X.; and Huang, R. Certificateless concurrent signature scheme. *Proceedings of the 9th International Conference for Young Computer Scientists*, (2008), 2102-2107.
30. *IEEE P1363.3: Standard for identity-based cryptographic techniques using pairings*, IEEE P1363.3, (April 2008).
31. Imamoto, K. and Sakurai, K. A certified email system with receiver's selective usage of delivery authority. *Proceedings of Indocrypt 2002*, LNCS 2551, (2002), 326-338.
32. Jakobsson, M. and Mao W. *Cryptographic Protocols: Techniques for Secure Protocol Design*. New Jersey: Prentice Hall, 2008.
33. Konar, D. and Mazumdar C. A generalised model of e-trading for gradual secret release fair exchange protocol. *International Journal of Electronic Security and Digital Forensics*, 2, (Mar. 2009), 101-111.
34. Kremer, S. and Markowitch, O. Selective receipt in certified e-mail. *Proceedings of Indocrypt 2001*, LNCS 2247, (2001), 136-148.
35. Li, X.; Wang, Q.; and Chen, L. Analysis on cyclic multi-party fair exchange protocols. *International Conference on Computer Science and Software Engineering*, 3, (2008), 601-604.
36. Liang, X.; Cao, Z.; Lu R.; and Qin L. Efficient and secure protocol in fair document exchange, *Computer Standards & Interfaces*, 30, (2008), 167-176.
37. Ma, C.; Li, S.; Chen, K.; and Liu, S. Analysis and improvement of fair certified e-mail delivery protocol. *Computer Standards & Interfaces*, 28, (2006), 467-474.
38. Ma, X.-L.; Cui, W.; Gu, L.-Z.; Yang, Y.-X.; and Hu, Z.-M. A novel id-based verifiably encrypted signature without random oracle. *International Conference on Computational Intelligence and Security*, 2, (2008), 359-363.
39. Mukhamedov, A. and Ryan, M. Fair multi-party contract signing using private contract signatures. *Information and Computation*, 206, (2008), 272-290.
40. Mukhamedov, A. and Ryan, M. Improved multi-party contract signing. *Proceedings of the 11th Financial Cryptography and Data Security*, LNCS 4535, (2007).
41. Monteiro, J.R.M. and Dahab, R. An attack on a protocol for certified delivery. *Proceedings of Information Security Conference*, LNCS 2433, (2002), 428-436.
42. National Bureau of Standards (NBS). NBS FIPS PUBS 197, *Advanced Encryption Standard, U.S. Department of Commerce*, (November 2001).
43. National Institute of Standards and Technology (NIST), Special Publication (SP) 800-57, *Part 1, Recommend for key management: General (Revised)*, (March 2007).
44. National Institute of Standards and Technology (NIST), FIPS PUB 180-3, *Secure Hash Standard (SHS)*, (Oct. 2008).
45. Nenadic, A.; Zhang, N.; and Barton S. A security protocol for certified e-goods delivery. *Proceedings of IEEE International Conference on Information Technology, Coding and*

Computing (ITCC 2004)-Information Assurance and Security Track, (2004), 22-28.
46. Nenadic, A.; Zhang, N.; and Barton S. Fair certified e-mail delivery. *Proceedings of the 9th ACM Symposium on Applied Computing-Computer Security Track*, (2004), 391-396.
47. Nenadic, A.; Zhang, N.; Shi, Q.; and Goble, C. Certified e-mail delivery with DSA receipts. *Proceedings of 19th IEEE International Parallel and Distributed Processing Symposium*, 1, (2005), 4-8.
48. Nenadic, A.; Zhang, N.; Shi, Q.; and Goble, C. DSA-based verifiable and recoverable encryption of signatures and its application in certified w-goods delivery. *Proceedings of IEEE Conference on e-Technology, e-Commerce and e-Service*, (2005) 94-99.
49. Nenadic, A.; Zhang, N.; Cheetham, B.; and Goble, C. RSA-based certified delivery of e-goods using verifiable and recoverable signature encryption. *Journal of Universal Computer Science*, 11, (2005) 175-192.
50. Onieva, J.; Lopez, J.; Roman, R.; Zhou, J.; and Gritzalis S. Integration of non-repudiation services in mobile DRM scenarios. *Telecommunication Systems*, 35, (2007), 161-176.
51. Oppliger, R. Certified mail: the next challenge for secure messaging. *Communications of the ACM*, 47, (2004), 75-79.
52. Ray, I.; Ray I.; and Natarajan, N. An anonymous and failure resilient fair-exchange e-commerce protocol. *Decision Support Systems*, 39, 3 (May 2005), 267-292.
53. Ray, I.; Zhang, H. Experiences in developing a fair-exchange e-commerce protocol using common off-the-shelf components. *Electronic Commerce Research and Applications*, (March 2007).
54. Rivest, R. and Kaliski B. RSA Problem. *Encyclopedia of Cryptography and Security*, 2005.
55. Rivest, R.; Shamir, A.; and Adleman, L. A method for obtaining digital signature and public key cryptosystems. *Communications of the ACM*, 21, 2 (Feb. 1978), 120-126.
56. Schmidt, A.; Kuntze, N.; and Hett, C. Non-repudiation in Internet telephony. *IFIP International Information Security Conference*, (2007) 361-372.
57. Shamus Software Limited. *Multiprecision Integer and Rational Arithmetic C/C++ Library (MIRACL)*, March 2009, http://www.shamus.ie/, Accessed on October 1, 2009.
58. Simplot-Ryl, I.; Traore, I.; and Everaere, P. Distributed architectures for electronic cash schemes: a survey. *International Journal of Parallel, Emergent and Distributed Systems*, 24, 3 (June 2009), 243-271.
59. Sun, H.-M.; Hung, C.-F.; and Chen, C.-M. An improved digital rights management system based on smart cards. *Digital EcoSystems and Technologies Conference*, (2007), 308-313.
60. Stallings W. *Cryptography and Network Security Principles and Practices, Fourth Edition*. New Jersey: Prentice Hall, (2005).
61. Wolf, M. *Security Engineering for Vehicular IT Systems: Improving the Trustworthiness and Dependability of Automotive IT Applications, 1st Edition*. Germany: Vieweg+Teubner, (2009).
62. Zhang, N.; Shi, Q.; and Merabti, M. An efficient protocol for anonymous and fair document exchange. *Computer Networks*, 41, (2003), 19-28.
63. Zhang, N.; Shi, Q.; and Merabti, M. A unified approach to a fair document exchange system. *The Journal of Systems and Software*, 72, (2004), 83-96.
64. Zhang, N.; Shi, Q.; Merabti, M.; and Askwith, R. Practical and efficient fair document exchange over networks. *Journal of Network and Computer Applications*, 29, (2006), 46-61.
65. Zhou, J. and Gollman, D. A fair non-repudiation protocol. *IEEE Symposium on Security and Privacy*, (1996), 55-61.
66. Zhou, J.; Onieva, J.; and Lopez, J. Optimized multi-party certified email protocols. *Information Management & Computer Security*, 13, (2005), 350-366.

六、附件：出席國際學術會議報告

行政院國家科學委員會補助國內專家學者出席國際學術會議報告

98 年　07 月 10 日

報告人姓名	黃仁俊	服務機關及職稱	淡江大學資訊工程系副教授
會議時間地點	98/7/5~98/7/8 韓國濟州島	本會核定補助文號	NSC 97-2221-E-032 -019 –
會議名稱	(中文) 24 屆國際電路/系統,電腦與通訊技術學術研討會 (英文) The 24th International Technical Conference on Circuits/Systems, Computers and Communications		

由今年三、四月全球 H1N1 流感在各國逐步漫延尤以美國最嚴重，甚至被 WHO 國際衛生組織發佈第六級警戒；又投稿國際學術會議論文，均有與會出席報告之義務，因此在 H1N1 疫情不明的狀況下，對於最晚在三、四月期間截止投稿並將於暑期舉行的國際學術研討會，不敢冒然投稿，也沒有規劃參加，但六月底時據報導 H1N1 雖還在流行但影響人體似乎不嚴重，故規劃善用此經費參加在韓國濟州島由 IEICE 國際知名學會支持舉辦的 The 24th International Technical Conference on Circuits/Systems, Computers and Communications，以促進國際學術交流，但已來不及投稿發表論文，僅出席參加。

目前由台灣到濟州島的飛機並不是很方便，除了到韓國再轉機到濟州島外，就得透過旅行社想辦法買包機直飛的機票，而包機幾天才有一班且有固定去回日期同時機位通常都被旅行團佔滿，前者交通方式費時但選擇日期有彈性，後者省時但日期必需配合包機，碰巧我透過旅行社買到 7/5 去 7/8 回華信航空包機，才解決此次會議的交通。

會議是在濟州市的 KAL Hotel 舉辦，此次出席參加者以韓國人佔大部份，其次為日本人，再者有部份我們國人、泰國人、中國人、法國人與美國人等，其中以亞洲人居多，整個會議的安排與規劃尚稱妥善便利。

The 24th International Technical Conference on Circuits/Systems, Computers and Communications 自 1986 首屆舉辦迄今已有廿四個年頭，算是很有歷史的一項學術研討會，學術領域涵概電路/系統,電腦與通訊技術，其中也包括資通安全相關的論文，今年共有廿三篇分四個 Session 進行，雖是研討會但其中有韓國 Kyung Hee 大學的學者針對 SHA-1 提出改良的技術屬應有較深入理論探討的論文，該方法以虛擬隨機亂數取代原始 SHA-1 的邏輯運算，其宣稱改良後的 Hash 結果使得每一訊息所產生的 Hash 值都唯一，但其改良的方法，卻犧牲了 Hash function 該有的函數定義域很大但對應域相對很

小的特性，且作者群可能受限於論文篇幅，使得論文的推論嚴謹性有待加強的空間，上台報告也因時間因素，蜻蜓點水帶過，實屬可惜。另外，日本 Okayama 大學學者提出 AES 的 S-Box 的 Inversion 也屬理論性質偏重的研究成果，然其口頭報告時，礙於時間因素，理論的論述說明極少，而論文內容也可能因論文篇幅的限制，使得論文的推論內容深度與嚴謹性有待加強的空間。其他廿一篇資通安全相關的論文，則較偏應用。經個人多次參加國際學術研討會的經驗，覺得國際學術研討會，受限於時間因素，通常每篇論文報告時間約十五至二十分鐘，而論文集對每篇論文的頁數也多所限制，因此對於需較深入探討或理論推論的論文主題似乎比較不適合，讀者或與會者對此類論文要完整瞭解作者的研究方法與成果，有一定的難度。學術會議似乎比較適合學者們針對一些應用性方向的論文或研究概念與方向，做討論與分享，而參加會議的學者也可從其中瞭解別人的研究方向與趨勢，這是研討會一個很重要的功能，畢竟研討會論文從完成到接受發表的期程遠短於期刊論文，期刊論文雖然通常比較嚴謹深入，篇幅也較多，但一般讀者能取得研讀的時間大部份是撰寫完成後一年，技術的新鮮度恐怕不足。

感謝國科會在本年度核定計畫經費中包含出席國際會議的費用，使得個人有機會了解多位他國學者在資通安全目前的研究方向與趨勢並與其交流。

行政院國家科學委員會補助國內專家學者出席國際學術會議報告

98 年　07 月 10 日

報告人姓名	黃仁俊	服務機關及職稱	淡江大學資訊工程系副教授
會議時間地點	98/7/5~98/7/8 韓國濟州島	本會核定補助文號	NSC 97-2221-E-032 -019 –
會議名稱	(中文) 24 屆國際電路/系統,電腦與通訊技術學術研討會 (英文) The 24th International Technical Conference on Circuits/Systems, Computers and Communications		

由今年三、四月全球 H1N1 流感在各國逐步漫延尤以美國最嚴重，甚至被 WHO 國際衛生組織發佈第六級警戒；又投稿國際學術會議論文，均有與會出席報告之義務，因此在 H1N1 疫情不明的狀況下，對於最晚在三、四月期間截止投稿並將於暑期舉行的國際學術研討會，不敢冒然投稿，也沒有規劃參加，但六月底時據報導 H1N1 雖還在流行但影響人體似乎不嚴重，故規劃善用此經費參加在韓國濟州島由 IEICE 國際知名學會支持舉辦的 The 24th International Technical Conference on Circuits/Systems, Computers and Communications，以促進國際學術交流，但已來不及投稿發表論文，僅出席參加。

目前由台灣到濟州島的飛機並不是很方便，除了到韓國再轉機到濟州島外，就得透過旅行社想辦法買包機直飛的機票，而包機幾天才有一班且有固定去回日期同時機位通常都被旅行團佔滿，前者交通方式費時但選擇日期有彈性，後者省時但日期必需配合包機，碰巧我透過旅行社買到 7/5 去 7/8 回華信航空包機，才解決此次會議的交通。

會議是在濟州市的 KAL Hotel 舉辦，此次出席參加者以韓國人佔大部份，其次為日本人，再者有部份我們國人、泰國人、中國人、法國人與美國人等，其中以亞洲人居多，整個會議的安排與規劃尚稱妥善便利。

The 24th International Technical Conference on Circuits/Systems, Computers and Communications 自 1986 首屆舉辦迄今已有廿四個年頭，算是很有歷史的一項學術研討會，學術領域涵概電路/系統,電腦與通訊技術，其中也包括資通安全相關的論文，今年共有廿三篇分四個 Session 進行，雖是研討會但其中有韓國 Kyung Hee 大學的學者針對 SHA-1 提出改良的技術屬應有較深入理論探討的論文，該方法以虛擬隨機亂數取代原始 SHA-1 的邏輯運算，其宣稱改良後的 Hash 結果使得每一訊息所產生的 Hash 值都唯一，但其改良的方法，卻犧牲了 Hash function 該有的函數定義域很大但對應域相對很

小的特性，且作者群可能受限於論文篇幅，使得論文的推論嚴謹性有待加強的空間，上台報告也因時間因素，蜻蜓點水帶過，實屬可惜。另外，日本 Okayama 大學學者提出 AES 的 S-Box 的 Inversion 也屬理論性質偏重的研究成果，然其口頭報告時，礙於時間因素，理論的論述說明極少，而論文內容也可能因論文篇幅的限制，使得論文的推論內容深度與嚴謹性有待加強的空間。其他廿一篇資通安全相關的論文，則較偏應用。經個人多次參加國際學術研討會的經驗，覺得國際學術研討會，受限於時間因素，通常每篇論文報告時間約十五至二十分鐘，而論文集對每篇論文的頁數也多所限制，因此對於需較深入探討或理論推論的論文主題似乎比較不適合，讀者或與會者對此類論文要完整瞭解作者的研究方法與成果，有一定的難度。學術會議似乎比較適合學者們針對一些應用性方向的論文或研究概念與方向，做討論與分享，而參加會議的學者也可從其中瞭解別人的研究方向與趨勢，這是研討會一個很重要的功能，畢竟研討會論文從完成到接受發表的期程遠短於期刊論文，期刊論文雖然通常比較嚴謹深入，篇幅也較多，但一般讀者能取得研讀的時間大部份是撰寫完成後一年，技術的新鮮度恐怕不足。

感謝國科會在本年度核定計畫經費中包含出席國際會議的費用，使得個人有機會了解多位他國學者在資通安全目前的研究方向與趨勢並與其交流。