南　華　大　學

資訊管理學系

碩士論文

基於使用者驗證的金鑰協議安全及模糊傳輸之研究

Security of Key Agreement and Oblivious Transfer Based on User Authenticated

研 究 生：侯咸伍

指導教授：周志賢 博士

中華民國 九十七 年 六 月

南　華　大　學

（系所名稱）

碩 士 學 位 論 文

基於使用者驗證的金鑰協議安全及模糊傳輸之研究

Security of key agreement and oblivious transfer based on user authenticated

研究生：侯咸伍

經考試合格特此證明

口試委員：

指導教授：周志賢

系主任(所長)：

口試日期：中華民國　97年　6月　26日

誌　　謝

在工作上伙伴的支持和朋友不斷的鼓勵下，讓我有機會實現進修的想法及機會，進入資管所重拾課業開啟了我人生另一個嶄新的體驗，轉眼三年研究所生涯即將劃下句點，回首進入研究所以來的點點滴滴，真是「如人飲水」其中甘苦只有自己才能體會。能順利走到這個階段，首先我要感謝指導老師周志賢博士，在他那嚴謹作風的指導下，不僅彫鑿出我追根究底的研究精神，問題的分析能力更養成我畏難的學習態度。三年下來苦樂參半，感謝研究室的夥伴雅玲學姊、彰原、宗亨、啟峰，不時在學業上提出的寶貴意見及觀念，讓我獲益良多。還有感謝士軒、其模及同學們，不僅是課上同甘共苦的伙伴，對於工作上的經驗分享、及長久以來的相互支持鼓勵，讓我在研究學業上增加不少信心，也是研究所生涯最令人難以忘懷的。同時更要感謝我親愛的家人，有他們的支持，讓我才能無後顧之憂安心完成研究所的學業。

基於使用者驗證的金鑰協議安全及模糊傳輸之研究

學生：侯咸伍　　指導教授：周志賢 博士

南　華　大　學　資訊管理學系碩士班

摘　　要

在現今網路快速發展的世界裡，資訊大量的公開交換取得，造成有心人士可以輕易的竊取、偽造他人訊息，因此為保障重要資訊交換的安全性，人們常採取許多的安全措施，其中常見的有加密及模糊傳輸這兩種技術。首先以金鑰協商技術來說，溝通兩方在傳輸重要訊息前先行協議建立一把共享的秘密金鑰，在 2005 年時 Zhou 他們提出一個應用憑證以達到遠端使用者身份相互認證及會議金鑰協議。不過他的架構存在著安全上的弱點，也就是無法阻擋攻擊者的偽裝攻擊。其次，在 n 個訊息中挑選 k 個的模糊傳輸的技術來說，接收端只能從 n 個訊息中獲得到 k 個，而傳送端無法得知接收端所挑選的 k 個訊息，在 2006 年時 Kim 他們發展出一個使用RSA加密方式的安全驗證非交換作用的糊模傳輸，不過我們發現他們的架構存在著安全上的弱點，無法抵擋攻擊者的偽裝攻擊。

因此，在本篇論文我們將個別的分析 Zhou 和 Kim 的架構，指出其安全上的弱點，並提出偽裝攻擊的演算法。我們將提出一個基於橢圓雙曲線的 n 選 k 模糊傳輸，以達到使用者相互身份驗證及有效率溝通的安全性需求，同時在安全性和溝通效率上與現存的其它方法提出比較。

關鍵字：金鑰協議、身份認證、模糊傳輸、偽裝攻擊

Security of Key Agreement and Oblivious Transfer Based on User Authenticated

Student：Xian-Wu Hou Advisors：Dr. Jue-Sam Chou

Department of Information Management
The M.I.M. Program
Nan-Hua University

ABSTRACT

The key agreement and oblivious transfer (OT) is an important primitive for designing secure protocols. At first, in the method of key agreement, two parties can establish a common secret session key over an insecure. In 2005, Zhou et al. proposed an end-to-end security protocol with certificate-based authentication to mutually authentication and session key agreement. But their scheme is suffers from the impersonation attack, it cannot achieve the claimed security. Secondly, in the oblivious transfer protocol, the sender has n encrypted messages to be sending to the receiver while the receiver only intends to get k messages among the n transmitted messages, the sender cannot figure out which messages the receiver selected. In 2006, Kim et al. proposed secure verifiable non-interactive oblivious transfer protocol using RSA. However, we found that their protocol suffers from impersonation attack.

We will take cryptanalysis of Zhou et al. scheme and Kim et al. scheme and propose impersonation attack for Zhou et al. scheme and Kim et al. scheme. We present an efficient mutual authentication k-out-of-n oblivious transfer protocol based on bilinear pairing, which offers the security requirements of mutual authentication and is communicationally efficient while compared with all of the existing schemes.

Keywords: key agreement, user authentication, oblivious transfer, impersonation attack

目　錄

List of Table

List of Figures

Chapter 1 Introduction

Diffie–Hellman key agreement protocol [2] is a famous scheme that two parties can establish a common secret session key over an insecure network. However, it does not authenticate the other party, thus suffers from the main-in-the-middle attack. In 1997, Pack [4] first discussed the certificate based protocols for wireless mobile communicates systems. In 2004, based on [4], Chang et al. [3] propose a certificate-based authentication combined with a session key agreement protocol. In their scheme, the session key agreement protocol is based on the Diffie-Hellman key exchange protocol. In 2005, Zhou et al. [1] pointed out that Chang et al.'s scheme is vulnerable to the impersonation attack, and proposed an improved scheme to prevent this security flaw. However, after our analysis, we find that Zhou's protocol is still insecure against the impersonation attack as well. We will show that by presenting a simple but powerful attack against their protocol.

Secondly, Oblivious transfer (OT) is an important primitive for designing secure protocols and has been widely used as a building block for secure communications. It is a two-party protocol between a sender and a receiver. The requirement is that the sender cannot figure out which part of the encrypted messages transmitted are known to the receiver while the receiver can learn only the messages he had selected in advance. In 1981, Rabin [9] first proposed the concept of oblivious transfer, in which the sender sends an encrypted message to the receiver and the receiver can decrypt the message with probability 1/2. In 1985, Even et al. [9] presented

a generalized 1-out-of-2 oblivious transfer protocol (OT_2^1) in which the sender sends two encrypted messages and the receiver can decrypt only one message that he had chosen in advance. In 1987, Crepeau [31] also proved the equivalence of OT_2^1 scheme and Rabin's OT scheme. In 1986, Brassard et al. [5] further extended 1-out-of-2 OT to 1-out-of-*n* OT (OT_n^1) for the case of *n* messages.

The more general case is *k*-out-of-*n* OT (OT_n^k) in which the sender possesses *n* messages and the receiver can only obtains *k* messages of them, where $k < n$ an OT_n^k scheme can be straightly constructed by executing *k* times of OT_n^1 scheme. However, such construction needs 2*k* rounds communication cost under the case that OT_2^1 is a two-round protocol. Many OT_n^k schemes [6, 7, 10, 12, 21, 22, 23, 24, 33] were proposed to have a better performance in round efficiency. Among these schemes, Chu et al.'s [6] has the best round efficiency. It needs only 2 rounds with $1024*(n+k+1)$ bits sent from the sender to the receiver and 1024*k* bits from the receiver to the sender. In 2007, Camenish et al. [7] presented a simulatable adaptive OT_n^k with stronger security, which allows the receiver to choose the *k* messages one by one adaptively. In 2008, Chang et al. [27] presented a OT_n^k based on blind signature and Chinese remainder theorem. Although Chang et al. claims that their scheme can achieve reducing bandwidth consumption, but its communication time is longer that their scheme requires three rounds.

The other studies [7, 11, 14, 17, 18, 25] in OT are diverse. In 2000, Naor-Pinkas [25] presented distributed OT_2^1 protocol. The sender distributes her messages among *n* servers, and the receiver task is to make contact with *k* servers in order to get one of these messages. However, in 2007, Ghodosi [7] pointed out that Naor-Pinkas OT_n^1 scheme [25] is vulnerable to the collaborating-server attack. In 2006, Peng [17] et al. presented an OT_n^1 protocol to be employed in the optimization of bid validity verification. In 2006, Parakh [18] also presented an OT scheme using elliptic curve, in order to increase the efficiency of performance. Although Parakh claims that their scheme can achieve oblivious transfer between two parties, we find that their protocol has a mistake. Since in the protocol, they assume that sender A has two points on an elliptic curve with two secret scalar multipliers respectly and the receiver B can retrieve one of these two secrets. However it is impossible for B to deduce such a scalar from a point on an elliptic curve due to the ECDLP. Hence, their assumption is incorrect. In 2007, Halevi et al. [14] presented a smooth projective hashing and two-message oblivious transfer. Their constructions do not need the requirement that the underlying RSA-composite is a product of safe primes. These recent studies are not the focus of this paper.

However, all of the above mentioned OT protocols [6, 10, 12, 18, 20, 21, 22, 23, 24] lack mutual authentication. It must be assumed that the two communicating parties communicate through a secure channel. For preventing attacks in an open environment such as internet, in 2006, Kim et al. [15] adopted additional functions into the OT_2^1 protocol so that the

receiver can authenticate the sender and prevent sender's repudiation. However, we found that their protocol suffers from the impersonation attack. We will analyze Kim et al.'s scheme later.

We present an efficient mutual authentication OT_n^k protocol based on bilinear pairing, which offers the security requirements of mutual authentication and is computationally efficient while compared with all of the existing schemes. Moreover, the proposed scheme can resist various attacks. The structure of this thesis is organized as follows. Chapter 2 is preliminaries. Chapter 3 is review of Zhou et al. scheme and Kim et al. scheme. After that, we show our protocol in Chapter 4. Then the security analysis and bandwidth consumption comparisons are made in Chapter 5. Finally, a conclusion is given in Chapter 6.

Chapter 2 Preliminaries

2.1 Bilinear pairings

In 1984, Shamir [19] proposed an ID-based encryption and signature scheme, in which each user uses his identity as his public key. This makes the key distribution easier than the conventional ones. In 1993, Menezes et al. [28] proposed the concept of elliptic curve attempting to attain the same securing level with less computational cost. In 2001, Boneh and Franklin [26] first proposed a practical ID-based cryptosystem using bilinear paring on elliptic curve. Since then, bilinear pairings, such as Weil pairing and Tate pairing, defined on elliptic curves applied to cryptosystem gradually. Many protocols have been designed based on the Weil pairing [8, 16]. Now, we briefly introduce Weil paring which will be applied in our study as follows.

Let P be a generator of group G_1 over a elliptic curve with order q and G_2 be a multiplicative group of the same order. It is assumed that solving the discrete logarithm problem (DLP) in both G_1 and G_2 is difficult. Let e: $G_1 \times G_1 \rightarrow G_2$ be the Weil pairing which has following properties [28].

(1) Identity: For all $P \in G_1$, $e(P,P)=1$.

(2) Alternation: For all $P_1, P_2 \in G_1$, $e(P_1,P_2)= e(P_2,P_1)$.

(3) Bilinearity: For all $P_1, P_2, P_3 \in G_1$, $e(P_1+ P_2, P_3)= e(P_1,P_3)\, e(P_2,P_3)$.

(4) Nondegeneracy: IF $P_1 \in G_1$, then $e(P_1,O)=1$. If $e(P_1,P_2)=1$ for all $P_2 \in G_1$, then $P_1=O$.

In the following, some assumptions related to our study are listed below.

(1) Computational Diffie-Hellman problem (CDHP): The CDHP is to compute abP when given P, aP and bP, where $a, b \in Z_q^*$.

(2) Discrete logarithm problem (DLP): The DLP is to compute a when given aP, where $a \in Z_q^*$.

(3) Bilinear computational Diffie-Hellman problem (BCDHP): The BCDHP is to compute $e(P,P)^{abc}$ when given P, aP, bP and cP, where a, b and $c \in Z_q^*$.

2.2 The security requirements of the oblivious transfer

In an OT_n^k scheme, the sender sends n encrypted messages to the receiver while the receiver only can to get k messages which he had selected in advance among the n transmitted messages. It should satisfy the following security requirements.

(1) The receiver's privacy: after performing the protocol, the sender cannot figure out which messages the receiver selected.

(2) The sender's privacy: the receiver cannot get any knowledge about other messages that he did not choose.

Chapter 3 Review Related Paper

3.1 Review of Zhou et al.'s protocol

In this section, we briefly review Zhou et al.'s scheme [1], then analyze the security features of their scheme.

3.1.1 Zhou et al.'s protocol

In a typical mobile communication system (e.g., GSM), communication between two mobile stations (MS) is usually established with the aid of two base stations (BS). It is usually that both the subscriber account information and the personal certificates of the mobile users are stored in the Subscriber Identity Module (SIM) card. Several parameters in Chang et al.'s protocol [3] which are also used in Zhou's protocol [1] are discussed as follows:

Let g be a generator of the multiplicative group Z_p^*, where p is a prime, and both g and p are made public. The private key of MS is $X_M \in Z_p^*$ and the public key is $Y_M = g^{-X_M} \bmod p$. Similarly, the private key and public key of BS are $X_B \in Z_p^*$ and $Y_B = g^{-X_B} \bmod p$, respectively. For simplicity, we will omit the operator " mod p" henceforth. The certificates of both MS and BS are represented in the following.

$$Cert_M = (ID_M, Y_M, data_M, [h(ID_M, Y_M, data_M)S_{CA}]),$$
$$Cert_B = (ID_B, Y_B, data_B, [h(ID_B, Y_B, data_B)S_{CA}]),$$

where $h(ID_i, R_i, data_i)S_{CA}$ means the hash value is signed by a CA's private key, S_{CA}. Both the private key X_M and the certificate $Cert_M$ of user M are

stored in the SIM card. They wished their protocol [3] to be a perfect protocol. However, in 2005, Zhou et al. [1] pointed out that their protocol is insecure. Besides, they also proposed an improvement. In the following, we only show Chang et al.'s protocol in figure 1 and omit the details.

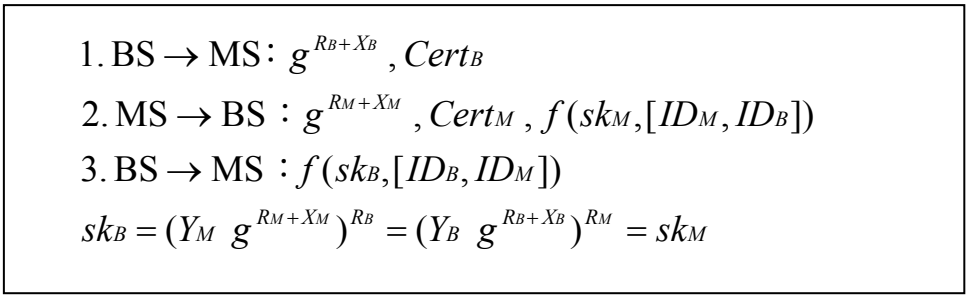

Figure 1: Chang's Protocol.

As for Zhou's protocol, we describe it as follows and illustrate it in figure 2.

(1) BS randomly selects a number R_B, then computes g^{R_B}, and sends g^{R_B}, $Cert_B$ to MS.

(2) MS randomly selects a number R_M, computes g^{R_M} and $sk_M=Y_B^{R_M}(g^{R_B})^{-X_M}$, where the public key of BS, Y_B, can be obtained from $Cert_B$. Finally, MS sends the message $<g^{R_M}, Cert_M, f(2,sk_M,[ID_M,ID_B,g^{R_M},g^{R_B}])>$ to BS.

(3) BS computes $sk_B=Y_M^{R_B}(g^{R_M})^{-X_B}$, and uses thus session key to check the validity of $f(2,sk_M,[ID_M,ID_B,g^{R_M},g^{R_B}])$. Finally, BS sends the message $f(3,sk_B,[ID_B,ID_M,g^{R_B},g^{R_M}])$ to MS. BS and MS can confirm each other's identity and session key after executing their protocol.

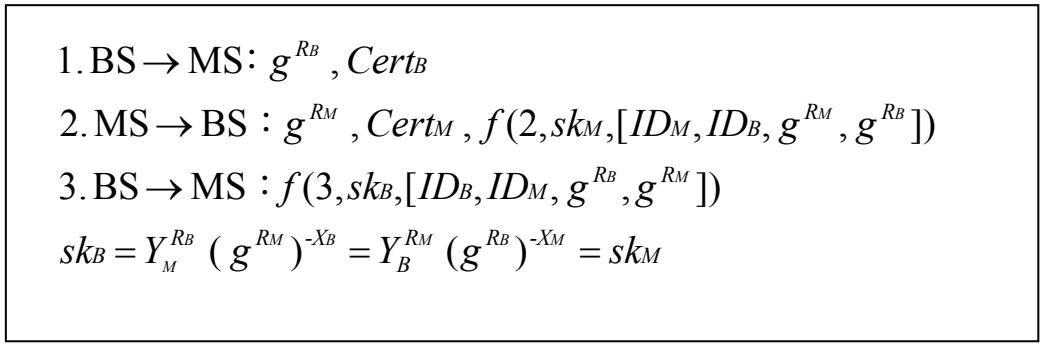

Figure 2: Zhou's Protocol.

3.1.2 Cryptanalysis of Zhou et al.'s protocol

Although, Zhou et al. claimed that their scheme can resist against the impersonation attack. However, we still can find its mistake as illustrated in figure 3.

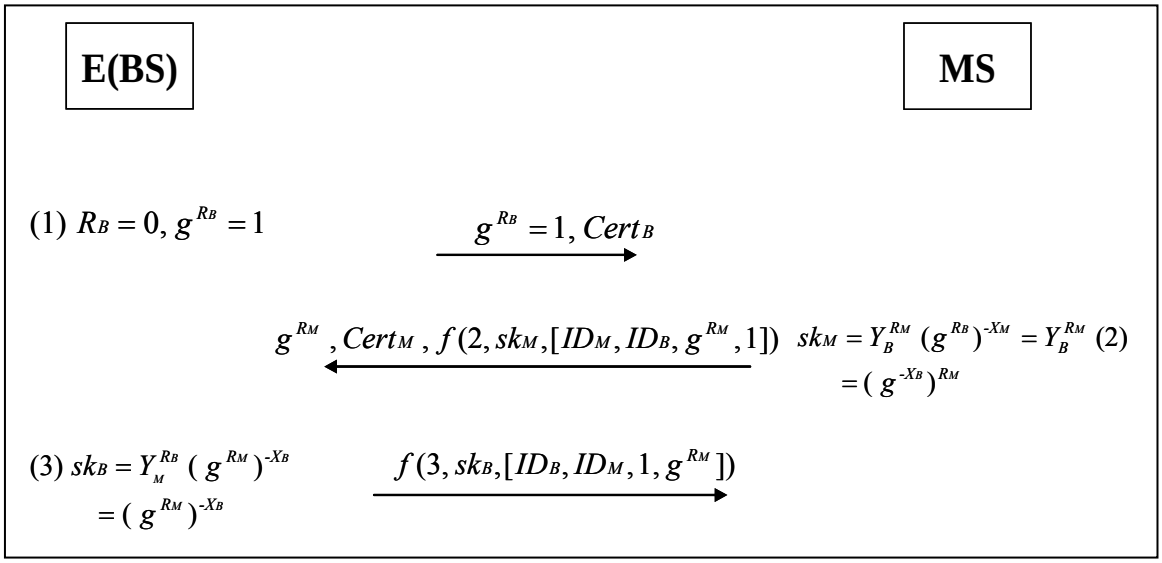

Figure 3: Impersonation attack against Zhou's protocol.

In our attack, we assume that an adversary E wants to impersonate BS to MS. We show our impersonation attack against the Zhou et al.'s protocol as follows.

(1) The adversary E selects R_B=0 and computes g^{R_B}=1, then he send 1, and $Cert_B$ to MS.

(2) MS randomly selects a number R_M, computes g^{R_M} and $sk_M = Y_B^{R_M} (g^{R_B})^{-X_M} = Y_B^{R_M} = (g^{-X_B})^{R_M}$, where the public key of BS, Y_B, can be obtained from $Cert_B$, then computes the hash value, $f(2, sk_M, [ID_M, ID_B, g^{R_M}, 1])$. Finally, MS sends the message $< g^{R_M}, Cert_M, f(2, sk_M, [ID_M, ID_B, g^{R_M}, 1]) >$ to BS.

(3) Because R_B=0, the adversary E computes $sk_B = Y_M^{R_B} (g^{R_M})^{-X_B} = (g^{R_M})^{-X_B}$. Then E can check to see if the received hash code $f(2, sk_M, [ID_M, ID_B, g^{R_M}, 1])$ is valid using the computed session key sk_B. If it is valid, E sends the message $f(3, sk_B, [ID_B, ID_M, 1, g^{R_M}])$ to MS. It is obvious that E can cheat MS successfully.

Conversely, an adversary E can also successfully impersonate MS to BS in the same way. We omit the details.

3.2 Review of Kim et al.s' protocol

3.2.1 Kim et al.'s OT_2^1 protocol

In 2006, Kim et al. proposed a secure verifiable non-interactive oblivious transfer protocols using RSA. Their method hopes to enable the receiver to authenticate the sender and prevent the sender from denying what he/she had sent. Their protocol contains two phases: (1) pre-processing phase and (2) obliviously transferring phase. We describe their scheme as follows and illustrate it in figure 1.

(1) Pre-processing phase

In this phase, the system, Alice and Bob perform the following four

steps:

(a) A large prime p, a generator g of Z_p^*, and a parameter $C \in Z_p^*$ are stored in the public directory.

(b) Bob selects a secret random number x and then publishes his OT public key as $\left(\beta_0,\ \beta_1\right) = \left(g^x, \frac{c}{g^x}\right)$ or $\left(\frac{c}{g^x}, g^x\right)$.

(c) Alice checks whether $\beta_0 \cdot \beta_1 = C$ holds. If it holds, Alice accepts the validity of Bob's OT public key (β_0, β_1).

(d) Bob has his RSA private key d_B and public key (n_B, e_B); Alice has her RSA private key d_A and public key (n_A, e_A).

(2) **Obliviously transferring phase:**

when Alice wants to obliviously transfer messages to Bob, they run their non-interactive oblivious transformation (NIOT) protocol as follows:

(a) Alice encrypts messages m_0 and m_1 by using Elgamal encryption scheme, producing $X_0 \equiv \left(g^{k_0}, m_0 \beta_0^{\ k_0}\right)$, $X_1 \equiv \left(g^{k_1}, m_1 \beta_1^{\ k_1}\right)$, and $X_A \equiv \left(X_0, X_1\right)$, where k_0 and k_1 are random integers from Z_p^*. Then, Alice signs on the message M_A which he wants to send to Bob with her RSA private key and encrypts the result with Bob's RSA public key, obtaining C_A. That is, $C_A = (M_A^{\ d_A} \bmod n_A)^{e_B} \bmod n_B$. Finally, Alice sends X_A, M_A and C_A to Bob.

(b) After receiving X_A, M_A and C_A, Bob decrypts C_A by computing $(C_A^{\ d_B} \bmod n_B)^{n_A} \bmod n_A$ to obtain M'_A. Then, he compares the equality of M_A and M'_A. If they are the same, Bob authenticates Alice's

identify; otherwise, Bob drops the receiving message.

(c) Finally, Bob can obtain the plaintext m_0 or m_1 that he has set in the pre-processing phase. Since he knows the secret random number x, by using the decryption of Elgamal, if he sets (β_0, β_1) as ($g^x, \frac{c}{g^x}$), he can obtain m_0. Else, if he sets (β_0, β_1) as ($\frac{c}{g^x}, g^x$), he can obtain m_1

Alice	Bob
(1) pre-processing phase:	
RSA public key: (n_A, e_A) RSA private key: d_A	OT public key: $(\beta_0, \beta_1) = \left(g^x, \frac{c}{g^x}\right)$ or $\left(\frac{c}{g^x}, g^x\right)$ OT private key: x RSA public key: (n_B, e_B) RSA private key: d_B
(2) obliviously transferring phase: 1. computes Elgamel encryptions for message m_0 and m_1 $X_0 = (g^{k_0}, m_0\beta^{k_0})$, $X_1 = (g^{k_1}, m_1\beta^{k_1})$, and $X_A = (X_0, X_1)$, where $k_0, k_1 \in_R Z_q^*$. 2. computes $C_A = (M_A{}^{d_A} \bmod n_A)^{e_B} \bmod n_B$, where M_A is a message from Alice to Bob. Alic $\xrightarrow{X_A, M_A, C_A}$ Bob	
	1. computes $M'_A = (C_A{}^{d_B} \bmod n_B)^{e_A} \bmod n_A$. 2. if $M'_A \neq M_A$ stops. 3. computes plaintext $m_b = m_b\beta_b^{k_b}/(g^{k_b})^x$, where $b \in \{0,1\}$.

Figure 4: Kim et al.s' protocol

3.2.2 Cryptanalysis of Kim's NIOT scheme

Although, Kim et al. claimed that, in their scheme, Bob can authenticate Alice and prevent Alice's denial of what she had sent by checking whether $M_A = (C_A^{d_B} \bmod n_B)^{e_A} \bmod n_A$ holds. However, X_A has never been signed by Alice. Hence, it exposes a serious vulnerability that any adversary E can impersonate Alice to communicate with Bob. We describe this impersonation attack as follows：

(1) When E intercepts X_A , C_A and M_A sent from Alice to Bob, he can compute another couple $(X_0', X_1')(= X_A')$ in the same manner specified in Section 3.(2).(a). Then he sends X_A' and C_A , M_A to Bob.

(2) After receiving X_A', C_A and M_A from E , Bob will verify the received message as being authentic if $M_A = (C_A^{d_B} \bmod n_B)^{e_A} \bmod n_A$. Thus, adversary E can easily impersonate Alice to communicate with Bob.

Moreover, since that (n_A, e_A) and (n_B, e_B) are Alice's and Bob's public keys, respectively. If $n_A > n_B$, then the message cannot be recovered by Bob. This is known as the reblocking problem [29].

Chapter 4 Proposed scheme

In this section, we describe our mutual authentication OT_n^k scheme using bilinear pairing. Although the performance of implementing bilinear pairings are generally more expensive than other cryptographic operations such as elliptic curve and modulo exponentiation [23], it can make key distribution easier. Moreover, if the protocol is well designed, it can resist KCI attack which means that, to some extent, it is more robust in security than the other kind of cryptographic protocols.

In our scheme, we assume that there exists a key generation center (KGC). It initially selects q, G_1, G_2, and e as defined in Section 2.1. It also chooses P as the generator of G_1 and defines two one-way hash functions $H_1:\{0;1\}^* \rightarrow G_1$ and $H_2:\{0,1\}^* \rightarrow \{0,1\}^{\iota}$. Moreover, it selects $s \in Z_q^*$ as secure master key and computes its corresponding public key $P_{pub}=sP$, then it publishes the system public parameters, $\{G_1, G_2, e, q, P, P_{pub}, H, H_1\}$. After that, an user U, can register his/her identity ID_U to KGC. KGC will compute a public/private key pair Q_U/S_U for U, where $Q_U = H_1(ID_U)$ and $S_U = sQ_U$. When a sender (owning Q_S/S_S) possessing n messages, $m_1, m_2, \ldots$ and m_n, wants to obliviously transfer messages $m_1, m_2, \ldots$ and m_n messages to the receiver (owning Q_R/S_R), they will execute the following protocol, where $\sigma_1, \sigma_2, \ldots$ and σ_k are the choice indices selected by the receiver in advance. The protocol is also depicted in Figure 5.

(1) The receiver randomly chooses two integers, a and $b \in Z_q^*$, and

compute $V=abQ_R$ and $V_j = bH(\sigma_j)S_R$, where j=1,2,…,k. Then, he generates a signature by computing $h = H(V)$ and $S = hS_R$. Finally, he sends ID_R, V, $V_1, \ldots V_k$ and S to the sender.

(2) On receiving ID_R, V, $V_1, \ldots V_K$ and S from the receiver, the sender computes $h = H(V)$ and verifies the receiver's signature by checking whether the equation $e(P,S) = e(P_{pub}, hQ_R)$ holds. If it holds, he believes that the receiver is the intended party. Then, he randomly chooses an integer $c \in Z_q^*$, and computes $U_j = cV_j, c_i = m_i \oplus H(e(H(i)V, S_S)^c)$, where j=1,…,k, i=1,…,n. He then sends $U_1, \ldots, U_k, c_1, \ldots$ and c_n to the receiver.

(3) On receiving the message $U_1, \ldots, U_j, c_1, \ldots$and c_n, the receiver can obtain the intended k plaintexts by computing $m_{\sigma_j} = c_{\sigma_j} \oplus H(e(U_j, Q_s)^a)$, for j=1 to k.

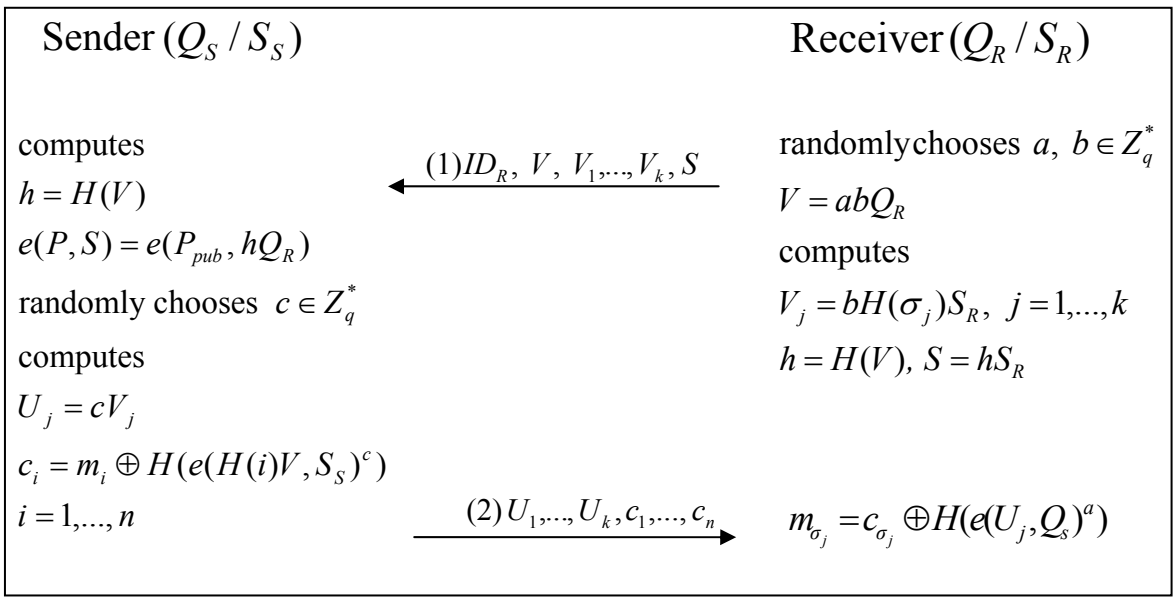

Figure 5: The proposed k-out-of-n OT scheme

Chapter 5 Security analysis and bandwidth comparisons

5.1 Security analysis

In this section, we will analyze our protocol to show that it satisfies the security requirements of an OT scheme by using the following claims.

Claim1. Correctness: if the receiver properly executes the protocol, he can obtain the exact *k* messages.

Proof: it can be easily seen that the receiver will obtain the exact *k* messages he selected by computing

$$c_{\sigma_j} \oplus H(e(U_j, Q_s)^a) = c_{\sigma_j} \oplus H(e(H(\sigma_j)bcsQ_R, Q_s)^a)$$

$$= c_{\sigma_j} \oplus H(e(H(\sigma_j)abQ_R, sQ_s)^c) = c_{\sigma_j} \oplus H(e(H(\sigma_j)V, S_S)^c) = m_{\sigma_j}.$$

Claim2. The proposed scheme satisfies the receiver's privacy.

Proof: In our scheme, the receiver chooses a randomized factor *b* each time to protect his choice indices σ_j by the form of $V_j = bH(\sigma_j)S_R$, where σ_j is the choice indices, *j*=1,2,…,*k*, and S_R is the receiver's private key. Nobody except the receiver can obtain m_{σ_j}, the clear message of his choice σ_j, since he does not know the secrecy S_R and random number *b*. Even the attacker can know the secrecy S_R, without the knowledge of *b* and σ_j, he can not compute $bH(\sigma_j)$ to obtain V_j which is necessary for the sender to

compute U_j and then for the receiver to decrypt c_{σ_j}.

Claim3. The proposed scheme satisfies the sender's privacy.

Proof: Since the messages m_i are masked by XOR operation with $H(e(H(i)V, S_S)^c)$, and the sender just sends $U_1, U_2, ...\text{and}\, U_k$ to the receiver, the receiver can get only k messages, $m_{\sigma_1}, m_{\sigma_2}, ...\text{and}\, m_{\sigma_k}$. For the other unselected encrypted messages $c_i = m_i \oplus H(e(H(i)V, S_S)^c)$ for $i \notin \sigma_1, \sigma_2, ..\sigma_k$, for decryption the receiver would get the plaintext only in case that he could compute the value of $H(e(H(i)V, S_S)^c)$. However, we know that $e(H(i)V, S_S)^c = e(H(i)abQ_R, sQ_S)^c = e(H(i)abS_R, Q_S)^c$. Although the receiver can compute $e(H(i)abS_R, Q_S)$, he cannot compute $e(H(i)abS_R, Q_S)^c$ due to lack of knowledge c.

Claim4. The proposed scheme can achieve mutual authentication.

Proof: Obviously, the sender can verify the identity of the receiver by authenticating it's signature which we have described in (2) of Section4. Now, we will show that how the receiver can authenticate the sender. As the ciphertext $c_i = m_i \oplus H(e(H(i)V, S_S)^c)$ is calculated by using the sender's private key S_S, the receiver can compute the planintext m_{σ_j} only via using sender's public key Q_S. This means that only the true sender can compute proper c_i, for i=1 to n; thus, the receiver can authenticate the sender.

Claim5. The proposed scheme can resist replay attack**.**

Proof: Assume that an adversary eavesdrops on the receiver's OT request and replays it later. When he receives the sender's response ($U_1,\ldots,U_k$, $c_1,\ldots,c_n$), he can not decrypt any one of the n encrypted messages $c_i, i = 1 \text{ to } n$ by computing $m_i = c_i \oplus H((e(U_j, Q_S)^a))$ since he hasn't the knowledge a. It is computationally infeasible for him to extract a from $V = abQ_R$ due to the ECDLP assumption.

Claim6. The proposed scheme can resist KCI attack.

Proof: KCI attack means that when the secret key of a member has been compromised, an adversary can impersonate the other member to communicate with him. To illustrate our assertion, in the following, we consider two cases, (a) and (b), of KCI attacks.

(a) Suppose that the sender's private key $S_S (= sQ_S)$ has been compromised by an adversary E and E tries to impersonate the receiver R to communicate with him. It can be easily seen that E will fail in such attack. For E dose not have the receiver's private key, E can not successfully forge $V', V_j' \text{ and } S'$ to be verified as valid by the sender, where S' is a signature of the receiver. Therefore, E can not succeed in such attack.

(b) Suppose that R's private key $S_R (= sQ_R)$ had been compromised by an adversary E and E tries to impersonate the sender S to communicate with him. We argue that E will fail.

It is because *E* can not compute the valid ciphertext c_i since he knows none of the knowledge of the sender's private key S_S.

Form the above analysis of (a) and (b), we prove the claim.

Claim7. The proposed scheme can resist man-in the –middle attack (MIMA).

Proof: MIMA is an attack that an adversary *E* slinkingly intercepts the communication line between the two communicating parties and uses some means to make them believe that they are talking to the intended party. Figure 6 illustrates the scenario of such MIMA. We argue that the adversary *E* cannot succeed in this scenario. First, *E* can not generate message (2) since he can not forge a valid signature S' to be verified by the sender without the knowledge of Receiver's private key. Secondly, although *E* can replace V with $V' = a'b'Q_R$, U_j with $U'_j = c'V_j$. However, he can't compute $e(H(i)V', S_S)^{c'} = e(H(i)a'b'S_R, Q_S)^{c'}$. For he does not know S_R. Without the knowledge of S_R *E* cannot correctly decrypt c_i or forge any valid $c'_1,...,c'_n$ which each is computed by

$c'_i = m'_i \oplus H(e(H(i)V, S_S)^c)$

$= m'_i \oplus H(e(H(i)abQ_R, S_S)^c) = m'_i \oplus H(e(H(i)abS_R, Q_S)^c)$, where m'_i is E's forged message. Therefore, we can conclude that our scheme can resist against MIMA attack.

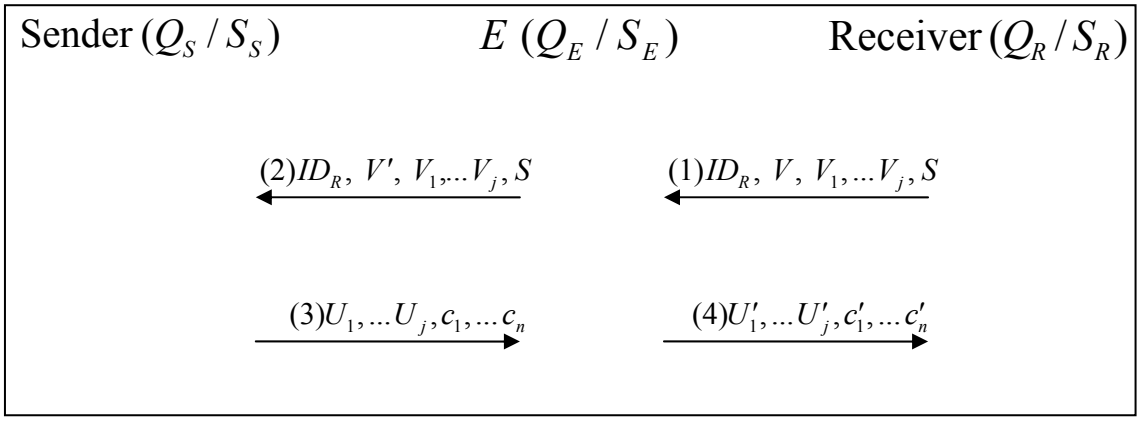

Figure 6: The scenario of man-in-the-middle attack

5.2 Bandwidth consumption comparisons

Bandwidth consumption is an important consideration in a busy network in which the time is not so critical, for example, the end-of-day financial settlement for the commercial transactions in a day. Due to OT_n^k scheme is more general and practical for real applications than the other OT schemes, in this paper, we focus our comparisons on the bandwidth consumption of our OT_n^k with the other existing OT_n^k schemes. To our best knowledge, Chu et al. [6] is the most efficient OT_n^k scheme at present. Hence, we will compare the bandwidth consumption of our scheme with Chu et al.'s. In addition, we also compare our scheme with some other famous OT_n^k schemes such as, [23] and [24], and recent OT_n^k studies [10, 22].

For the computation in RSA/Elgamal cryptographic system is typically 1024 bits long. Elliptic curves (ECC) has an computational advantage than RSA/Elgamal, it uses only a 160 bit key to provide the same level of security. Suppose our scheme $|ID_R|$ is equals to 160 bits, the receiver sends

ID_R, V, $V_1,\ldots,V_k$ and S to the sender, the size of message transmitted is 160$*$(k+2) bits from the receiver to the sender. And the sender sends $U_1,\ldots,U_k,c_1,\ldots,c_n$ to the receiver, the size of message transmitted is 160$*$(n+k) bits from the sender to the receiver. However, the scheme of Chu et al. [6] use of Elgamal cryptographic encryption system. It therefore has 1024k bits transmitted from the receiver to the sender, and 1024$*$(n+k+1) bits transmitted from the sender to the receiver. Green et al. [10] use proof of knowledge (Pok) in his scheme. The size of message transmitted is 160$*$(2k+n)+2$*$|Pok| bits from the sender to the receiver and $k*$|Pok| bits from receiver to sender, where |Pok| is the bit length of a message element transmitted by a proof a knowledge scheme. Moreover, Green et al. [10] also presented an OT_n^k scheme that the receiver can extract decryption keys by adopting blind ID-based encryption [30]. However, us found that it can not achieve mutual authentication for it uses the indices (σ_i) to take place of the identities. Hence, we don't compare with their OT_n^k scheme. Zhang et al.'s scheme [22] uses of modular exponentiation operations. Its communication cost is 1024k bits transmitted from the receiver to the sender, and 1024$*$(n+k) bits from the sender to the receiver. Mu et al.'s [23] protocol uses of signature scheme, it therefore needs 1024$*$2n bits transmitted from the receiver to the sender, and 1024n bits from the sender to the receiver. Naor et al. [24] proposed an OT_n^k scheme builds upon of their scheme [32], it needs OT_2^1 scheme by performing it wk log n times, where w is a times that mask with XOR a pseudo-random function, in order

for the probability of receiver no more than k values be smaller than δ, we need w to be such that $(\frac{k^4}{\sqrt{N}})^w < \delta$, i.e $w > \log\delta / \log(k^4/\sqrt{n})$, it therefore get that when $k \le N^{1/4}$ this process works. Chu et al. [6] point out that Naor et al.'s scheme needs the sender sending O(n + wk log n) messages to the receiver, and receiver sending O(wk log n) messages to the sender. For Naor et al.'s scheme uses of modular exponentiation operators, it therefore has 1024∗(wk log n) bits transmitted from the receiver to the sender, and 1024∗(n + wk log n) bits transmitted from the sender to the receiver. In 2008, Chang et al. [27] presented a OT_n^k based on blind signature and Chinese remainder theorem, but its communication time is longer that their scheme requires three rounds. Its communication cost is 1024k bits

Table 1: Comparisons of transmitted data for k-out-of-n oblivious transfer schemes.

	rounds	size of message: R→S (bits)	size of message: S→R (bits)
Ours	2	160∗(k+2) bits	160∗(n+k) bits
Chu et al. [6]	2	1024k bits	1024∗(n+k+1) bits
Green et al. [10]	3	k∗|Pok| bits	160(2k+n) +2∗|Pok| bits
Zhang et al. [22]	3	1024k bits	1024∗(n+k) bits
Mu et al. [23]	2	1024∗2n bits	1024n bits
Naor et al. [24]	wk log n	1024∗(wk log n) bits	1024∗(n + wk log n) bits
Chang et al. [27]	3	1024k bits	1024∗(n+k) bits

|Pok|: the size of a message transmitted in a proof of knowledge scheme.
w: times of mask with XOR a pseudo-random function.

transmitted from the receiver to the sender, and $1024*(n+k)$ bits transmitted from the sender to the receiver. After the comparisons made above as shown in Table 1, we can conclude that our bilinear pairing OT_n^k protocol not only can satisfy the security requirements of mutual authentication but also is more efficient in bandwidth consumption while compared with all the existing OT_n^k schemes. We compare of security analysis with related scheme as shown in Table 2.

Table 2: Comparisons of security analysis

	Against MIMA	Against KCI	Mutual authentication
Ours	yes	yes	yes
Chu et al. [6]	no	no	no
Green et al. [10]	yes	no	no
Zhang et al. [22]	no	no	no
Mu et al. [23]	no	no	no
Naor et al. [24]	no	no	no
Chang et al. [27]	no	no	no

Chapter 6 Conclusion

At first, in the method of key agreement, we have shown that the Zhou et al.'s scheme suffers from the impersonation attacks. An adversary can utilize the simple method to impersonate one party to the other. Secondly, in the oblivious transfer protocol, traditional OT protocols lack of the consideration of mutual authentication for the communicating parties. It is assumed that they communicate through a secure channel. If this assumption does not hold, traditional OT schemes will suffer from the impersonation attack. Hence, we propose a new OT_n^k protocol based on bilinear pairing to provide mutual authentication. After analysis, we can conclude that our scheme not only is the first scheme which has the mutual authentication and can resist various malicious attacks, but also efficient in bandwidth consumption. These properties are important to be applied in a scheme used in a busy financial network.

References

[1] Y. B. Zhou, Z. F. Zhang, and D. G. Feng, Cryptanalysis of the End-to-End Security Protocol for Mobile Communications with End-User Identification/Authentication, IEEE Communications Letters 9, 2005.

[2] W. Diffie and M. E. Hellman, "New directions in cryptography, IEEE Trans. Inform. Theory 22, pp. 644-654, 1976.

[3] C. C. Chang, K. L. Chen, and M. S. Hwang, End-to-end security protocol for mobile communications with end-user identification/authentication, Wireless Personal Communications 28, pp. 95-106, 2004.

[4] C. S. Park, On certificate-based security protocols for wireless mobile communication systems, IEEE Network 11, pp. 50-55, 1997.

[5] G. Brassard, C. Cre'peau, and J.-M. Robert, All-or-nothing disclosure of secrets. Advances in Cryptology – CRYPTO '86, LNCS 263, Springer-Verlag, pp. 234–238, 1986.

[6] C. K. Chu, W. G. Tzeng, Efficient k-out-of-n oblivious transfer Schemes with adaptive and non-adptive queries. PKC 2005, LNCS 3386, pp. 172-183, 2005.

[7] J. Camenish, G. Neven, and A. shelat. Simulatable adaptive oblivious transfer. EUROCRYPT 2007, LNCS 4515, pp. 573-590, 2007.

[8] M. L. Das, A. Saxena, V. P. Gulati and D. B. Phatak, A novel remote user authentication scheme using bilinear pairings, Computers & Security 25, pp. 184-189, 2006.

[9] S. Even, O. Goldreich, and A. Lempel, A randomized protocol for

signing contracts, Communications of the ACM 28, pp. 637–647, 1985.

[10] M. Green, S. Hohenberger, Blind identity-based encryption and simulatable oblivious transfer, Cryptology ePrint Archive 2007/235, 2007.

[11] H. Ghodosi, On insecurity of Naor–Pinkas' distributed oblivious transfer, Information Processing Letters (2007) 104, 2007.

[12] H. F. Huang, C. C. Chang, A New Design for Efficient t-out-n Oblivious Transfer Scheme, Advanced Information Networking and Applications 2, IEEE, pp. 28-30, 2005.

[13] O. Rabin, Exchange secrets by oblivious transfer, Computer Science Lab, Harvard University, Cambridge, MA, TR-81, 1981.

[14] S. Halevi, Y. T. Kalai, Smooth projective hashing and two-message oblivious transfer, Cryptology ePrint Archive 2007/118, 2007.

[15] S. Kim, S. Kim, and G. Lee, Secure verifiable non-interactive oblivious transfer protocol using RSA and Bit commitment on distributed environment, Future Generation Computer Systems, 2006.

[16] C. Y. Lin, T. C. Wu, and F. Zhang and J. J. Hwang, New identity-based society oriented signature schemes from pairings on elliptic curves, Applied Mathematics and Computation 160, pp 245-260, 2005.

[17] K. Peng, C. Boyd and E. Dawson, Batch verification of validity of bids in homomorphic e-auction, Computer Communications 29, pp. 2798-2805, 2006.

[18] A. Parakh, Oblivious Transfer Using Elliptic Curves, the 15th International Conference on Computing, IEEE , pp. 323-328 , 2006.

[19] Shamir, Identity based cryptosystems & signature schemes. Advances

in Cryptology, CRYPTO’84, LNCS, pp. 47–53, 1984.

[20] W. G. Tzeng, Efficient 1-out-n oblivious transfer schemes, the Public-Key Cryptography (PKC ’02), Springer-Verlag, pp. 159-171. 2002.

[21] J. Zhang, Y. Wang, Two provably secure k-out-of-n oblivious transfer schemes, Applied Mathematics and Computation 169, pp. 1211-1220, 2005.

[22] J. Zhang, W. Zou, Two t-out-of-n oblivious transfer schemes with designated reeiver, wuhan university journal of natural sciences 11, pp. 2006.

[23] Y. Mu, J. Zhang, and V. Varadharajan, m out of n oblivious transfer, the 7th Australasian Conference on Information Security and Privacy (ACISP ’02), 2384 , LNCS, pp. 395-405, Springer-Verlag, 2002.

[24] M. Naor, B. Pinkas, Oblivious transfer with adaptive queries, Advances in Cryptology–CRYPTO ’99, LNCS 1666, pp. 573–590. Springer-Verlag, 1999.

[25] M. Naor, B. Pinkas, Distributed oblivious transfer, Advances in Cryptology–Proceedings of ASIACRYPT’00, LNCS 1976, Springer-Verlag, 2000.

[26] D. Boneh, M. K. Franklin, Identity-based encryption from the Weil Pairing, In CRYPTO'01, pp. 213-229, 2001.

[27] C. C. Chang, J. S. Lee, Robust t-out-of-n oblivious transfer mechanism based on CRT, Journal of Network and Computer Applications, 2008.

[28] A. Menezes, T. Okamoto, and S. Vanston, Reducing elliptic curve logarithms to logarithms in a finite field, IEEE Transaction on Information Theory 39, pp. 1639-1646, 1993.

[29] L.M. Kohnfelder, On the signature reblocking problem in public-key cryptography, Communications of the ACM 21 (2) 179, 1978.

[30] D. Boneh, X. Boyen, Efficient selective-ID secure Identity-Based Encryption without random oracles. In EUROCRYPT '04, LNCS 3027, pp. 223-238, 2004.

[31] C. Crepeau, Equivalence between two floavors of oblivious transfer, EUROCRYPTO 87, pp.350-354, 1987.

[32] M. Naor, B. Pinkas, Oblivious transfer and polynomial evaluation, Proc. 31th ACM Symp. on Theory of Computing, pp. 245-254, 1999.