

# Security Analysis of a Single Sign-On Mechanism for Distributed Computer Networks

Guilin Wang, Jiangshan Yu, and Qi Xie

**Abstract**—Single sign-on (SSO) is a new authentication mechanism that enables a legal user with a single credential to be authenticated by multiple service providers in a distributed computer network. Recently, Chang and Lee proposed a new SSO scheme and claimed its security by providing well-organized security arguments. In this paper, however, we demonstrative that their scheme is actually insecure as it fails to meet credential privacy and soundness of authentication. Specifically, we present two impersonation attacks. The first attack allows a malicious service provider, who has successfully communicated with a legal user twice, to recover the user's credential and then to impersonate the user to access resources and services offered by other service providers. In another attack, an outsider without any credential may be able to enjoy network services freely by impersonating any legal user or a nonexistent user. We identify the flaws in their security arguments to explain why attacks are possible against their SSO scheme. Our attacks also apply to another SSO scheme proposed by Hsu and Chuang, which inspired the design of the Chang–Lee scheme. Moreover, by employing an efficient verifiable encryption of RSA signatures proposed by Ateniese, we propose an improvement for repairing the Chang–Lee scheme. We promote the formal study of the soundness of authentication as one open problem.

**Index Terms**—Authentication, distributed computer networks, information security, security analysis, single sign-on (SSO).

## I. INTRODUCTION

WITH the widespread use of distributed computer networks, it has become common to allow users to access various network services offered by distributed service providers [1], [2]. Consequently, user authentication (also called user identification) [3], [4] plays a crucial role in distributed computer networks to verify if a user is legal and can therefore be granted access to the services requested. To avoid bogus servers, users usually need to authenticate service providers. After mutual authentication, a session key may be

negotiated to keep the confidentiality of the data exchanged between a user and a service provider [4], [5]. In many scenarios, the anonymity of legal users must be protected as well [4], [6]. However, practice has shown that it is a big challenge to design efficient and secure authentication protocols with these security properties in complex computer network environments [7], [8].

In 2000, Lee and Chang [4] proposed a user identification and key distribution scheme to maintain user anonymity in distributed computer networks. Later, Wu and Hsu [9] pointed out that the Lee–Chang scheme is insecure against both impersonation attacks and identity disclosure attacks. Meanwhile, Yang *et al.* [10] identified a weakness in the Wu–Hsu scheme and proposed an improvement. In 2006, however, Mangipudi and Katti [11] pointed out that Yang *et al.*'s scheme suffers from Deniable of Service (DoS) attacks and presented a new scheme. In 2009, Hsu and Chuang [12] showed that the schemes of both Yang *et al.* and Mangipudi–Katti were insecure under identity disclosure attack and proposed an RSA-based user identification scheme to overcome this weakness. Recently, authentication and privacy have been attracted a lot of attentions in RFID systems [13], [14], industrial networks [8], as well as general computer networks [15].

On the other side, it is usually not practical by asking one user to maintain distinct pairs of identity and password for different service providers, since this could increase the workload of both users and service providers as well as the communication overhead of networks. To tackle this problem, the single sign-on (SSO) mechanism [16] has been introduced so that, after obtaining a credential from a trusted authority for a short period (say one day), each legal user's authentication agent can use this single credential to complete authentication on behalf of the user and then access multiple service providers. Intuitively, an SSO scheme should meet at least three basic security requirements, i.e., *unforgeability*, *credential privacy*, and *soundness*. Unforgeability demands that, except the trusted authority, even a collusion of users and service providers are not able to forge a valid credential for a new user. Credential privacy guarantees that colluded dishonest service providers should not be able to fully recover a user's credential and then impersonate the user to log in to other service providers. Soundness means that an unregistered user without a credential should not be able to access the services offered by service providers. Formal security definitions of unforgeability and credential privacy were given in [17].

A similar concept, called the generalized digital certificate (GDC), was proposed in [18] to provide user authentication and key agreement in wireless networks, in which a user, who holds a digital signature of his/her GDC issued by an authority, can

Manuscript received February 01, 2012; revised May 15, 2012; accepted July 24, 2012. Date of publication August 28, 2012; date of current version December 19, 2012. The work of G. Wang was supported in part by the National Natural Science Foundation of China under Grant 61070153. The work of Q. Xie was supported in part by the National Natural Science Foundation of China under Grant 61070153 and the Natural Science Foundation of Zhejiang Province under Grant LZ12F02005. Paper no. TII-12-0047.

G. Wang and J. Yu are with the Center for Computer and Information Security Research, School of Computer Science and Software Engineering, University of Wollongong, Wollongong, NSW 2522, Australia (e-mail: guilin@uow.edu.au; jy898@uowmail.edu.au).

Q. Xie is with the School of Information Science and Engineering, Hangzhou Normal University, Hangzhou 310036, China (e-mail: qxie68@yahoo.com.cn).

Digital Object Identifier 10.1109/TII.2012.2215877

authenticate him/herself to a verifier by proving the knowledge of the signature without revealing it.

Chang and Lee [19] made a careful study of SSO mechanism. First, they argued that the Hsu–Chuang user identification scheme, actually an SSO scheme, has two weaknesses: 1) an outsider can forge a valid credential by mounting a credential forging attack since the Hsu–Chang scheme employed naive RSA signature without using any hash function to issue a credential for any random identity selected by a user (in fact, this feature inherits from [10]) and 2) the Hsu–Chuang scheme requires clock synchronization since it uses a time stamp. Then, Chang and Lee presented an interesting RSA-based SSO scheme, which does not rely on clock synchronization by using a nonce instead of a time stamp. Their scheme is suitable for mobile devices due to its high efficiency in computation and communication. Finally, they presented a well-organized security analysis to show that their SSO scheme supports secure mutual authentication, session key agreement, and user anonymity. In [17], Han *et al.* proposed a generic SSO construction which relies on broadcast encryption plus zero knowledge (ZK) proof [20] showing that the prover knows the corresponding private key of a given public key. So, implicitly, each user is assumed to have been issued a public key in a public key infrastructure (PKI). In the setting of RSA cryptosystem, such a ZK proof is very inefficient due to the complexity of interactive communications between the prover (a user) and the verifier (a service provider). Therefore, compared with Han *et al.*'s generic scheme, the Chang–Lee scheme has several attracting features: less underlying primitives without using broadcast encryption, high efficiency without resort to ZK proof, and no requirement of PKI for users. Unfortunately, as we shall discuss later this efficient SSO scheme is not secure.

In this paper, we show that the Chang–Lee scheme [19] is actually insecure by presenting two impersonation attacks, i.e., *credential recovering attack* and *impersonation attack without credentials*. In the first attack, a malicious service provider who has communicated with a legal user twice can successfully recover the user's credential. Then, the malicious service provider can impersonate the user to access resources and services provided by other service providers. The other attack may enable an outside attacker without any valid credential to impersonate a legal user or even a nonexistent user to have free access to the services. These two attacks imply that the Chang–Lee SSO scheme fails to meet credential privacy and soundness, which are essential requirements for SSO schemes and authentication protocols. We also identify the flaws in their security arguments in order to explain why it is possible to mount our attacks against their scheme. Similar attacks can also be applied to the Hsu–Chuang scheme [12], on which the Chang–Lee scheme is based. Finally, to avoid these two impersonation attacks, we propose an improved SSO scheme to enhance the user authentication phase of the Chang–Lee scheme. To this end, we employ the efficient RSA-based verifiable encryption of signatures (VES) proposed by Ateniese [21] to verifiably and securely encrypt a user's credential. In fact, Ateniese's VES was originally introduced to realize fair exchange. There are no similar attacks in the setting of SSO,

TABLE I  
NOTATIONS

SCPC	Smart Card Producing Center
$U_i, P_j$	User and Service provider, respectively
$ID_i, ID_j$	The unique identity of $U_i$ and $P_j$ , respectively
$e_X, d_X$	The public/private RSA key pair of identity $X$
$S_i$	The credential of $U_i$ created by SCPC
$S_x$	The long term private key of SCPC
$S_y$	The public key of SCPC
$E_K(M)$	A symmetric key encryption of plaintext $M$ using a key $K$
$D_K(C)$	A symmetric key decryption of ciphertext $C$ using a key $K$
$\sigma_j(SK_j, M)$	The signature $\sigma_j$ on $M$ signed by $P_j$ with signing key $SK_j$
$Ver(PK_j, M, \sigma_j)$	Verifying signature $\sigma_j$ on $M$ with public key $PK_j$
$h(\cdot)$	A given one way hash function
$\parallel$	The operation of concatenation

and this is also the first time of using VES to design an SSO scheme, to the best of our knowledge.

The remainder of this paper is organized as follows. Section II reviews Chang–Lee scheme [19]. After that, we present two attacks against the Chang–Lee scheme in Section III and briefly analyze Hsu–Chuang scheme [12] in Section IV. Then, the improved SSO scheme using VES is given in Section V. Finally, the conclusion is given in Section VI.

## II. REVIEW OF THE CHANG–LEE SCHEME

Chang and Lee's single sign-on scheme [19] is a remote user authentication scheme, supporting session key establishment and user anonymity. In their scheme, RSA cryptosystems are used to initialize a trusted authority, called an SCPC (smart card producing center), and service providers, denoted as  $P_j$ 's. The Diffie–Hellman key exchange technique is employed to establish session keys. In the Chang–Lee scheme, each user  $U_i$  applies a credential from the trusted authority SCPC, who signs an RSA signature for the user's hashed identity. After that,  $U_i$  uses a kind of knowledge proof to show that he/she is in possession of the valid credential without revealing his/her identity to eavesdroppers. Actually, this is the core idea of user authentication in their scheme and also the reason why their scheme fails to achieve secure authentication as we shall show shortly. On the other side, each  $P_j$  maintains its own RSA key pair for doing server authentication. The Chang–Lee's SSO scheme consists of three phases: system initialization, registration, and user identification. Table I explains notations, and the details of Chang–Lee scheme are reviewed as follows.

### A. System Initialization Phase

The trusted authority SCPC first selects two large safe primes  $p$  and  $q$  and then sets  $N = pq$ . After that, SCPC determines its RSA key pair  $(e, d)$  such that  $ed = 1 \bmod \phi(N)$ , where  $\phi(N) = (p-1)(q-1)$ . SCPC chooses a generator  $g \in \mathbb{Z}_N^*$ , where  $n$  is also a large prime number. Finally, SCPC publishes  $(e, g, n, N)$ , keeps  $d$  as a secret, and erases  $(p, q)$  immediately once this phase has been completed.

### B. Registration Phase

In this phase, each user  $U_i$  chooses a unique identity  $ID_i$  with a fixed bit-length and sends it to SCPC. After that, SCPC will return  $U_i$  the credential  $S_i = (ID_i \| h(ID_i))^d \bmod N$ , where  $\|$  denotes a concatenation of two binary strings and  $h(\cdot)$  is a collision-resistant cryptographic one-way hash function. Here, both  $ID_i$  and  $S_i$  must be transferred via a secure channel.

At the same time, each service provider  $P_j$  with identity  $ID_j$  should maintain its own RSA public parameters  $(e_j, N_j)$  and private key  $d_j$  as does by SCPC.

### C. User Identification Phase

To access the resources of service provider  $P_j$ , user  $U_i$  needs to go through the authentication protocol specified in Fig. 1. Here,  $k$  and  $t$  are random integers chosen by  $P_j$  and  $U_i$ , respectively;  $n_1, n_2$  and  $n_3$  are three random nonces; and  $E(\cdot)$  denotes a symmetric key encryption scheme which is used to protect the confidentiality of user  $U_i$ 's identity  $ID_i$ . We highlight this phase as follows.

- Upon receiving a service request message  $m_1$  from user  $U_i$ , service provider  $P_j$  generates and returns user message  $m_2$  which is made up primarily by its RSA signature on  $(Z, ID_j, n_1)$ . Once this signature is validated, it means that user  $U_i$  has authenticated service provider  $P_j$  successfully. Here,  $Z = g^k \bmod n$  is the temporal Diffie–Hellman (DH) key exchange material issued by  $P_j$ .
- After that, user  $U_i$  correspondingly generates his/her temporal DH key exchange material  $w = g^t \bmod n$  and issues proof  $x = S_i^{h(K_{ij} \| w \| n_2)} \bmod N$ , where  $K_{ij} = h(ID_i \| k_{ij})$  is the derived session key and  $k_{ij} = Z^t \bmod n = w^k \bmod n = g^{kt} \bmod n$  is the raw key obtained by using the DH key exchange technique.
- Proof  $x = S_i^{h(K_{ij} \| w \| n_2)} \bmod N$  is used to convince  $P_j$  that  $U_i$  does hold valid credential  $S_i$  without revealing the value of  $S_i$ . Namely, after receiving message  $m_3$  service provider  $P_j$  can confirm  $x$ 's validity by checking if  $SID_i^{h(K_{ij} \| w \| n_2)} \bmod N = x^e \bmod N$ , where  $SID_i = (ID_i \| h(ID_i))$ . If this quality holds, it means that user  $U_i$  has been authenticated successfully by service provider  $P_j$ . It worth noting that proof  $x$  is designed in a particular way so that except  $P_j$  and  $U_i$ , no one else can verify it as both  $U_i$ 's identity  $ID_i$  and the newly established session key  $K_{ij}$  are used to produce  $x$ . This aims to achieve user anonymity as no eavesdropper can learn the values of  $ID_i$  and  $K_{ij}$ .
- Finally, message  $m_4$  (i.e.  $h(n_3)$ ) is employed to show that  $P_j$  has obtained message  $m_3$  correctly, which implies the success of mutual authentication and session key establishment.

### III. ATTACKS AGAINST THE CHANG–LEE SCHEME

As can be seen from the previous section, it seems that the Chang–Lee SSO scheme achieves secure mutual authentication, since server authentication is done by using traditional RSA signature issued by service provider  $P_j$ . Without valid credential  $S_i$  it looks impossible for an attacker to impersonate a legal user  $U_i$  by going through the user authentication procedure.

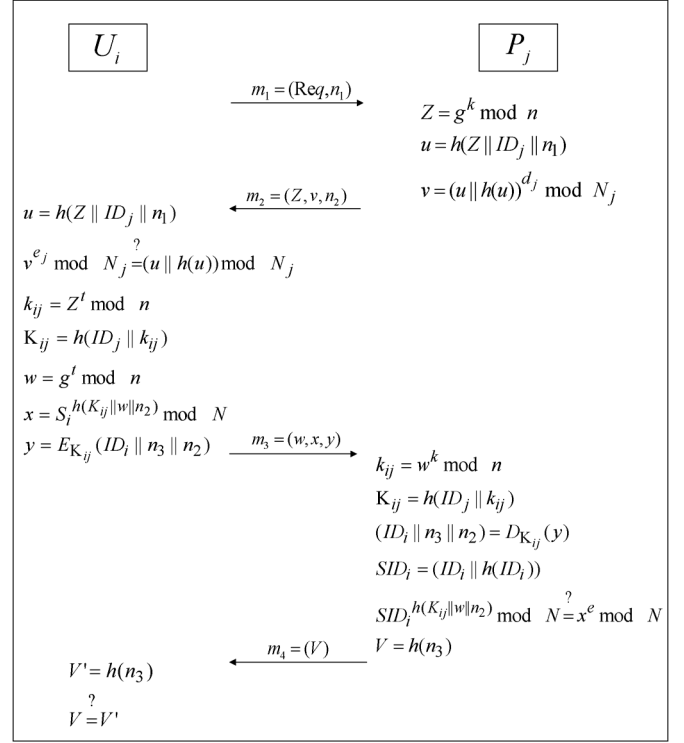


Fig. 1. User identification phase of the Chang–Lee scheme.

It can be seen from the following, however, that the Chang–Lee scheme is actually not a secure SSO scheme because there are two potential effective and concrete impersonation attacks. The first attack, the “credential recovering attack” compromises the credential privacy in the Chang–Lee scheme as a malicious service provider is able to recover the credential of a legal user. The other attack, an “impersonation attack without credentials,” demonstrates how an outside attacker may be able to freely make use of resources and services offered by service providers, since the attacker can successfully impersonate a legal user without holding a valid credential and thus violate the requirement of soundness for an SSO scheme. In real life, these attacks may put both users and service providers at high risk.

We now first describe our attacks together with the assumptions required, justify why these assumptions are reasonable, and finally discuss why the security analysis and proofs given in [19] are not enough to guarantee the security of the Chang–Lee SSO scheme.

#### A. Credential Recovering Attack

Intuitively, the Chang–Lee SSO scheme seems to satisfy the requirement of credential privacy since receiving credential proof  $x = S_i^{h_2} \bmod N$ , where  $h_2$  denotes  $h(K_{ij} \| w \| n_2)$ , does not allow service provider  $P_j$  to recover user  $U_i$ 's credential  $S_i$  by computing  $S_i = x^{h_2^{-1}} \bmod N$ , where  $h_2^{-1}$  refers to  $h_2^{-1} \bmod \phi(N)$ . In fact, the difficulty of calculating  $h_2^{-1}$  from the given  $(e, N, x, h_2)$  is the exact rationale why the RSA cryptosystem is secure, i.e, it should be intractable for an attacker to derive the RSA private key from the public key (and a given

ciphertext). This is because here we could treat  $(h_2, h_2^{-1})$  as another RSA public/private key pair w.r.t the same RSA modulus  $N$ . Moreover, directly recovering  $S_i$  from  $x = S_i^{h_2} \bmod N$  also looks impossible as this seems equivalent to decrypt the RSA ciphertext  $x$  w.r.t. the (ephemeral) public key  $h_2$ .

Nevertheless, there is a pitfall in the production of proof  $x = S_i^{h_2} \bmod N$  as here the same credential  $S_i$  is encrypted multiple times under different (ephemeral) public keys  $h_2$  w.r.t. the same RSA modulus  $N$ . Consequently, under the assumption that malicious service provider  $P_j$  has run the Chang–Lee SSO scheme with the same user  $U_i$  twice,  $P_j$  will be able to recover  $U_i$ 's credential  $S_i$  with high probability by using the extended Euclidean algorithm. Namely,  $P_j$  can solve  $S_i$  from two equations  $x = S_i^{h_2} \bmod N$  and  $x' = S_i^{h'_2} \bmod N$ . The details of the attack, which share some features of common-modulus attacks against RSA [22, p. 46], are given as follows.

- 1) After successfully running the Chang–Lee SSO scheme twice with the same user  $U_i$ , malicious service provider  $P_j$  stores all messages exchanged in these two instances, denoted as  $(ID_i, x, K_{ij}, w, n_2, \dots)$  for the first instance, and  $(ID_i, x', K'_{ij}, w', n'_2, \dots)$  for the second instance.
- 2) By denoting  $h_2 = h(K_{ij} \| w \| n_2)$  and  $h'_2 = h(K'_{ij} \| w' \| n'_2)$ ,  $P_j$  first checks if  $h_2$  and  $h'_2$  are co-prime, i.e. if  $\gcd(h_2, h'_2) = 1$ . In the case that  $\gcd(h_2, h'_2) = 1$ ,  $P_j$  then runs the extended Euclidean algorithm [22, pp. 290–292] to compute two integers  $a$  and  $b$  such that  $a \cdot h_2 + b \cdot h'_2 = 1$  (in  $\mathbb{Z}$ ). Finally, malicious  $P_j$  can recover  $U_i$ 's credential  $S_i$  by computing

$$S_i = x^a \cdot x'^b \bmod N. \quad (1)$$

Equation (1) is justified by the following equalities:

$$\begin{aligned} x^a \cdot x'^b \bmod N &= \left(S_i^{h_2}\right)^a \cdot \left(S_i^{h'_2}\right)^b \bmod N \\ &= S_i^{a \cdot h_2 + b \cdot h'_2} \bmod N \\ &= S_i^1 \bmod N \\ &= S_i. \end{aligned}$$

- 3) If  $\gcd(h_2, h'_2) \neq 1$ , then  $P_j$  needs to run more instances with  $U_i$  so that it can get two instances such that  $\gcd(h_2, h'_2) = 1$ .

There are a number of comments to be made regarding the above attacks. First, it has a success rate of about 60% due for two reasons: 1) for two randomly selected integers  $u$  and  $v$ , the probability that  $\gcd(u, v) = 1$  holds is  $6/\pi^2 \approx 0.6$  [23], [24] and 2) as the outputs of hash function  $h$ ,  $h_2$  and  $h'_2$  can be regarded as random numbers. This means that after executing the Chang–Lee SSO scheme with the same user  $U_i$  twice, malicious  $P_j$  will be able to recover  $U_i$ 's credential  $S_i$  with a probability of about 0.6. Consequently, it is easy to see that after running the scheme with  $U_i$  a couple of times,  $P_j$  can recover  $S_i$  almost certainly. Second, it is not hard to see that the above attack could be mounted by two or multiple malicious service providers who collude together once they put the values of  $h_2$  together. Finally, the attack will lead to serious consequences since after recovering the valid credential of a legal user, malicious  $P_j$  can impersonate this user by running the Chang–Lee SSO scheme in

the same way as a legal user does to freely make use of the services offered by other service providers.

How could service provider  $P_j$  be malicious and then mount the above attack? On the one hand, the Chang–Lee SSO scheme specifies that *SCPC* is the trusted party (refer to Section IV-A [19]). So, this implies that service providers are not trusted parties and that they could be malicious. By agreeing with Yang *et al.* [10], when they said that “the Wu–Hsu’s modified version could not protect the user’s token against a malicious service provider...”, the work in [19] also implicitly agrees that there is the potential for attacks from malicious service providers against SSO schemes. Moreover, if all service providers are assumed to be trusted, to identify him/herself user  $U_i$  can simply encrypt his/her credential  $S_i$  under the RSA public key of service provider  $P_i$ . Then,  $P_i$  can easily decrypt this ciphertext to get  $U_i$ 's credential and verify its validity by checking if it is a correct signature issued by *SCPC*. In fact, such a straightforward scheme with strong assumption is much simpler, more efficient and has better security, at least against this type of attack.

On the other hand, according to the security models given in [10] and [17], malicious service providers could be attackers in SSO schemes. In fact, this is a traditional as well as prudential way to deal with trustworthiness, since we cannot simply assume that beside the trusted authority *SCPC*, all service providers are also trusted. The basic reason is that assuming the existence of a trusted party is the strongest supposition in cryptography but it is usually very costly to develop and maintain. In particular, Han *et al.* [17] defined collusion impersonation attacks as a way to capture the scenarios in which malicious service providers may recover a user’s credential and then impersonate the user to login to other service providers. It is easy to see that the above credential recovery attack is simply a special case of collusion impersonation attack where a single malicious service provider can recover a user’s credential.

### B. Impersonation Attack Without Credentials

We now study the soundness of the Chang–Lee SSO scheme, which seems to satisfy this security requirements as well. The main reason is that to get valid proof  $x$  satisfying  $SID_i^{h_2} \bmod N = x^e \bmod N$  for a random hash output  $h_2$ , there seems no other way but to compute  $x$  by  $x = SID_i^{h_2 \cdot e^{-1}} \bmod N$ , i.e.,  $x = (SID_i^d)^{h_2}$  or  $x = (S_i)^{h_2} \bmod N$ . Therefore, an attacker should not be able to log in to any service provider if it does not have the knowledge of either *SCPC*'s RSA private key  $d$  or user  $U_i$ 's credential  $S_i$ .

Again, however, such a plausible discussion simply explains the rationale of the Chang–Lee SSO scheme but cannot guarantee its security w.r.t. the soundness. This is also the essential reason why the current focus of research in information security is on formal proofs which rigorously show the security of cryptosystems. Indeed, no one can formally prove that without knowing either *SCPC*'s RSA private key  $d$  or user  $U_i$ 's credential  $S_i$ , it is unfeasible to compute a proof  $x$  that passes through authentication, as an outside attacker is able to get a shortcut if the *SCPC*'s RSA public key  $e$  is a small integer so that  $e$ 's binary length is less than the output length of hash function  $h$ , i.e.,  $|e| < |h(\cdot)|$ . The attack is explained in detail as follows.

- 1) To impersonate legal user  $U_i$  with identity  $ID_i$  for accessing service provider  $P_j$ , an attacker  $E$  first sends  $P_j$  request message  $m_1$  normally, as  $U_i$  does.
- 2) Upon receiving message  $m_2$  from  $P_j$ ,  $E$  then checks  $P_j$ 's signature and chooses a random integer  $t$  to compute  $(k_{ij}, K_{ij}, w)$ . Before moving on to the next step, attacker  $E$  needs to check whether  $h(K_{ij}||w||n_2)$  is divisible by  $e$ . If not,  $E$  has to choose another  $t$  or start a new session to satisfy this condition.
- 3) As  $h(K_{ij}||w||n_2)$  is divisible by  $e$ , let  $h(K_{ij}||w||n_2) = e \cdot b$  for some integer  $b \in \mathbb{Z}$ . Now,  $E$  sets  $x = SID_i^b \bmod N$ , where  $SID_i = ID_i || h(ID_i)$ .
- 4) Finally,  $E$  can impersonate user  $U_i$  to pass the authentication by sending  $m_3 = (w, x, y)$  to  $P_j$ , since  $P_j$  will notice that  $SID_i^{h(K_{ij}||w||n_2)} \bmod N = x^e \bmod N$ . This is because we have:  $SID_i^{h(K_{ij}||w||n_2)} \bmod N = SID_i^{b \cdot e} \bmod N = x^e \bmod N$ .

There are a number of things worth noting in regard to the above impersonation attack without credentials. First, the attack will succeed at a rate of about  $1/e$  for one random number  $t$  in a new session. The reason is that  $e | h(K_{ij}||w||n_2)$  holds with a probability of about  $1/e$ , since  $|e| < |h(\cdot)|$  and the output of hash function  $h$  can be treated as random numbers. Consequently, if  $e = 3$  the above attack can succeed once by trying about three values of  $t$  on average. Even if  $e$  is as large as  $65537 (= 2^{16} + 1)$ , trying 65537 times to get a successful impersonation may not be difficult for attacker  $E$  as it may explore a machine, which can be much more powerful than a mobile device, to do the computations needed for each try, i.e., two modular exponentiations and two hash evaluations. Moreover, even when timeout is introduced into the Chang–Lee scheme it may be not a real obstacle for attacker  $E$  as it can initialize new sessions (w.r.t. the same or different identities).

Second, in the above attack we assume that  $e$  is a small integer and attacker  $E$  may know the value of one legal user's identity  $ID_i$ . This is reasonable as explained below. On the one hand, in the system initialization phase (Section IV-A) the Chang–Lee scheme only specifies that the trusted party  $SCPC$  needs to set its RSA key pair  $(e, d)$  but does not give any limitation on the length of public exponent  $e$ . So,  $e$  could be a small integer with binary length less than the output length of hash function  $h$ , i.e.,  $|e| < |h(\cdot)|$ . Moreover, in practice this is likely to happen because: 1) to speed up the RSA signature verification, some security standards (e.g., PKCS #1 [25]), academic papers (e.g. [26]) and popular web sites (e.g., Wikipedia [27]) suggest that  $e$  can be set as 3 or 65537; and 2) as the Chang–Lee scheme is claimed to be efficient even for mobile devices in distributed networks, using small exponent  $e$  can provide further computational advantage for these devices as they usually have limited resources for computation and storage [28]. In addition, the security analysis given in [19] neither excludes the case of small  $e$  nor relies on the concrete procedure of setting  $SCPC$ 's RSA key pair  $(e, d)$ .

On the other hand, in the Chang–Lee SSO scheme users' identities are not as crucial as their credentials, though the identities are transferred in ciphertext to provide user anonymity. So, users' identities could be known by an attacker due to rea-

sons, such as users' negligence. At least service providers know users' identities. Moreover, even if users' identities are well protected so that attacker  $E$  cannot impersonate registered user  $U_i$  as above,  $E$  can freely forge an identity  $ID$ . This is possible because in the Chang–Lee scheme, each user selects his/her identity by following only one requirement: each identity is a string with fixed bit-length. Therefore, even an outside attacker  $E$  can use an arbitrary such string as an identity to mount the above attack, since the service providers are not provided any additional mechanism to check whether identity  $ID$  has been registered with  $SCPC$ . This also implies that if  $e$  is a small integer,  $E$  can even impersonate a nonexistent user to make use of the resources and services offered by service providers.

Finally, it must be emphasized that impersonation attacks without valid credentials seriously violate the security of SSO schemes as it allows attackers to be successfully authenticated without first obtaining a valid credential from the trusted authority after registration. In other words, it means that in an SSO scheme suffering these attacks there are alternatives which enable passing through authentication without credentials.

### C. Discussion

In [19], Chang and Lee provided a well-organized security analysis to show that their SSO scheme is secure. However, the two impersonation attacks presented in the previous section mean that their SSO scheme is actually not secure. So, why is their analysis not enough to guarantee the security of their scheme? What is the security flaw in their scheme leading to the above attacks? And what could we learn from these attacks to prevent similar situations in the future design of SSO schemes? These are the topics of this section.

In [19], the security of the Chang–Lee SSO scheme has been analyzed in three different ways: 1) BAN logic [29] was used to show the correctness of the Chang–Lee schemes; 2) informal security arguments were given to demonstrate that their scheme can resist some attacks, including impersonation attacks; and 3) a formal security proof was given to prove that their scheme is a secure authenticated key exchange (AKE) protocol [30]. However, these security analyses and proofs still do not guarantee the full security of the Chang–Lee scheme and there are a number of reasons for this. First, as early as the 1990s, it was known that although BAN logic had been shown useful to identify some attacks, it could approve protocols which are actually unsound in practice because of some technical weaknesses in the logic [31]. Moreover, in [19] the authors did not give details to show how the BAN logic can be used to prove that their scheme guarantees mutual authentication. In fact, at the end of Section V-A of [19], the authors claimed to be able to: “prove that  $U_i$  and  $P_j$  are able to authenticate each other using our protocol.” but they provided no argument to show why each party could not be impersonated by an attacker. Second, the authors did discuss informally why their scheme could withstand impersonation attacks by considering two scenarios, for example, an attacker re-uses previous nonce  $n_2$  to forge message  $m_3$  or selects random credential  $S_i$  to compute  $SID_i$  by  $SID_i = S_i^e \bmod N$ . However, such informal arguments neither strongly confirm their scheme's security against these two concrete attacks nor exclude the exis-

tence of other scenarios of impersonation attacks, such as those presented in previous sections. Finally, their formal proof about AKE only focuses on the session key security, i.e., an attacker with all reasonable resources is not able to know the session key established between the two parties under the computational DH (CDH) assumption (refer to [19, Theorem 1], and not the security of mutual authentication. According to the definitions given by Bellare and Rogaway [30], one fundamental requirement of a secure AKE protocol is that there be a secure mutual authentication in the first place.

From the above, we can see that it is the use of credential proof  $x = S_i^{h_2} \bmod N$  which leads to the above two attacks against the Chang–Lee SSO scheme. More specifically,  $x = S_i^{h_2} \bmod N$  is a kind of knowledge proof which shows that a prover (usually played by user  $U_i$ ) knows credential  $S_i$ . However, this is not a secure proof as a malicious verifier (i.e., service provider  $P_j$ ) can recover  $S_i$  and an outside attacker may be able to get authenticated without a credential. Based on this observation, a natural improvement on the Chang–Lee scheme would be to replace non-interactive proof  $x$  by a rigorous but interactive ZK proof [20] that shows the prover’s knowledge of secret  $S_i = SID_i^d \bmod N$  without revealing any additional information about credential  $S_i$ . In other words, using the verifiably encrypted signature introduced in [33], user  $U_i$  can encrypt his/her credential  $S_i$  under the public key of a trusted party and verifiably convince service provider  $P_j$  that the ciphertext does contain  $S_i$  w.r.t.  $U_i$ ’s identity  $ID_i$  without allowing  $P_j$  to get any additional information about credential  $S_i$ . Compared with two modular exponentiations used for generating and verifying proof  $x$ , however, ZK proofs for showing the possession of an RSA signature usually require hundreds of modulo exponentiations [32], [33] since these proofs rely on inefficient “cut and choose” method, i.e., binary challenges.

From the two attacks presented above, we can learn that both credential privacy and soundness are crucial for SSO schemes. As mentioned in Section III-A, credential privacy has been studied in Yang *et al.* [10] and Han *et al.* [17]. To the best of our knowledge, however, there is surprisingly, no existing research which has given a careful treatment of soundness. For example, Han *et al.* [17] did not investigate soundness, though they did carefully study how to formally define credential forgery and recovery attacks from outsiders, users, service providers and their potential collusion. According to the most traditional form of authentication, a user will be authenticated if he/she can provide a valid pair of user name and password (i.e. credential), and soundness is obviously satisfied because a user is not able to go through authentication without providing a valid credential which is registered and maintained by a server. In complex scenarios, like the Chang–Lee scheme, the situation may be less obvious and, in fact, quite challenging. For this reason, the problem remains an open one for future study. The question of formally defining the soundness of SSO/authentication schemes and rigorously proving them for concrete solutions remains an interesting and important one.

Finally, it must be noted that the analysis above shows only that the Chang–Lee SSO scheme fails to achieve secure authentication, without violating its security for achieving user anonymity and session key privacy.

#### IV. ATTACKS ON THE HSU–CHUANG SCHEME

Here, we briefly highlight the difference between the Chang–Lee scheme [19] and the Hsu–Chuang scheme [12] to see why the above describe impersonation attacks apply to this latter as well. The two schemes have similar structures and use similar notations, but the technical details differ. In summary, the Hsu–Chuang scheme is differs from the Chang–Lee scheme in three ways. First, in the Hsu–Chuang scheme user  $U_i$ ’s credential  $S_i$  is a naive RSA signature signed by the trusted party *SCPC*, i.e.,  $S_i = ID_i^d \bmod N$ , where  $ID_i$  is  $U_i$ ’s identity selected by him/herself. Second, to authenticate itself, service provider  $P_j$  sends signature  $u = g_j^{h(Z\|T_1\|ID_j) \cdot d_j} \bmod N_j$ , where  $Z$  is the DH key material generated by  $P_j$ ,  $T_1$  is the current timestamp, and  $ID_j$  is  $P_j$ ’s identity. Finally, for user authentication user  $U_i$  issues and sends proof  $x = S_i^{h(K_{ij}\|Z\|w\|T_2)} \bmod N$  to  $P_j$ , who validates  $x$  by checking if  $ID_i^{h(K_{ij}\|Z\|w\|T_2)} = x^e \bmod N$ . For more detail, see [12] or Section II of [19].

As pointed out in [19], the Hsu–Chuang scheme is vulnerable to impersonation attack as an attacker can forge a valid credential  $S_i$  w.r.t. identity  $ID_i$  by simply selecting random  $S_i \in \mathbb{Z}_N^*$  and then computing  $ID_i = S_i^e \bmod N$ . This attack can be excluded if a specific encoding format is required for identities and the credential is issued by using a secure hash  $h$ , i.e.,  $S_i = h(ID_i)^d \bmod N$ , as in the Chang–Lee scheme. According to the discussion in Section III, the Hsu–Chuang scheme is still not secure even with such a countermeasure. The reason is that our two attacks against the Chang–Lee scheme apply to the Hsu–Chuang scheme as well. This means that the Hsu–Chuang scheme also fails to satisfy both credential privacy and soundness of authentication. In addition, there is another flaw in the Hsu–Chuang scheme. Attacker  $E$  can impersonate service provider  $P_j$  to cheat legal users, as service authentication is conducted by using a non-traditional RSA signature,  $u = g_j^{h(Z\|T_1\|ID_j) \cdot d_j} \bmod N_j$ . By communicating with  $P_j$  twice attacker  $E$  can get messages  $(Z, T_1, ID_j, u)$  and  $(Z', T'_1, ID_j, u')$  satisfying  $u = g_j^{h(Z\|T_1\|ID_j) \cdot d_j} \bmod N_j$  and  $u' = g_j^{h(Z'\|T'_1\|ID_j) \cdot d_j} \bmod N_j$ . Once  $\gcd(h(Z\|T_1\|ID_j), h(Z'\|T'_1\|ID_j)) = 1$  (this holds with probability about 0.6, as we discussed in Section III-A),  $E$  can run the extended Euclidean algorithm [22, pp. 290–292] to find two integers  $a$  and  $b$  such that  $a \cdot h(Z\|T_1\|ID_j) + b \cdot h(Z'\|T'_1\|ID_j) = 1$  in  $\mathbb{Z}$  (without knowing the factors of  $S_j$ ’s RSA modulus). Hence,  $E$  can recover  $g_j^{d_j} \bmod N_j$  by computing  $g_j^{d_j} \bmod N_j = u^a u'^b \bmod N_j$ . After that,  $E$  can impersonate  $P_j$  to any legal user by using the value of  $g_j^{d_j} \bmod N_j$  to issue signature  $u = (g_j^{d_j} \bmod N_j)^{h(Z\|T_1\|ID_j)}$ , without knowing  $P_j$ ’s RSA private key  $d_j$ .

#### V. PROPOSED IMPROVEMENT

To overcome the flaws in the Chang–Lee scheme [19], we now propose an improvement by employing an RSA-based verifiable encryption of signatures (RSA-VES), which is an efficient primitive introduced in [21] for realising fair exchange of RSA signatures. VES comprises three parties: a trusted party

and two users, say Alice and Bob. The basic idea of VES is that Alice who has a key pair of signature scheme signs a given message and encrypts the resulting signature under the trusted party's public key, and uses a noninteractive zero-knowledge (NZK) proof [35] to convince Bob that she has signed the message and the trusted party can recover the signature from the ciphertext. After validating the proof, Bob can send his signature for the same message to Alice. For the purpose of fair exchange, Alice should send her signature in plaintext back to Bob after accepting Bob's signature. If she refuses to do so, however, Bob can get her signature from the trusted party by providing Alice's encrypted signature and his own signature, so that the trusted party can recover Alice's signature and sends it to Bob, meanwhile, forwards Bob's signature to Alice. Thus, fair exchange is achieved.

The basic idea of the improved scheme can be highlighted as follows. User  $U_i$ 's credential is  $S_i = h(ID_i)^{2d} \bmod N$ , i.e., SCPC's RSA signature on the square of the hashed user identity (in contrast to  $S_i = h(ID_i)^d \bmod N$  in [19]). For user authentication,  $U_i$  will encrypt his/her credential  $S_i$  using ElGamal encryption of SCPC's other public key  $y = g^u$  by computing  $P_1 = S_i \cdot y^r \bmod N$  and  $P_2 = g^r \bmod N$ , where  $g \in \mathbb{Z}_N^*$  of big order and  $u$  is SCPC's secret decryption key. In this improvement, SCPC also plays the role of the trust authority in VES. To convince a service provider that  $(P_1, P_2)$  does encrypt his/her credential  $S_i$  (i.e. SCPC's RSA signature for  $ID_i$ ),  $U_i$  must also provide an NZK proof  $x$  to show that he or she knows a secret  $r$  such that  $P_1^e / h(ID_i)^2 = (y^e)^r \bmod N$  and  $P_2 = g^r \bmod N$ . Such a proof  $x$ , is called 'proving the equality of two discrete logarithms in a group of unknown order' [21], will convince the service provider without leaking any useful information about  $U_i$ 's credential  $S_i$ . For server authentication, service providers can simply issue signatures as the work in [19] did, though the proposed changes give service providers the freedom to employ any secure signature scheme. The other procedures are the same as in the Chang-Lee scheme.

#### A. Initialization Phase

SCPC selects two large safe primes  $p$  and  $q$  to set  $N = pq$ . Namely, there are two primes  $p'$  and  $q'$  such that  $p = 2p' + 1$  and  $q = 2q' + 1$ . SCPC now sets its RSA public/private key pair  $(e, d)$  such that  $ed \equiv 1 \bmod 2p'q'$ , where  $e$  is a prime. Let  $Q_N$  be the subgroup of squares in  $\mathbb{Z}_N^*$  whose order  $\#G = p'q'$  is unknown to the public but its bit-length  $l_G = |N| - 2$  is publicly known. SCPC randomly picks generator  $g$  of  $Q_N$ , selects an ElGamal decryption key  $u$ , and computes the corresponding public key  $y = g^u \bmod N$ . In addition, for completing the Diffie-Hellman key exchange SCPC chooses generator  $\bar{g} \in \mathbb{Z}_N^*$ , where  $n$  is another large prime number. SCPC also chooses a cryptographic hash function  $h(\cdot) : \{0, 1\}^* \rightarrow \{0, 1\}^k$ , where security parameter  $k$  satisfies  $160 \leq k \leq |N| - 1$ . Another security parameter  $\epsilon > 1$  is chosen to control the tightness of the ZK proof [34]. Finally, SCPC publishes  $(e, N, h(\cdot), \epsilon, g, y, \bar{g}, n)$ , and keeps  $(d, u)$  secret.

#### B. Registration Phase

In this phase, upon receiving a register request, SCPC gives  $U_i$  fixed-length unique identity  $ID_i$  and issues credential  $S_i =$

$h(ID_i)^{2d} \bmod N$ .  $S_i$  calculated as SCPC's RSA signature on  $h(ID_i)^2$  is an element of  $Q_N$ , which will be the main group we are calculating.

As in [19], each service provider  $P_j$  with identity  $ID_j$  should maintain a pair of signing/verifying keys for a secure signature scheme (not necessarily RSA).  $\sigma_j(SK_j, Msg)$  denotes the signature  $\sigma_j$  on message  $Msg$  signed by  $P_j$  using signing key  $SK_j$ .  $Ver(PK_j, Msg, \sigma_j)$  denotes verifying of signature  $\sigma_j$  with public key  $PK_j$ , which outputs "1" or "0" to indicating if the signature is valid or invalid, respectively.

#### C. Authentication Phase

In this phase, RSA-VES is employed to authenticate a user, while a normal signature is used for service provider authentication. The details are illustrated in Fig. 2 and further explained as follows.

- 1)  $U_i$  sends a service request with nonce  $n_1$  to service provider  $P_j$ .
- 2) Upon receiving  $(Req, n_1)$ ,  $P_j$  calculates its session key material  $Z = g^k \bmod n$  where  $k \in \mathbb{Z}_n^*$  is a random number, sets  $u = Z || ID_j || n_1$ , issues a signature  $v = \sigma_j(SK_j, u)$ , and then sends  $m_2 = (Z, v, n_2)$  to the user, where  $n_2$  is a nonce selected by  $P_j$ .
- 3) Upon receiving  $m_2 = (Z, v, n_2)$ ,  $U_i$  sets  $u = Z || ID_j || n_1$ .  $U_i$  terminates the conversation if  $Ver(PK_j, u, v) = 0$ . Otherwise,  $U_i$  accepts service provider  $P_j$  because the signature  $v$  is valid. In this case,  $U_i$  selects a random number  $t \in \mathbb{Z}_n^*$  to compute  $w = g^t \bmod n$ ,  $k_{ij} = Z^t \bmod n$ , and the session key  $K_{ij} = h(ID_j || k_{ij})$ . For user authentication,  $U_i$  first encrypts his/her credential  $S_i$  as  $(P_1 = S_i \cdot y^r \bmod N, P_2 = g^r \bmod N)$ , where  $r$  is a random integer with binary length  $l_G$ . Next,  $U_i$  computes two commitments  $a = (y^e)^{r_1} \bmod N$  and  $b = g^{r_1} \bmod N$ , where  $r_1 \in \pm\{0, 1\}^{\epsilon(l_G+k)}$  is also a random number. After that,  $U_i$  computes the evidence showing that credential  $S_i$  has been encrypted in  $(P_1, P_2)$  under public key  $y$ . For this purpose,  $U_i$  calculates  $c = h(K_{ij} || w || n_2 || y^{er} || P_2 || y^e || g || a || b)$  and  $s = r_1 - c \cdot r$  (in  $\mathbb{Z}$ ). Then,  $x = (P_1, P_2, a, b, c, s)$  is the NIZK proof for user authentication. In fact, it is precisely, the processes of generating  $x$  which is the proof part of RSA-VES [21]. Finally,  $U_i$  encrypts his/her identity  $ID_i$ , new nonce  $n_3$ , and  $P_j$ 's nonce  $n_2$  using session key  $K_{ij}$  to get ciphertext  $CT = E_{K_{ij}}(ID_i || n_3 || n_2)$ , and thereafter sends  $m_3 = (w, x, CT)$  to service provider  $P_j$ .
- 4) To verify  $U_i$ ,  $P_j$  calculates  $k_{ij} = w^k \bmod n$ , the session key  $K_{ij} = h(ID_j || k_{ij})$ , and then uses  $K_{ij}$  to decrypt  $CT$  and recover  $(ID_i, n_3, n_2)$ . Then,  $P_j$  computes  $y^{er} = P_1^e / h(ID_i)^2 \bmod N$ ,  $a = (y^e)^s \cdot (y^{er})^c \bmod N$ ,  $b = g^s \cdot P_2^c \bmod N$ , and checks if  $(c, s) \in \{0, 1\}^k \times \pm\{0, 1\}^{\epsilon(l_G+k)+1}$  and  $c = h(K_{ij} || w || n_2 || y^{er} || P_2 || y^e || g || a || b)$ . If the output is negative,  $P_j$  aborts the conversation. Otherwise,  $P_j$  accepts  $U_i$  and believes that they have shared the same session key  $K_{ij}$  by sending  $U_i m_4 = (V)$  where  $V = h(n_3)$ .
- 5) After  $U_i$  receives  $V$ , he checks if  $V = h(n_3)$ . If this is true, then  $U_i$  believes that they have shared the same session key  $K_{ij}$ . Otherwise,  $U_i$  terminates the conversation.

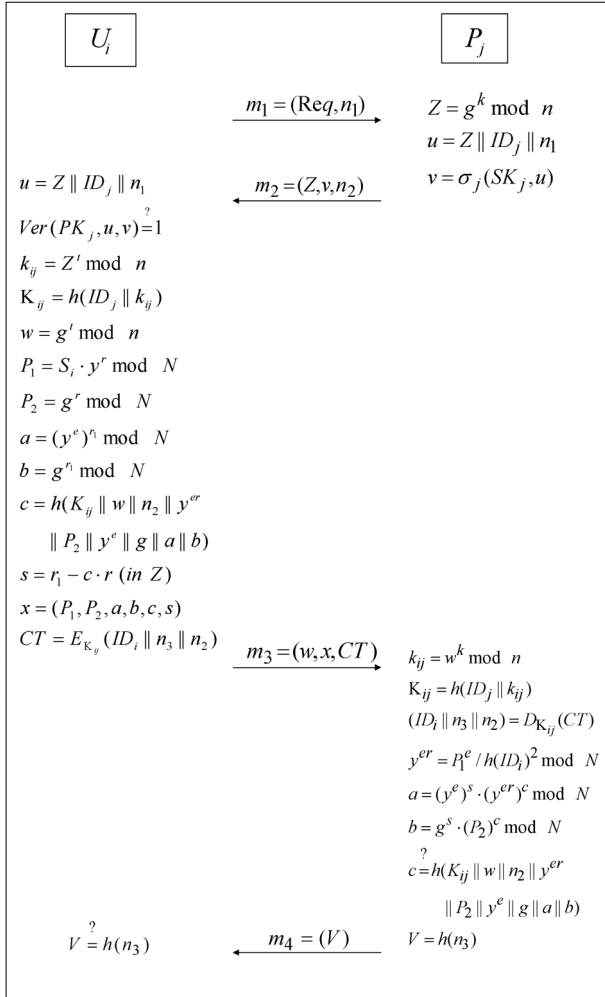


Fig. 2. Our improved scheme.

#### D. Security Analysis

We now analyze the security of the improved SSO scheme by focusing on the security of the user authentication part, especially soundness and credential privacy due to two reasons. On the one hand, the unforgeability of the credential is guaranteed by the unforgeability of RSA signatures, and the security of service provider authentication is ensured by the unforgeability of the secure signature scheme chosen by each service provider. On the other hand, other security properties (e.g., user anonymity and session key privacy) are preserved, since these properties have been formally proved in [19] and the corresponding parts of the Chang–Lee scheme are kept unchanged.

Soundness requires that without holding valid credential  $S^*$  corresponding to a target user  $U^*$ , an attacker, who could be a collusion of users and service providers, has at most a negligible probability of generating proof  $x^*$  and going through user authentication by impersonating user  $U^*$ . The soundness of the above improved SSO scheme relies on the soundness of the NIZK proof, which also guarantees the soundness of RSA-VES, defined as the second property of Definition 1 in [21]. Namely, if the user authentication part is not sound, i.e., an attacker can

present valid proof  $x^*$  without holding the corresponding credential  $S^*$  in non-negligible probability, then this implies the NIZK proof of proving equality of two discrete logarithms in a group of unknown order is not sound, contradictory to the analysis given in [21, Sec. 3.7].

Credential privacy or credential irrecoverableness requires that there be a negligible probability of an attacker recovering a valid credential from the interactions with a user. Again this property can be deduced from the signature hiding property of RSA-VES, defined as the third property of Definition 1 in [21]. Signature hiding means that an attacker cannot extract a signature from VES without help from the user who encrypted the signature or the trusted authority who can decrypt a VES. So, if this improved SSO scheme fails to meet credential privacy, it implies that Ateniese’s RSA-VES fails to satisfy signature hiding, which is contrary to the analysis given in [21, Sec. 3.7]. In fact, soundness and signature hiding are the two core security properties to guarantee the fairness of digital signature exchange using VES.

More rigorous security proofs are interesting topics for further study by considering formal definitions first.

## VI. CONCLUSION

In this paper, we demonstrated two effective impersonation attacks on Chang and Lee’s single sign-on (SSO) scheme [19]. The first attack shows that their scheme cannot protect the privacy of a user’s credential, and thus, a malicious service provider can impersonate a legal user in order to enjoy the resources and services from other service providers. The second attack violates the soundness of authentication by giving an outside attacker without credential the chance to impersonate even a non-existent user and then freely access resources and services provided by service providers. We also discussed why their well-organized security arguments are not strong enough to guarantee the security of their SSO scheme. In addition, we explained why Hsu and Chuang’s scheme [12] is also vulnerable to these attacks. Furthermore, by employing an efficient verifiable encryption of RSA signatures introduced by Ateniese [21], we proposed an improved Chang–Lee scheme to achieve soundness and credential privacy. As future work, it is interesting to formally define authentication soundness and construct efficient and provably secure single sign-on schemes. Based on the draft of this work [36], a preliminary formal model addressing the soundness of SSO has been proposed in [37]. Further research is necessary to investigate the maturity of this model and study how the security of the improved SSO scheme proposed in this paper can be formally proven.

## REFERENCES

- [1] A. C. Weaver and M. W. Condry, “Distributing internet services to the network’s edge,” *IEEE Trans. Ind. Electron.*, vol. 50, no. 3, pp. 404–411, Jun. 2003.
- [2] L. Barolli and F. Xhafa, “JXTA-OVERLAY: A P2P platform for distributed, collaborative and ubiquitous computing,” *IEEE Trans. Ind. Electron.*, vol. 58, no. 6, pp. 2163–2172, Oct. 2010.
- [3] L. Lamport, “Password authentication with insecure communication,” *Commun. ACM*, vol. 24, no. 11, pp. 770–772, Nov. 1981.



- [4] W. B. Lee and C. C. Chang, "User identification and key distribution maintaining anonymity for distributed computer networks," *Comput. Syst. Sci. Eng.*, vol. 15, no. 4, pp. 113–116, 2000.
- [5] W. Juang, S. Chen, and H. Liaw, "Robust and efficient password authenticated key agreement using smart cards," *IEEE Trans. Ind. Electron.*, vol. 15, no. 6, pp. 2551–2556, Jun. 2008.
- [6] X. Li, W. Qiu, D. Zheng, K. Chen, and J. Li, "Anonymity enhancement on robust and efficient password-authenticated key agreement using smart cards," *IEEE Trans. Ind. Electron.*, vol. 57, no. 2, pp. 793–800, Feb. 2010.
- [7] M. Cheminod, A. Pironti, and R. Sisto, "Formal vulnerability analysis of a security system for remote fieldbus access," *IEEE Trans. Ind. Inf.*, vol. 7, no. 1, pp. 30–40, Feb. 2011.
- [8] A. Valenzano, L. Durante, and M. Cheminod, "Review of security issues in industrial networks," *IEEE Trans. Ind. Inf.*, vol. PP, no. 99, 2012, DOI 10.1109/TII.2012.2198666.
- [9] T.-S. Wu and C.-L. Hsu, "Efficient user identification scheme with key distribution preserving anonymity for distributed computer networks," *Comput. Security*, vol. 23, no. 2, pp. 120–125, 2004.
- [10] Y. Yang, S. Wang, F. Bao, J. Wang, and R. H. Deng, "New efficient user identification and key distribution scheme providing enhanced security," *Comput. Security*, vol. 23, no. 8, pp. 697–704, 2004.
- [11] K. V. Mangipudi and R. S. Katti, "A secure identification and key agreement protocol with user anonymity (SIKA)," *Comput. Security*, vol. 25, no. 6, pp. 420–425, 2006.
- [12] C.-L. Hsu and Y.-H. Chuang, "A novel user identification scheme with key distribution preserving user anonymity for distributed computer networks," *Inf. Sci.*, vol. 179, no. 4, pp. 422–429, 2009.
- [13] B. Wang and M. Ma, "A server independent authentication scheme for RFID systems," *IEEE Trans. Ind. Inf.*, vol. 8, no. 3, pp. 689–696, Aug. 2012.
- [14] B. Fabian, T. Ermakova, and C. Muller, "SHARDIS: A privacy-enhanced discovery service for RFID-based product information," *IEEE Trans. Ind. Inf.*, vol. 8, no. 3, pp. 707–718, Aug. 2012.
- [15] H.-M. Sun, Y.-H. Chen, and Y.-H. Lin, "oPass: A user authentication protocol resistant to password stealing and password reuse attacks," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 651–663, Apr. 2012.
- [16] "Security Forum on Single Sign-On," The Open Group [Online]. Available: <http://www.opengroup.org/security/12-ss0.htm>
- [17] J. Han, Y. Mu, W. Susilo, and J. Yan, "A generic construction of dynamic single sign-on with strong security," in *Proc. SecureComm*, 2010, pp. 181–198, Springer.
- [18] L. Harn and J. Ren, "Generalized digital certificate for user authentication and key establishment for secure communications," *IEEE Trans. Wireless Commun.*, vol. 10, no. 7, pp. 2372–2379, Jul. 2011.
- [19] C.-C. Chang and C.-Y. Lee, "A secure single sign-on mechanism for distributed computer networks," *IEEE Trans. Ind. Electron.*, vol. 59, no. 1, pp. 629–637, Jan. 2012.
- [20] U. Feige, A. Fiat, and A. Shamir, "Zero-knowledge proofs of identity," *J. Cryptography*, vol. 1, no. 2, pp. 77–94, 1988.
- [21] G. Ateniese, "Verifiable encryption of digital signatures and applications," *ACM Trans. Inf. Syst. Secur.*, vol. 7, no. 1, pp. 1–20, 2004.
- [22] H. Delfs and H. Knebl, *Introduction to Cryptography: Principles and Applications*, 2nd ed. Berlin, Germany: Springer, 2006.
- [23] G. Tenenbaum, *Introduction to Analytic and Probabilistic Number Theory*. Cambridge, U.K.: Cambridge Univ., 1995, p. 41.
- [24] E. W. Weisstein, "Relatively Prime," MathWorld-A Wolfram Web Resource [Online]. Available: <http://mathworld.wolfram.com/RelativelyPrime.html>
- [25] *Public Key Cryptography Standards, PKCS #1 v2.1*, RSA Cryptography Standard, Draft 2, PKCS, 2001 [Online]. Available: <http://www.rsasecurity.com/rsalabs/pkcs/>
- [26] D. Boneh, "Twenty years of attacks on the RSA cryptosystem," *Notices Amer. Math. Soc.*, vol. 46, no. 2, pp. 203–213, 1999.
- [27] Wikipedia, RSA (algorithm) [Online]. Available: [http://en.wikipedia.org/wiki/RSA\\_\(algorithm\)](http://en.wikipedia.org/wiki/RSA_(algorithm))
- [28] Y. Xu, R. Song, L. Korba, L. Wang, W. Shen, and S. Y. T. Lang, "Distributed device networks with security constraints," *IEEE Trans. Ind. Inf.*, vol. 1, no. 4, pp. 217–225, Nov. 2005.
- [29] M. Burrows, M. Abadi, and R. Needham, "A logic of authentication," *ACM Trans. Comput. Syst.*, vol. 8, no. 1, pp. 18–36, 1990.
- [30] M. Bellare and P. Rogaway, "Entity authentication and key distribution," in *Proc. of CRYPTO*, 1993, pp. 232–249.
- [31] C. Boyd and W. Mao, "On a limitation of BAN Logic," in *Proc. of EUROCRYPT*, 1994, pp. 240–247.
- [32] N. Asokan, V. Shoup, and M. Waidner, "Optimistic fair exchange of digital signatures," *IEEE J. Sel. Areas Commun.*, vol. 18, no. 4, pp. 591–606, Apr. 2000.
- [33] J. Camenisch and M. Michels, "Conformer signature schemes secure against adaptive adversaries," in *Proc. EUROCRYPT*, 2000, pp. 243–258.
- [34] G. Ateniese, J. Camenisch, M. Joye, and G. Tsudik, "A practical and provably secure coalition-resistant group signature scheme," in *Proc. CRYPTO*, 2000, pp. 255–270.
- [35] D. Chaum and T. P. Pedersen, "Wallet databases with observers," in *Proc. of CRYPTO*, 1993, pp. 89–105.
- [36] G. Wang, J. Yu, and Q. Xie, "Security analysis of a single sign-on mechanism for distributed computer networks Cryptology ePrint Archive, Rep. 102, Feb. 2012 [Online]. Available: <http://eprint.iacr.org/2012/107>
- [37] J. Yu, G. Wang, and Y. Mu, "Provably secure single sign-on scheme in distributed systems and networks," in *Proc. 11th IEEE TrustCom*, Jun. 2012, pp. 271–278.

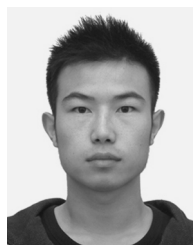


**Guilin Wang** received the Ph.D. degree in computer science from the Institute of Software, Chinese Academy of Sciences, Beijing, China, in 2001.

He is currently a Senior Lecturer with the School of Computer Science and Software Engineering, University of Wollongong, Australia. Before this, he was a Lecturer with the School of Computer Science, University of Birmingham, Birmingham, U.K., a Research Scientist with the Institute for Info-comm Research (I<sup>2</sup>R), Singapore, and an Assistant Professor with the Institute of Software, Chinese

Academy of Sciences, Beijing, China. He has authored or coauthored more than 70 research publications in the areas of applied cryptography, information security, and electronic commerce. His main research interests include the analysis, design, and applications of digital signatures and security protocols.

Dr. Wang has served as a program co-chair for six international security conferences, a committee member for more than 50 international conferences or workshops, and a reviewer for over 20 international journals.



**Jiangshan Yu** received the M.S. degree in computer science from the Center for Computer and Information Security Research, School of Computer Science and Software Engineering, University of Wollongong, Australia, in 2011, where he is currently working toward the M.S. degree.

His research topic is authentication in distributed computer networks.



**Qi Xie** received the Ph.D. degree in applied mathematics from Zhejiang University, Hangzhou, China, in 2005.

He is a Professor with the School of Information Science and Engineering, Hangzhou Normal University, Hangzhou, China. He was a Visiting Scholar between 2009 and 2010 with the Department of Computer Science, University of Birmingham, Birmingham, U.K., and a Visiting Scholar with the Department of Computer Science, City University of Hong Kong, in 2012. His research area is applied

cryptography, including digital signatures, authentication and key agreement protocols etc. He has authored or coauthored over 40 research papers in international and domestic journals and conferences.