A NEW SECRET HANDSHAKES SCHEME WITH DYNAMIC MATCHING BASED ON ZSS

Preeti Kulshrestha and Arun Kumar Pal

Department of Mathematics, Statistics & Computer Science

G.B. Pant University of Agriculture and Technology

Pant Nagar, India

ABSTRACT

Balfanz et al. in 2003, introduced the primitive secret handshakes (SH) as a two party protocol together with a notion of roles and implements it using pairing based cryptography, the scheme allows two parties to make a match (authentication & verification) and derive a shared common session key if and only if they belong to same group. If the parties do not belong to the same group, they cannot make any conclusion about the veracity of other's affiliation. Ateniese et al. in 2007 presented a SH with dynamic matching in which each party can specify both the group and the role the other must have in order to complete a successful handshake. This paper presents a new SH scheme with dynamic matching which is computationally comparable with the scheme of Ateniese et al. The proposed scheme is inspired on an identity based authenticated key agreement proposed by McCullagh et al. and uses ZSS signature. The paper also gives security proofs for the new scheme in the random oracle.

KEYWORDS

Secret Handshakes, Authentication, Dynamic Matching, Pairing based Cryptography, Bilinear Pairing, ZSS Signature.

1. INTRODUCTION

The secret handshakes (SH) are an important research subject in the field of privacy-preserving authentication protocols. It is a cryptographic protocol introduced by Balfanz et al. [2] in 2003, which allows two members of a specific group to authenticate themselves secretly in the sense that each party reveals his affiliation to the other only if the other party is also a member of the same group. They also introduced the SH with roles, so that a group member *A* can specify a role another group member *B* must have in order to successfully complete the handshake. As in secret handshakes group members can play different roles within a group, and can authenticate themselves in these roles. For example, a CBI agent *A* wants to discover and communicates with other agent *B*, but they don't want to reveal their affiliations to non-agents. If *B* is not a CBI agent, then the protocol should not help *B* in determining whether *A* is a CBI agent or not, and vice versa. In other words, the SH scheme enables two members who belong to same group *G* to authenticate each other in a way that hides their affiliation from all others.

DOI:10.5121/ijnsa.2015.7106

2. Related Work

The secret handshakes scheme by Balfanz adapts the non interactive key agreement protocol of Sakai et al. [12] based on bilinear maps. The scheme is secure under the BDH assumption. It uses one time credentials to achieve the unlinkability, which means that each user must store a large number of credentials. In 2004 Castelluccia et al. [3] constructed two party secret handshakes scheme with one group by using CA-Oblivious encryption. This solution is secure under CDH assumption. Both these schemes are secure in the random oracle model.

Ateniese et al. [1] introduced SH with dynamic matching which is the first efficient unlinkable SH scheme, allowing to verify the presence of properties different from the user's own. Their scheme treats a set of members with identical attribute as an entity instead of different individual. It is essentially a group key agreement scheme between different sub-group members in a large group environment. Property credentials are issued by a certification authority (CA). This scheme is somewhat in between SH and secures matchmaking protocol.

Sorniotti et al. [13] also proposed a similar concept of dynamic controlled matching allowing an authorized prover to convince an authorized verifier that she owns a property. Both schemes allow more flexible types of secret handshakes. Users holding credentials for different properties can conduct successful secret handshakes; if credentials match the other user's matching references. The difference between the two schemes is the control that the CA retains over the matching ability. However, neither of them supports revocation of credentials. Sorniotti and Molva [14] presented an SH scheme with revocation which allows a user to prove to a verifier possession of a credential. Credentials can be revoked simply by publishing a value in a revocation list.

Lu et al. [9] introduced secure same symptom based SH scheme which allows a patient to securely share a PHI (Patient Health Information) and conduct extensive simulations to evaluate its efficiency in terms of PHI reporting delay. Ryu et al. [11] introduced unlinkable SH for anonymous communications allowing two arbitrary communication parties with the same role in either one single group or multiple groups to privately authenticate each other. Recently Kulshrestha et al. [8] points out that Ryu et al. scheme is insecure to key compromise impersonation attack. Wen et al. [17] proposed an unlinkable SH with fuzzy matching for social network, it supports more flexible threshold based appropriate matching under the multiple groups environment which is not limited to authenticate between members from the same group and which is secure under the decisional bilinear Diffie -Hellman assumption.

Vergnaud [16] constructed a SH scheme using RSA signature and Zhou et al. [24] constructed a SH scheme using ElGamal and DSA signature. Both the schemes rely on random oracles for their security and uses one time credential to insure that handshake protocol performed by the same party cannot be linked. Xu -Yung [20] proposed SH scheme that achieves unlinkability with reusable credentials. They introduced the concept of k-anonymous secret handshakes where k is an adjustable parameter indicating the desired anonymity assurance. Huang -Cao [5] in 2009 proposed an efficient unlinkable secret handshakes scheme and claimed that scheme achieves affiliation hiding and unlinkability. However Su [15] and Youn -Park [22] proved that Huang -Cao scheme has a design flaw and is insecure.

Gu -Xue [4] in 2011 proposed an improved secret handshakes scheme with unlinkability based on the Huang -Cao scheme. Yoon [21] in 2011 points out that Gu -Xue scheme is insecure to key compromise impersonation attack and cannot provide master key forward secrecy. Jarecki and Liu [6] proposed a practical unlinkable secret handshakes scheme that supports both traceability and revocation with reusable credentials. Resorting to group signature with message recovery, Kawai et al. [7] proposed a conditional unlinkable secret handshakes scheme. Wen et al. [19] proposed a new generic framework for constructing two-party secret handshakes schemes from ID-based message recovery signatures. Inspired by Kawai et al. scheme [7], Wen et al. [18] also proposed unlinkable secret handshakes from message recovery signature.

In this paper we propose a new SH scheme with dynamic matching from bilinear pairing. Our scheme is constructed from Bilinear Inverse Diffie- Hellman. Our proposed SH scheme is constructed using Ateniese et al. [1]. Our scheme is based on ZSS signature [23] and is inspired by identity based authenticated key agreement by McCullagh et al. [10]. We also give security proofs for the new scheme in the random oracle model.

Organization:

The remainder of this paper is organized as follows. Section 3 recalls the preliminaries related to our work. Section 4 describes definitions and security requirements of a secret handshakes scheme. In Section 5 we give our secret handshakes scheme with dynamic matching based on ZSS signature. Section 6 gives the security analysis of our proposed scheme. In section 7 we discuss efficiency issues. Finally we draw our conclusion in Section 8.

3. Preliminaries

3.1 Bilinear Pairing:

Let G_1 and G_2 be two cyclic groups of the same large prime order q. G_1 is denoted as an additive group and G_2 as a multiplicative group. Let P denote a generator of G_1.
A *Bilinear Pairing* is a function $e: G_1 \times G_1 \rightarrow G_2$ with the following properties:
(1) [Bilinearity] for $P \in G_1$ and $a, b \in_R Z_q^*$, $e(aP, bP) = e(P, P)^{ab}$.
(2) [Non-degeneracy] $e(P, P) \neq 1$.
(3) [Computability] *e* can be efficiently computed in polynomial time.

3.2 Some Mathematical problems in G_1, G_2 are described as follows:

- ***Computational Diffie-Hellman (CDH) problem:*** The CDH problem is to compute *abP* when given *P*, *aP* and *bP* for some $a, b \in_R Z_q^*$.
- ***Inverse Computational Diffie-Hellman (ICDH) problem:*** The ICDH problem is to compute $a^{-1}P$ when given *P* and *aP* for some $a \in_R Z_q^*$.
- ***Modified Inverse Computational Diffie-Hellman (mICDH) problem:*** The mICDH problem is to compute $(a+b)^{-1}P$ when given *bP, P, aP* and *(a+b)P* for some $a, b \in_R Z_q^*$.
- ***Bilinear Diffie Hellman Problem (BDH):*** The BDH problem is to compute $e(P, P)^{abc}$ when given P, aP, bP and cP for some $a, b, c \in_R Z_q^*$.
- ***Bilinear Inverse Diffie Hellman Problem (BIDH):*** The BIDH problem is to compute $e(P, P)^{a^{-1}b}$ when given P, aP and bP for some $a, b \in_R Z_q^*$.
- ***Modified Bilinear Inverse Diffie- Hellman (mBIDH) Problem:*** The mBIDH problem is to compute $e(P, P)^{(a+b)^{-1}c}$ when given b, P, aP and cP for some $a, b, c \in_R Z_q^*$.

3.3 ZSS Signature:

ZSS Signature was proposed by Zhang et al. [23] in 2004. The signature scheme consists of four algorithms a parameter generation algorithm ***ParamGen*****,** a key generation algorithm ***KeyGen*****,** a signature generation algorithm ***Sign*** and a signature verification algorithm ***Ver***.

Signature scheme is as follows:

ParamGen:

Given a security parameter the algorithm generates the system parameter $\langle G_1, G_2, e, q, P, H\rangle$ where G_1 and G_2 are the two cyclic groups of same order q, and P is a generator of G_1, e is the bilinear map and $H : \{0,1\}^* \rightarrow Z_q^*$ is the cryptographic hash function.

KeyGen:

Randomly selects $s \in_R Z_q^*$ as the secret key and computes $P_{Pub} = sP$ as the public key.

Sign:

Given a secret key s, and a message m, computes the signature $S = \frac{1}{H(m)+s} P$.

Ver:

Given a public key P_{Pub}, a message m, and a signature S, verifies if

$$e(H(m)P + P_{Pub}, S) = e(P, P).$$

The verification works because

$$e(H(m)P + P_{Pub}, S) = e(H(m)P + sP, (H(m) + s)^{-1}P) = e(P, P).$$

4. Secret Handshakes (SH) Scheme

In SH scheme there exists three entities for a group G, a user who may or may not be a member of G, a user who belongs to the group and a group administrator (GA) who creates and adds members into the group, and issues certificate in a form of secret key to members.

A **secret handshakes** scheme consists of the following algorithms:

Create Group:

This is an algorithm run by a group administrator GA, which takes params as input and generates a key pair GP_K (group public key) and GS_K (group secret key).

Add User:

This is an algorithm between a user U and the GA of some group. It takes params and GA's secret GS_K as input and output a public key P_K and secret key S_K for U and makes U a valid member of the group.

Handshake:

This is the authentication protocol. It is executed between users *A* and *B*, who want to authenticate each other on the public inputs ID_A, ID_B and params. The private input of each party is their secret credential and the output of the protocol for either party is either 'reject' or 'accept' (*A* and *B* belong to the same group if and only if the output is 'accept'). At the end of the protocol, if *A's* requirements for *B* are matched by *B's* credentials and *B's* requirements for *A* are matched by *A's* credentials, *A* and *B* authenticate by sharing a common key otherwise such authentication fails**.**

A secret handshakes scheme must have the following **security properties:**

Completeness/ Correctness:

If two honest members *A, B* belonging to the same group and run handshake protocol with valid credentials of their ID_S and group public keys, then both members always output "accept".

Impersonator Resistance:

An adversary not satisfying the rules of the handshake protocol is unable to successfully authenticate to an honest member.

Detector Resistance:

An adversary not satisfying the rules of the handshake protocol cannot decide whether some honest party satisfies the rule or not.

Unlinkability:

It is not feasible to tell whether two execution of the handshake protocol were performed by the same party or not, even if both them were successful.

5. Proposed Scheme

In this section we propose a secret handshakes scheme with dynamic matching based on of ZSS signature [23]. Our scheme uses same technique as Ateniese et al. [1].

Create Group:

The GA inputs a security parameter *k* into BDH parameter generator which returns

Params: $\langle G_1, G_2, e, P, q, H, P_{Pub} \rangle$ as defined in section 3.

Add User:

For a user U, GA computes $Q_U = H(group\, ID_U \parallel r_U)$ where group ID_U is the group identity of the user U and r_U is its role. It then issues public key as $\alpha_U = (Q_U + s)P$ and secret key as $\beta_U = (Q_U + s)^{-1}P$.

Handshake:

Suppose *A* with secret β_A on the identity $group\, ID_A$ and role r_A and *B* with secret β_B on the identity $group\, ID_B$ and role r_B engage in a handshake protocol. They should successfully complete the protocol if the group and the role specified by *A* for *B* matches *B*'s credentials and group and role specified by *B* for *A* matches *A*'s credentials.

The protocol proceeds as follows:

1. A chooses unique random nonce $x \in_R Z_q^*$ and sends

$$X = x((H(group\ ID'_B \,||r'_B\,))P + P_{Pub}),$$

where r'_B is the role and $groupID'_B$ is the group identity that B must have in order to complete the handshake.

2. Similarly, B chooses unique random nonce $y \in_R Z_q^*$ and sends

$$Y = y((H(group\ ID'_A \,||r'_A\,))P + P_{Pub}),$$

where r'_A is the role and $groupID'_A$ is the group identity that A must have in order to complete the handshake.

3. Using the knowledge of x and what A just received from B, A computes the following key:
$k_1 = e(P,P)^x$ and $k_2 = e(Y,\beta_A)$.

4. Using the knowledge of y and what B just received from A, B computes the following key:
$k_1 = e(X,\beta_B)$ and $k_2 = e(P,P)^y$.

If $group\ ID_A = group\ ID'_A$, $group\ ID_B = group\ ID'_B$, $r_A = r'_A$, and $r_B = r'_B$, then at the end of the handshake both A and B share a secret key $k = (k_1, k_2)$.

Correctness:

If the participants satisfy the rules of the handshakes protocol, they will successfully share a common key. For correctness of scheme we show that the shared key that A and B computes the same.

For A we have

$$k_2 = e(Y,\beta_A) = e\left(y\left(\left(H(group\ ID'_A \parallel r'_A)\right)P + P_{Pub}\right), (H(group\ ID_A \parallel r_A) + s)^{-1}P)\right),$$

if $group\ ID_A = group\ ID'_A$, and $r_A = r'_A$, then

$k_2 = e(P,P)^y$.

Similarly for user B

$$k_1 = e(X,\beta_B) = e\left(x\left(\left(H(group\ ID'_B \parallel r'_B)\right)P + P_{Pub}\right), (H(group\ ID_B \parallel r_B) + s)^{-1}P)\right),$$

if $group\ ID_B = group\ ID'_B$, and $r_B = r'_B$, then

$k_1 = e(P,P)^x$.

6. Security

An adversary A who can forge a valid ZSS signature can surely attack the SH protocol just as an honest member. Hence the probability to attack SH scheme cannot be smaller than the probability to forge a valid ZSS signature.

Group Member Impersonation:

For an adversary *A* we define a member impersonation game, during which *A* is allowed to corrupt users of her choice, but not GA.

Create:

Adversary *A* setup a new oracle in the system that has public key and secret key for some users. We denote by U_A the users that *A* controls.

Selects:

Adversary *A* selects a target user U_t such that $U_t \notin U_A$ with whom she would like to communicate and wants to detect a target role r_t under which she wants to detect a target user U_t.

Interaction:

Adversary *A* interacts with U_t where $U_t \notin U_A$ in which case U_t may be assumed that he interacts with legitimate user. Since in this scheme during the handshake U_t sends only $a\big((H(group\ ID'_U \parallel r'_U))P + P_{Pub}\big),\ a \in_R Z_q^*$, where $group\ ID'_U \parallel r'_U$ is the expected identity of the other end, this message can be generated by anyone. *A* can impersonate U_t, if U_t cannot distinguish between *A's* message and the real execution of the handshake protocol.

Challenge:

We claim that at the end of the interaction *A* cannot compute the same key that U_t obtains because for calculating the shared key she must possess the secret key which corresponds to the same identity or requirement that U_t want, because even knowing the public key or requirement send by U_t, $(Q_U P + P_{Pub})$ the probability to calculate the secret key $(Q_U + s)^{-1}P$ which correspond to a specific identity is negligible.

$Adv_A^{imp} = Pr[A\ wins\ member\ Impersonation\ Game] < \varepsilon$ is negligible.

Impersonation Resistance:

If *A* never corrupts a member of the target group G_t with role r_t then $U_A \cap U_{G_t,r_t} = \emptyset$. The secret handshakes scheme is said to ensure impersonation resistance if Adv_A^{imp} is negligible for all *A*.

Group Member Detection:

For an adversary *A* we define a member detection game, in which *A* can corrupt users of her choice, the goal of *A* to learns, how to identify member of a certain group.

Create:

Adversary *A* setup a new oracle in the system that has public key and secret key for some users. We denote by U_A the users that *A* controls.

Select:

Adversary *A* selects a target user U_t such that $U_t \notin U_A$ with whom she would like to communicate and wants to detect a target role r_t under which she wants to detect a target user U_t.

Challenge:

An adversary *A* unable to distinguish between U_t and simulator *R* because in our proposed scheme during the handshake U_t sends only $a\big((H(group\ ID'_U \parallel r'_U))P + P_{Pub}\big)$, $a \in_R Z_q^*$, where $group\ ID'_U \parallel r'_U$ is the expected identity of the other end. This message can be generated by anyone. Therefore *A* cannot determine whether it was sent by U_t or a simulator *R* either *A* interacts with U_t or a simulator R. Specifically, to answer a query the oracle flips a fair coin $c \in \{0,1\}$; if the answer is 0, it outputs the target user U_t, and if the answer is 1, it outputs a random simulator. *A* then must decide whether *C* is 0 or 1; call this prediction c'. *A's* advantage in distinguish the target user and random simulator in this game, is given by

$$Adv_A^{det} = |Pr[c' = c] - \frac{1}{2}| .$$

Detection Resistance:

Let G_t be the group to which U_t belongs with role r_t in G_t and suppose *A* never corrupts member of G_t with role r_t the secret handshake scheme is said to ensure detection resistance if $U_A \cap U_{G_t,r_t} = \emptyset$. Then Adv_A^{det} is negligible for all *A*.

Unlinkability:

The property of unlinkability requires that it should be computationally hard for an adversary to link transmitted message by the same party. For an adversary *A* we define a linking game, during which *A* is allowed to corrupt users of her choice, but not GA.

Create:

Adversary *A* setup a new oracle in the system that has secret key for some users. We denote by U_A the users that *A* controls.

Interaction:

Adversary *A* interacts with users of her choice and obtains secrets for some users U_A.

Selects:

Adversary *A* selects a target user U_t such that $U_t \notin U_A$ with whom she would like to communicate and engage in handshake protocols with U_t.

Challenge:

Given a transmitted messages X and Y for secret handshakes, the only way for an adversary to distinguish the messages by the same or different parties is to compute a type of shared secrets $k = (k_1, k_2)$.

In our proposed scheme during the handshake user send only, $a\big((H(group\ ID'_U \parallel r'_U))P + P_{Pub}\big)$, $a \in_R Z_q^*$, where $group\ ID'_U \parallel r'_U$ is the expected identity of the other end. Specifically, to answer a query the oracle flips a fair coin $b = \{0,1\}$; if the answer is 0, it output a handshake protocol with the same user, and if the answer is 1, it outputs a different member which is not corrupted by adversary. *A* then must decide whether *b* is 0 or 1; call this prediction b'. *A's* advantage in linking the target user is given by

$$Adv_A^{link} = |Pr[b' = b] - \frac{1}{2}|.$$

If G_t be the group to which U_t belongs with role r_t in G_t and suppose *A* never corrupts member of G_t with role r_t and a GA of G_t then adversary *A* has at most negligible linking advantage.

6.1 Theorem:

The proposed SH scheme is a secure SH scheme with dynamic matching assuming that BIDH assumption hold.

Proof:

All queries by the adversary *A* now pass through simulator *S*.

Create:

When *A* corrupts users by querying their private keys, *S* answer those queries as follows:

S chooses $y_i \in_R Z_q^*$ creates public keys as

$u_i P = y_i P - sP$

$y_i P = u_i P + sP$

and computes the private key as $y_i^{-1} P$.

Select:

Once *A* declared the target user U_t, simulator *S* answers αP as public key. Since *S* does not know α, it cannot calculate $\alpha^{-1} P$ the correct private key for the user U_t.

Interaction:

Simulator needs to send to *A* message for U_t. *S* chooses βP for an unknown β which is $x(\alpha P)$, where $x \in_R Z_q^*$. In response it will get a value from U_t as the value δP. This is genuine value from U_t and *S* does not influence it.

Compute:

Now the key can be computed by $e(P,P)^{\alpha^{-1}\beta + \delta y_i^{-1}}$ *S* must have non-negligible advantage in calculating $e(P,P)^{\alpha^{-1}\beta + \delta y_i^{-1}}$, because *S* does not know private key $\alpha^{-1} P$ of U_t. *S* sets $\gamma = e(P,P)^{\alpha^{-1}\beta + \delta y_i^{-1}}$. *S* can calculate $e(P,P)^{\alpha^{-1}\beta}$, since it know γ and calculate $\eta = e(P,P)^{\delta y_i^{-1}}$. So *S* can solve BIDH as compute $e(P,P)^{\alpha^{-1}\beta} = \frac{\gamma}{\eta}$.

Hence S can successfully break the BIDHP with non negligible probability ε.

7. Performance Analysis

In this section we compare our construction with Atenniese et al. [1] scheme in terms of computation cost, assumptions and the security properties achieved in table. The following notations are used to analyze the computational cost; **M** is used for multiplication, **E** for exponentiation, **P** for pairing. For both scheme we show the computational cost per party in secret handshake phase. As shown in table-1, computation cost of our scheme is as good as Atenniese et al. [1] schemes.

Table 1.

Schemes	*Computation*	*Assumptions*	*Security Properties*
Ateniese et al.	2M+2P+1E	BDH,SXDH	UL, IR, DR
Proposed	2M+2P+1E	BIDH	UL,IR,DR

BDH, SXDH and BIDH stand for the Bilinear Diffie-Hellman, Symmetric External Diffie-Hellman and Bilinear Inverse Diffie-Hellman assumptions, respectively.

8. Conclusion

In this paper, we have proposed a secret handshakes scheme with dynamic matching, in which each party can specify both the group and the role the other must have in order to complete the handshake. Our secret handshakes scheme is inspired by the McCullagh et al. identity based authenticated key agreement protocol. We constructed the scheme using the technique of Ateniese et al. Our scheme is based on ZSS signature and is secure under BIDH assumption. Since the credential in our scheme is a short signature proposed by Zhang et al.[23], the proofs of completeness, IR and DR can be easily deduced from Zhang et al. signature scheme[23].In terms of computation cost our scheme is as good as Ateniese [1] et al. scheme though our construction is more simple.

ACKNOWLEDGEMENTS

The authors express sincere thanks to Professor Sunder Lal and Mr. Manmohan Singh Chauhan for their help and encouragement.

REFERENCES

[1] G. Ateniese, M. Blanton & J. Kirsch, (2007). "Secret Handshakes with Dynamic and Fuzzy Matching". In Network and Distributed System Security Symposium CERIAS TR, pp. 159-177.

[2] D. Balfanz, G. Durfee, N. Shankar, D. Smetters, J. Staddon, & H. C. Wong, (2003), "Secret Handshakes from Pairing based Key Agreement". In IEEE Symposium on Security and Privacy, pp. 180-196.

[3] C. Castelluccia, S. Jarecki, & G. Tsudik, (2004), "Secret Handshake from CA-Oblivious Encryption". In ASIACRYPT-04, LNCS # 3329 pp. 293-307.

[4] J. Gu & Z. Xue, (2011) "An Improved Efficient Secret Handshakes Scheme with Unlinkability". IEEE Communications Letters, Vol. 15, No. 2, pp. 259-261.

[5] H. Huang & Z. Cao, (2009) "A Novel and Efficient Unlinkable Secret Handshakes Scheme". IEEE Communications Letters, Vol. 13, No. 5, pp. 363-365.

[6] S. Jarecki & X. Liu, (2007) "Unlinkable Secret Handshake & Key Private Group Key Management Scheme". In ACNS-07, LNCS # 4521. Springer-Verlag, pp. 270–287.

[7] Y. Kawai, K. Yoneyama , & K. Ohta , (2009) "Secret Handshake: Strong Anonymity Definition and Construction". In The 5th Information Security Practice an Experience Conference, LNCS # 5451. Springer-Verlag, pp. 219–29.

[8] P. Kulshrestha, A. K. Pal, & M. S. Chauhan, (2015) "Cryptanalysis of Efficient Unlinkable Secret Handshakes for Anonymous Communications". IOSR Journal of Computer Engineering, Vol. 17, issue II, pp. 71-74.

[9] R. Lu, X. Lin, X. Liang & X. Shen, (2010) "Secure Handshake with Symptoms-Matching: Essential to the Success of Mhealthcare Social Network". Proceedings of the 5th International Conference on Body Area Networks, pp. 8-15.

[10] N. McCullagh & Paulo S. L. M. Barreto, (2005) "A New Two Party Identity based Authenticated Key Agreement". Topics in Cryptology CT-RAS-2005, LNCS Volume 3376, pp. 262-274.

[11] E. K. Ryu, K.Y. Yoo & K. S. Ha, (2010) "Efficient Unlinkable Secret Handshakes for Anonymous Communications", Journal of Security Engineering, Vol. 17, No. 6, pp. 619-626.

[12] R. Sakai, K. Ohgishi & M. Kasahara, (2000) "Cryptosystems based on Pairing". In SCIS-2000, Symposium on Cryptography and Information Security, pp. 26-28.

[13] A. Sorniotti & R. Molva (2009) "A Provably Secure Secret Handshake with Dynamic Controlled Matching". In SEC, pp. 330-341.

[14] A. Sorniotti & R. Molva, (2009) "Secret Handshakes with Revocation Support" Proceedings in ICISC Seoul, Korea, pp. 2-4.

[15] R. Su (2009) "On the Security of a Novel and Efficient Unlinkable Secret Handshakes Scheme". IEEE Communications Letters, Vol. 13, No. 9, pp. 712-713.

[16] D. Vergnaud, (2005) "RSA-based Secret Handshakes", Proceedings in WCC 2005, LNCS #3969 Springer-Verlag pp. 252-274.

[17] Y. Wen & Z, Gong, (2013) "An Unlinkable Secret Handshake With Fuzzy Matching For Social Network". 8th International Conference on P2P, Parallel Grid, Cloud & Internet Computing, Vol. 59, pp. 347-352.

[18] Y. Wen, F. Zhang & L. Xu, (2010) "Unlinkable Secret Handshakes from Message Recovery Signature". Chinese Journal of Electronics, Vol.19, No.4, pp. 705-709.

[19] Y. Wen, F. Zhang & L. Xu (2012) "Secret Handshakes from ID-Based Message Recovery Signatures: a Generic Approach" Computers & Electrical Engineering Vol. 38, pp. 96-104.

[20] S. Xu & M. Yung (2004) "K- Anonymous Secret Handshakes with Reusable Credentials" in Proc. CCS'04: 11th ACM Conference on Computer and Communications Security, pp. 158-167.

[21] E. J. Yoon (2011) "Cryptanalysis of an Efficient Secret Handshakes Scheme with Unlinkability". International Conference on Advances in Engineering, Vol. 24 pp. 128-132.

[22] T. Y. Youn & Y. H. Park, (2010) "Security Analysis of an Unlinkable Secret Handshakes Scheme". IEEE Communications Letters, Vol. 14, No. 1, pp. 4-5.

[23] F. Zhang, R. Safavi-Naini & W. Susilo, (2004) "An Efficient Signature Scheme from Bilinear Pairing and its Application". Proceeding in LNCS, Springer Verlag, pp. 277-290.

[24] L. Zhou, W. Susilo & Y. Mu, (2006) "Three Round Secret Handshakes based on ElGamal and DSA". Proceedings in ISPEC 2006, of LNCS #3903, Springer-Verlag, pp. 332-342.

[25] L. Zhou, W. Susilo & Y. Mu, (2007) "New Construction of Group Secret Handshakes based on Pairing", ICICS 2007, LNCS #4861, Springer -Verlag, pp. 16-30.

Authors

Preeti Kulshrestha is a Research Scholar in the Department of Mathematics, Statistics & Computer Science, G. B. Pant University of Agriculture and Technology PantNagar, India. She obtained her M.Phil. degree from Dr. B. R. A. (Agra) University, India in 2008. Her research interest includes secret handshakes, identity based cryptography and digital signature.
Email Id: ibspreeti@gmail.com

Dr. Arun Kumar Pal is an Associate Professor in the Department of Mathematics, Statistics & Computer Science, G. B. Pant University of Agriculture and Technology PantNagar, India. His research areas are Computer Network & RDBMS Soft Computing, Queuing Network and cryptography.

Email Id: arun_pal1969@yahoo.co.in