Identity – Based Multiple Key Agreement Scheme

Massoud Hadian Dehkordi[1] and Reza Alimoradi[1,2]
[1]Department of Mathematical Sciences, Iran University of Science and Technology,
Narmak, Tehran, Iran
[e-mail: mhadian@iust.ac.ir]
[2]Faculty of Science, University of Qom,
Qom, Iran
[e-mail: alimoradi.r@gmail.com]
*Corresponding author: Reza Alimoradi

Received March 12, 2011; revised June 16, 2011; accepted November 13, 2011; published December 31, 2011

Abstract

In order to protect some important information communicated through an insecure network, a common hidden key must be used. One can produce the common hidden key using key agreement protocols; and this helps to have high security in modern data networks. Today, the designers of public key cryptography protocols try to set the public identity of a system's users (like their email addresses) as their public key. This not only makes a cryptographic protocol more efficient but also decreases its cost. These protocols are called "identity – based ". In this article, an identity – based multiple key agreement scheme will be presented; this scheme uses the challenge – response method to do the verification. While the number of random values produced in our scheme is the same as other schemes, the number of keys generated in this scheme is much more than what many other key agreement schemes produce,. Therefore, we will have less computational complexities campered with other schems. In this paper, we consider the security of our scheme and consequently,we will show that it satisfies many security conditions such as strong security.

Keywords: Multiple key agreement, pairing, zero – knowledge proof, identity – based cryptosystems

DOI: 10.3837/tiis.2011.12.007

1. Introduction

With the increasing use of computer networks, designing secure and more efficient protocols in cryptography is more needed. Key agreement and identification protocols are two groups of them which are much applied in internet services like in e – commerce. One of the recent important research topics is methods of producing a secure and efficient common hidden key. The first key agreement scheme was introduced in 1976 by Diffie – Hellman [1]. This scheme's security is based on the difficulty of computing the discrete logarithm problem. In this scheme, the two sides of the protocol succeed in making a common hidden key. Unfortunately, because of not checking the other side's identity against man – in – the – middle attack, the Diffie – Hellman scheme is insecure and every intruder will be able to cheat users. The scheme introduced in this article makes use of challenge – response identification method to verify the user's identities. Some public key challenge – response identification schemes are mentioned in [2][3][4][5][6]. In this article, a multiple key agreement protocol will be introduced which uses pairing functions to produce key. Identity – based cryptography uses a user's public identity (with the desired length), like his/her email address or IP address, as his/her public key. And its corresponding private key is generated by compounding an identity string with the hidden key of a trusted authority called key generation center. The first practical scheme of identity – based cryptography (IBE) was introduced by Boneh – Franklin [7] and was based on pairing. After that many identity – based key agreement protocols came to the scene. In 2002, Smart [8] compounded Boneh – Franklin's idea with the three_ part protocol of Joux [9] and so introduced the first identity – based key agreement protocol. On the other hand, Shim [10][11] rejected Smart's scheme on the grounds of its not having the forward security; and to correct it offered a new identity – based key agreement protocol. Then, Sun – Hiesh [12] found Shim's scheme insecure because of the man – in – the – middle attack. Other identity – based key agreement schemes such as [13][14][15][16][17][18][19][20][21] are also able to generate a key. In 1998, Lin – Harn [5], were the first presenters of multiple key agreement protocols. These protocols are far more efficient compared with other single key agreement protocols. Oh et.al [22] introduced an identity – based key agreement scheme which could produce 2 session keys at the protocol. But as shown in [23], this scheme was insecure too. The identity – based protocol presented by Kim et.al [24] could generate 4 shared keys. It was Shim [25] who found it also insecure. Identity – based schemes, like those mentioned above, make use of pairing functions. Some examples of pairings can be Weil's and Tate's which are defined on a group resulted from the definition of an algebraic curve, like an elliptic curve, over a finite field. These functions' characteristics will be more elaborated on in the coming sections. In this article, we will introduce an identity – based multiple key agreement protocol which produces more keys and is much more secure in comparison with the current schemes. Because this scheme uses public key challenge – response identification method to verify the opposite person, therefore, this scheme can be compared with identification schemes of this sort, too. Challenge – response schemes like [2][3][4][5][6][26] have 3 main stages of information transmitting (including commitment, challenge, and response). The scheme presented in this paper, in addition to identification, makes the production of shared keys possible. This is done through increasing the quantity of the transmitted values in this stage. So, it is more efficient than the so far mentioned identification schemes. The article will proceed with the next section's elucidation of some introductory concepts. In part 3, we will offer our suggested scheme. In part 4, we will check its security. In

part 5, the required computation of each part of the presented scheme will be computated and in the final part, this scheme will be compared with other existing schemes.

2. Introductory Concepts

Definition 1: Elliptic curve discrete logarithm problem (ECDLP) states that if the elliptic curve E is defined over the field F_q, and the point $P \in E(F_q)$ with the order *n* and the point $Q \in \langle P \rangle$ are known, then an integer number $l \in [0, n-1]$ will be found so that $Q = lP$ holds.

Definition 2: Assuming q is a prime number; if G_1 and G_2 are two cyclic groups of order q; it will be a pairing $e : G_1 \times G_1 \to G_2$ with these propertys:

1. *Bilinear:* $\hat{e}(aP, bQ) = e(P,Q)^{ab}$ for all $P, Q \in G_1$, $a, b \in Z_q^*$;
2. *Non-Degenerate:* There exists $P, Q \in G_1$ so that $\hat{e}(P,Q) \neq 1$;
3. *Computable:* There is an efficient algorithm to compute $\hat{e}(P,Q)$ for all $P, Q \in G_1$.

3. The Proposed scheme

In this section, the article will introduce the new identity – based multiple key agreement scheme. An identity – based scheme has three stages of set up, key extract, and key agreement. A more detailed look at these stages will follow.

The Set up Stage:

Assuming E is an elliptic curve defined over the field F_p. The key generation center (KGC) selects the point $P \in E\left(F_p\right)$ in a way that its order equals the prime number q. Now, the KGC selects cyclic groups $G_2, G_1 = \langle P \rangle$ of the order q and lets the pairing $e : G_1 \times G_1 \to G_2$. Then the KGC selects the hash function $H_1 : \{0,1\}^* \to Z_q^*, H : \{0,1\}^* \to G_1$. The H function takes a string with a desired length to a point which is a member of $G_1 = \langle P \rangle$. The key generation center, in order to produce its private key, randomly chooses the value of $s \in Z_q^*$ and computes the value of its public key i.e. $P_{pub} = sP$. The system's public parameters are $\{p, q, G_1, G_2, E, P, P_{pub}, H, H_1, e\}$ and the value of $s \in Z_q^*$ must also remain hidden.

The Key extract Stage:

For each user with the identity $ID \in \{0,1\}^*$ and public key $Q_{ID} = H(ID)$, the key generation center computes the value of $S_{ID} = sQ_{ID}$ as the user's private key and sends it to him/her through a secure channel. Thus, there will be a pair of identity – based keys equal to $\{Q_{ID}, S_{ID}\}$ so that $Q_{ID}, S_{ID} \in G_1$. Each user with this identity $ID \in \{0,1\}^*$ can verify his/her private key by checking this equation:

$e\left(P, S_{ID}\right) = e\left(P_{pub}, Q_{ID}\right)$.

So, the KGC produces a pair of identity – based keys for each side, i.e. A and B, in a way that the value of $\{Q_{IDA}, S_{IDA}\}$ is for the side A and the value of $\{Q_{IDB}, S_{IDB}\}$ for the side B.

The Multiple key agreement Stage:

Now, to generate shared keys, the sides A and B will do as follows:

Commitment: B randomly selects the value of $c \in Z_q^*$ and computes the value of $C = cQ_{IDB}$ and sends it to A.

Challenge: A randomly selects the value of $t \in Z_q^*$ and computes the values of $T = tQ_{IDA}$ and $\bar{Y} = (t + H_1(C \| IDB \| IDA))S_{IDA}$ and sends the set $\{T, \bar{Y}\}$ to B.

Response: B first finds the value of $f = H_1(T \| IDA \| IDB)$ and then computes $Y = (c + f)S_{IDB}$ and sends the value of Y to A.

Verification: A first computes $f = H_1(T \| IDA \| IDB)$ and then accepts B's identity if and only if this equation holds:

$$e(P, Y) = e(P_{pub}, C + f\, Q_{IDB}).$$

Key agreement: After verifying B's identity, A produces shared keys this way:

$$\begin{aligned} K_1 &= e(S_{IDA}, C)^t \\ &= e(s\,Q_{IDA}, c\,Q_{IDB})^t \\ &= e(Q_{IDA}, Q_{IDB})^{tcs}. \\ K_2 &= e(S_{IDA}, Q_{IDB})K_1 \\ &= e(s\,Q_{IDA}, Q_{IDB})K_1 \\ &= e(Q_{IDA}, Q_{IDB})^s K_1. \\ K_3 &= e(S_{IDA}, C)K_1 \\ &= e(s\,Q_{IDA}, c\,Q_{IDB})K_1 \\ &= e(Q_{IDA}, Q_{IDB})^{cs} K_1. \end{aligned}$$

$$\begin{aligned} K_4 &= e(S_{IDA}, Q_{IDB})^t K_1 \\ &= e(\,sQ_{IDA}, Q_{IDB})^t K_1 \\ &= e(\,Q_{IDA}, Q_{IDB})^{ts} K_1. \end{aligned}$$

B first computes $f' = H_1(C \| IDB \| IDA)$ and then considers this equation $e(P, \bar{Y}) = e(P_{pub}, T + f'Q_{IDA})$ and if it was affirmed, B produces shared keys this way:

$$
\begin{aligned}
K_1 &= e\left(T, S_{IDB}\right)^c \\
&= e\left(t\,Q_{IDA}, s\,Q_{IDB}\right)^c \\
&= e\left(Q_{IDA}, Q_{IDB}\right)^{tcs}, \\
K_2 &= e\left(Q_{IDA}, S_{IDB}\right) K_1 \\
&= e\left(Q_{IDA}, s\,Q_{IDB}\right) K_1 \\
&= e\left(Q_{IDA}, Q_{IDB}\right)^s K_1, \\
K_3 &= e\left(Q_{IDA}, S_{IDB}\right)^c K_1 \\
&= e\left(Q_{IDA}, s\,Q_{IDB}\right)^c K_1 \\
&= e\left(Q_{IDA}, Q_{IDB}\right)^{cs} K_1, \\
K_4 &= e\left(T, S_{IDB}\right) K_1 \\
&= e\left(t\,Q_{IDA}, sQ_{IDB}\right) K_1 . \\
&= e\left(Q_{IDA}, Q_{IDB}\right)^{ts} K_1 .
\end{aligned}
$$

4. Security Analysis

In this section, the security notes of the above scheme will be examined.

Note 3: Because in the commitment stage, the value of c in the challenge stage and the value of t are randomly selected; so, respectively the values of $f' = H_1\left(C \| IDB \| IDA\right), C = c\,Q_{IDB}$ and $f = H_1\left(T \| IDA \| IDB\right), T = t\,Q_{IDA}$ related to them are also random.

Note 4: If in this scheme, we take A as the center (server) and B as the user, A will not need to send the value of D in the challenge stage. As a result, B also will not need to check the verification relation. This way, the computational complexity and the quantity of the sent values decrease and the scheme's efficiency increases.

Theorem 5: This paper's proposed scheme has the completeness property; this means that an honest verifier affirms the real prover (user) after the verification stage.

Proof: Generally this scheme has 2 verification relations; and we will first prove the first one which is used in the 4^{th} stage of the scheme:

$$
\begin{aligned}
e\left(P, Y\right) &= e\left(P, \left(c + f\right) S_{IDB}\right) \\
&= e\left(P, \left(c + f\right) s\,Q_{IDB}\right) \\
&= e\left(sP, cQ_{IDB} + fQ_{IDB}\right) \\
&= e\left(P_{pub}, C + fQ_{IDB}\right).
\end{aligned}
$$

Therefore this verification relation is complete. Now, we will take a look at the second

verification relation which is executed by B in the 5^{th} stage:

$$\begin{aligned} e(P,\overline{Y}) &= e(P,(t+H_1(C\|IDB\|IDA))S_{IDA}) \\ &= e(P,(t+f')S_{IDA}) \\ &= e(P,(t+f')sQ_{IDA}) \\ &= e(sP,tQ_{IDA}+f'Q_{IDA}) \\ &= e(P_{pub},T+f'Q_{IDA}). \end{aligned}$$

Consequently, the second verification relation is also complete.

Theorem 6: The scheme offered here has the soundness property.

Proof: In order to prove this property, we will have to show that impersonating somebody needs having his/her private parameters (or the ability to compute them) by the forger. Now, assuming the forger can impersonate B, s/he has succeeded, at least twice, in cheating A with these values $(Y_1,f_1),(Y_2,f_2)$ in the verification relation. Thus, we'll have:

$$\begin{aligned} &Y_1=(c+f_1)S_{IDB} \\ &Y_2=(c+f_2)S_{IDB} \\ &\Rightarrow Y_2-Y_1=cS_{IDB}+f_2S_{IDB}-cS_{IDB}-f_1S_{IDB} \\ &\Rightarrow Y_2-Y_1=(f_2-f_1)S_{IDB} \\ &\Rightarrow S_{IDB}=(f_2-f_1)^{-1}(Y_2-Y_1). \end{aligned}$$

As a result, some one able to forge B's identity twice, will surely be able to compute B's private key. This is true also for the other side. The opposite of what we have so far mentioned is also absolutely obvious, i.e. anybody having A's and B's private parameters will be able to forge their identities.

Theorem 7: The verification relation introduced in the key extract stage of our scheme has the completeness property. This relation confirms the user's private key which is issued by the key generation center.

Proof: The user having $\{Q_{ID},S_{ID}\}$ has to use this equation to affirm his or her private key.

$$\begin{aligned} e(P,S_{ID}) &= e(P,sQ_{ID}) \\ &= e(sP,Q_{ID}) \\ &= e(P_{pub},Q_{ID}). \end{aligned}$$

Theorem 8: This Paper's scheme has the zero – knowledge proof property. It means that the prover succeeds in proving his/her identity to the verifier without revealing any of his/her hidden information.

Proof: A (B) has this information $(\{Q_{IDA},T,\overline{Y}\})\{Q_{IDB},C,Y\}$ of the other side. Finding B's

(A's) private key i.e. $(S_{IDA})S_{IDB}$ from $(\bar{Y} = (t + f')S_{IDA})Y = (c + f)S_{IDB}$ is impossible because the random value of c (t) is unknown. On the other hand, finding c (t) from the relation $(T = tQ_{IDA})$ $C = cQ_{IDB}$ requires solving the discrete logarithm problem. Therefore, this scheme has zero – knowledge proof property.

Theorem 9: This paper's scheme has the perfect forward secrecy. It means that if both A's and B's private keys are revealed, the security of their previous common hidden keys will not be endangered and no intruder will be able to compute previous session's keys.

Proof: We will show that if an intruder has the private keys of both sides of A and B, s/he must know at least one of the randomly produced values of the previous session's keys. Assuming an intruder has the values of $\{S_{IDA}, S_{IDB}, Q_{IDA}, Q_{IDB}, T, C\}$; with regard to the relation $K_1 = e(S_{IDA}, C)^t = e(T, S_{IDB})^c$, it is clear that the intruder must have one of the random values of t or c in order to compute K_1. Therefore, the intruder's disability to compute K_1, prevents his finding the previous session's keys. Thus this scheme has the property of perfect forward secrecy .

Theorem 10: If the intruder can guess the challenge value, then s/he will be able to cheat the verifier in the verification relation.

Proof: Assuming the intruder knows (or can guess) the value of *f*; (thus, s/he sends the value $C = P - fQ_{IDB}$ in the commitment stage, and the value $Y = P_{pub}$ in the response stage to the opposite person. Now, with regard to the verification relation, we have:

$$\begin{aligned} e(P_{pub}, C + fQ_{IDB}) &= e(P_{pub}, P - fQ_{IDB} + fQ_{IDB}) \\ &= e(P_{pub}, P) \\ &= e(P, P_{pub}) \\ &= e(P, Y) \end{aligned}$$

Therefore, the intruder will succeed in cheating the other side in the verification relation. Because $f \in Z_q^*$ is a random value, thus the probability of the intruder's correctly guessing the challenge value is $\frac{1}{q-1}$. Now, regarding the fact that q is a very large prime number, this probability is negligible. This happens in many well-known identification schemes such as [4] [5][6].

Theorem 11: The scheme introduced here has the property of key-compromise impersonation security. This means that if A's long-term private key is revealed, the intruder even having it, will not be able to introduce himself instead of B to A.

Proof: Because A's private key has no impact on B's sent value (the signature or the answer of $Y = (c + f)S_{IDB}$); so, the intruder having A's private key cannot impersonate B. It is the same for the opposite side.

Theorem 12: The scheme offered in this paper has the property of known-key security; meaning that if the intruder gets access to a session key, s/he will not be able to compute the

succeeding session keys.

Proof: Because the succeeding session keys are dependent on the private keys and random values of the two sides of the protocol, the intruder will not be able to compute the next session keys.

Theorem 13: The scheme proposed in this paper has the property of unknown key security and is immune against the man-in-the-middle attack.

Proof: The property of unknown key security means that assuming A and B are executing the key agreement protocol, the active intruder C must not be able to interfere in the protocol in a way that after ending the protocol, A believes he has done key agreement protocol with B; but on the other hand, B believes that he has produced a common secret key with C (the intruder). The man-in-the-middle attack is: suppose A and B are executing the key agreement protocol; in this attack, the active intruder C interferes in doing the protocol in a way that makes the two sides of the protocol agree different keys. Now, in this paper's scheme before the two sides' key agreement stage, the challenge-response method will be used for the opposite side's identification; and therefore they will make use of the other side's identity before the production of the shared key. Thus, this scheme is secure against the above mentioned attacks.

Theorem 14: Our suggested scheme has the strong security property. This means that in case any of the pairs (A's private key, B's random value) or (A's random value, B's private key) or (A's random value, B's private key) or (A's random value, B's random value) is revealed, the protocol's security will not be at risk.

Proof: This scheme is designed in a way that in case of disclosing any of the pairs (S_{IDB}, S_{IDA}) or (t, S_{IDB}) or (c, S_{IDB}) or (c, t), the value of the K_1 key cannot be computed. As mentioned before, with regard to $K_1 = e(S_{IDA}, C)^t = e(T, S_{IDB})^c$, we can compute K_1 only when we have access to one of these pairs (S_{IDA}, t) or (S_{IDB}, c). Therefore, the K_1 key has the strong security property and so other keys resulted from it, also enjoy this property.

5. Computational Complexity

Here is a brief account of the needed computations for each stage of the above protocol:

- *Setup Stage:*
  1 scalar multiplication in G_1.
- *Key Extract Stage:*
  1 scalar multiplication in G_1, 1 hash function to produce key for each user.
- *Key Verification Stage:*
  2 pairings.
- *Key Agreement Stage:*
  Commitment: 1 scalar multiplication in G_1.
  Challenge: 2 scalar multiplications in G_1, 1 addition in G_2, 1 hash function.
  Response: 1 scalar multiplication in G_1, 1 addition in G_2, 1 hash function.
  Verification: 2 pairings, 1 scalar multiplication and 1 addition in G_1, 1 hash function for each user.

Key Agreement: To produce K_1, 1 pairing, 1 exponentiation in G_2 and to produce other keys, 3 pairings, 1 exponentiation and 3 multiplications in G_2 are required for each user.

6. Comparison

In this section, there will be a comparison between our newly introduced scheme and other similar schemes and at the end the gist of this discussion will come in table 1. As stated before, public key challenge-response identification protocols like [2][3][4][5][6][26] have 3 general stages (commitment, challenge, response) like the scheme offered in this paper where for some more operation and the multiple key agreement ability added to these stages of the scheme, our protocol has become much more superior over the mentioned schemes. In identity-based key agreement schemes like [13][14][17][18][19][20][21] for 2 randomly chosen values, they will be able to produce 1 key. The schemes [15][16] produce only one shared key for 4 randomly produced values. Also, Oh et.al's scheme [22] is able to generate 2 shared keys for 2 random points. Moreover, it is worth noting that not all existing key agreement schemes such as [5][22][24] satisfy some of the security conditions mentioned above. The number of shared keys produced in some protocols such as [5][24] are at most 4 shared keys for making 4 random numbers; and this number equals the shared keys produced in this article's scheme for producing 2 random values. In addition, in many multiple key agreement schemes like [5][24], the number of randomly produced values by each of the two sides is 2. This means, in the total protocol, 4 random values are produced and for each of the random values, a multiple of P is computed: while in the protocol suggested in this article, each of the two sides generates only one random value and computes one multiple of P and in the whole protocol, two random values and their corresponding P multiples are produced which also adds to the efficiency of this scheme. Also, as proved above, this scheme satisfies some important security conditions like perfect forward secrecy and strong security.

Table 1. Comparison

Index of scheme	Type of Scheme	Identity – Based	Number of selected random number in scheme	Number of mutual key
[2][3][4][5][6]	Identification	×	2	×
[26]	Identification	✓	2	×
[27]	Key agreement-Identification	×	1	1
[13][14][17][18][19][20][21]	Key agreement	✓	2	1
[22]	Key agreement	✓	2	2
[15][16]	Key agreement	✓	4	1
[5][24]	Key agreement		4	4
Our scheme	Key agreement-Identification	✓	2	4

7. Conclusions

In this paper, a multiple key agreement scheme is presented which is identity-based and uses the challenge-response method to verify the identities of the two sides of the protocol. Moreover, this scheme is zero-knowledge proof: and for the 2 randomly produced values in the scheme, 4 shared keys are generated. This article's proposed scheme satisfies all the security conditions related to key agreement like perfect forward secrecy and strong security. Therefore, in comparison with many current key agreement schemes, this is more efficient.

References

[1] U. Feige, A. Fiat, A. Shamir, "Zero- Knowledge Proofs of Identity," *Journal of Cryptology*, vol. 1, pp. 77-94, 1988. Article (CrossRef Link)

[2] M. H. Dehkordi, R. Alimoradi, "Zero-Knowledge Identification Scheme Based on Weil Pairing," *Lobachevskii Journal of Mathematics*, vol. 30, no. 3, pp. 203-207, 2009. Article (CrossRef Link)

[3] M. H. Dehkordi, R. Alimoradi, "A New Batch Identification Scheme," *Discrete Mathematics, Algorithms and Applications*, vol. 1, no. 3, pp. 369-376, 2009.

[4] A. Fiat, A. Shamir, "How To Prove Yourself: Practical Solutions of Identification and Signature Problems," in *Proc. of International Conference on Advances in Cryptology (CRYPTO'86)*, pp. 186-194, 1987.

[5] L. Harn, H.-Y. Lin, "An Authenticated Key Agreement Protocol Without using One-way Function," in *Proc. of 8th Information Security Conference*, pp. 155–60, May 1998. Article (CrossRef Link)

[6] M. Scott, "Authenticated ID-based Key Exchange and Remote Log-in with Insecure Token and PIN Number," in *Proc. of International Conference on Advances in Cryptology (CRYPTO'01)*, pp. 213-229, 2001. Article (CrossRef Link)

[7] H. Sun, B. Hsieh, "Security Analysis of Shim's Authenticated Key Agreement Protocols from Pairings," Cryptology ePrint Archive, Report 2003/113, http://eprint.iacr.org/2003/113.

[8] S. Kim, H. Lee, H. Oh, "Enhanced ID-Based Authenticated Key Agreement Protocols for a Multiple Independent PKG Environment," in *Proc. of ICICS 2005*, pp. 323-335, 2005.

[9] K. Shim, "Efficient ID-based Authenticated Key Agreement Protocol based on the Weil Pairing," *Electronics Letters*, vol. 39, pp. 653-654, 2003. Article (CrossRef Link)

[10] K-A. Shim and S-H. Seo, "Cryptanalysis of ID-Based Authenticated Key Agreement Protocols from Bilinear Pairings," in *Proc. of ICICS 2006*, pp. 410-419, 2006. Article (CrossRef Link)

[11] S. Wang, Z. Cao, Z. Cheng, K.-K.R. Choo, "Perfect Forward Secure Identity-Based Authenticated Key Agreement Protocol in the Escrow Mode," Cryptology ePrint Archive, Report 2007.

[12] Y.-J. Choie, E. Jeong and E. Lee, "Efficient Identity based Authenticated Key Agreement Protocol from Pairings," *Journal of Applied Mathematics and Computation*, vol. 162, no. 1, pp. 179-188, 2005. Article (CrossRef Link)

[13] S.S.M. Chow and K.-K.R. Choo, "Strongly-Secure Identity-Based Key Agreement and Anonymous Extension," in *Proc. of ISC 2007*, pp. 203-220, 2007. Article (CrossRef Link)

[14] M. Kim and K. Kim, "A New Identification Scheme Based on the Bilinear Diffie- Hellman Problem," in *Proc. of the 7th Australian Conference on Information Security and Privacy*, pp. 362-378, 2002. Article (CrossRef Link)

[15] N.-Y. Lee, C.-N. Wu, C.-C. Wang, "Authenticated Multiple Key Exchange Protocols based on Elliptic Curves and Bilinear Pairings," *Computers and Electrical Engineering*, vol. 34, pp. 12-20, 2008. Article (CrossRef Link)

[16] C. P. Schnorr, "Efficient Signature Generation by Smart Cards," *Journal of Cryptology*, vol. 4, pp. 161-174, 1991. Article (CrossRef Link)

[17] J. Shao, R. Lu, and Z. Cao, "A New Efficient Identification Scheme Based on the Strong Diffie-Hellman Assumption, in *Proc. of the International Symposium on Future Software Technology*, 2004. Article (CrossRef Link)

[18] Y. Wang, "Efficient Identity-Based and Authenticated Key Agreement Protocol," Cryptology

ePrint Archive, Report 2005/108, 2005, http://eprint.iacr.org/2005/108/.
[19] Y. Xun, "Efficient ID-based Key Agreement from Weil Pairing," *Electronics Letters*, vol. 23, pp. 206-208, 2003. Article (CrossRef Link)
[20] Q. Yuan and S.-P. Li, "A New Efficient ID-Based Authenticated Key Agreement Protocol," Cryptology ePrint Archive: Report 309/2005, *http://*eprint.iacr.org/2005/309.pdf.
[21] E.-K. Ryu, E.-J. Yoon, and K.-Y. Yoo, "An Efficient ID-Based Authenticated Key Agreement Protocol from Pairings," in *Proc. of 3rd International IFIP-TC6 Networking Conference on Networking Technologies, Services, and Protocols (NETWORKING'04)*, pp. 1464-1469, 2004. Article (CrossRef Link)
[22] J.-B. Oh, E.-J. Yoon and K.-Y. Yoo, "An Efficient ID Based Authenticated Key Agreement Protocol with Pairings," in *Proc. of 5th International Symposium on Parallel and Distributed Processing and Applications (ISPA 2007)*, pp. 446-456, 2007. Article (CrossRef Link)
[23] H. Lee, D. Kim, S. Kim, H. Oh, "Identity-based Key Agreement Protocols in a Multiple PKG Environment," in *Proc. of the Int. Conf. on Computational Science and Its Applications (ICCSA'05)*, pp. 877-886, 2005. Article (CrossRef Link)
[24] N. Smart, "An Identity based Authenticated Key Agreement Protocol based on the Weil Pairing," *Electronics Letters*, vol. 38, pp. 630-632, 2002. Article (CrossRef Link)
[25] K. Kim, E. Ryu and K. Yoo, "ID-based Authenticated Multiple-key Agreement Protocol from Pairing," in *Proc. of International Conference on Computational Science and Its Applications (ICCSA'04)*, pp. 672-680, 2004. Article (CrossRef Link)
[26] A. M Allam, I. I. Ibrahim, I. A. Ali, A.H. Elsawy, "Efficient Zero-Knowledge Identification Scheme with Secret Key Exchange," in *Proc. of IEEE 46th Midwest Symposium on Circuits and Systems*, pp. 516-519, Dec. 2004. Article (CrossRef Link)

Massoud Hadian Dehkordi received the Ph.D. degree in Applicable Number Theory from the University of Loughborough, Loghborough,United Kingdom in 1998. He is an associate professor in the School of Mathematical Sciences in Iran University of Science and Technology. His research interests includes cryptography, applicable Number theory and other related topics.

Reza Alimoradi received his BS degree in Mathematics from Bu- Ali Sina University, Iran, in 2005. In 2007, he received his MS degree in Mathematics from Iran University of Science and Technology, Iran. In 2012, he received his PhD degree in Mathematics from Iran University of Science and Technology, Iran. He is an associate professor of the Faculty of Science at In Qom University, Iran. His current research interests include cryptography, and coding theory.